



European Center for Constitutional and Human Rights

Filed with:

Constitutional Court  
Place Royale, 7  
1000 Brussels  
Belgium

**Request for Intervention**

Pursuant to Article 87(2) of the Special Law of 6 January 1989 and filed in support of the application (of 1 March 2010, published in the Official Journal on 21 April 2010) for annulment of the legislation implementing Council Decision 2007/551/CFSP/JHA (of 23 July 2007) on the 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 US Department of Homeland Security (DHS).

On behalf of:

European Center for Constitutional and Human Rights  
Zossener Str. 55-58, Aufgang D  
D-10961 Berlin  
Germany.

Represented by:

Christophe Marchand  
Jus Cogens Avocats  
Rue Marche au Charbon 83  
B-1000 Brussels  
Belgium

17 May 2010

## Introduction

This submission has been prepared by the European Center for Constitutional Rights (ECCHR) and is filed pursuant to Article 87(2) of the Special Law (dated 6 January 1989) of the Constitutional Court. It aims to both provide the basis for ECCHR's request to join the current proceedings as an interested party and support the application (filed on 1 March 2010 and published in the Official Journal on 21 April 2010) for annulment of the legislation implementing Council Decision 2007/551/CFSP/JHA (of 23 July 2007) on the 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 US Department of Homeland Security (DHS) (hereafter, the Agreement).

ECCHR is an independent, non-profit legal and educational organisation dedicated to protecting civil and human rights throughout, and beyond, Europe. Founded by a small group of human rights lawyers in 2007 and based in Berlin, ECCHR aims to facilitate, support and directly engage in innovative litigation - using international, European and national laws - to enforce and defend human rights standards and hold state and non-state actors accountable for egregious abuses. For the purposes of the current application, ECCHR is represented by our Belgian representative and advocate, Christophe Marchand.

ECCHR have considerable experience and legal expertise in the area of counter-terrorism and human rights, with a particular emphasis on supporting litigation in the defence of fundamental rights. We have, for example, previously undertaken high-profile litigation in a number of different European jurisdictions against key US officials responsible for the design and implementation of the US 'war on terror' program in the post 9-11 context – including the filing of two criminal complaints in Germany (in 2004 and 2006) and a similar complaint in France (in 2007) against former US Secretary of Defense Donald Rumsfeld and other high ranking US military personnel involved *inter alia* in the detention and torture of detainees in Iraq and Guantánamo. We have also been active on the issue of extraordinary rendition – including intervening (in March 2010, by way of amicus curiae brief) in the US Supreme Court case of Maher Arar who was abducted by US officials in 2002 and rendered to Syria and tortured and publishing (in January 2009) the second edition of the report "CIA 'Extraordinary Rendition' Flights, Torture and Accountability: A European Approach" providing a comprehensive overview of European legal proceedings against the CIA rendition program. ECCHR have also actively defended fundamental rights in the context of both the EU and UN 'terror list' / targeted sanctions programs, representing *inter alia* Jose Maria Sison in his successful challenge against his listing before the European Court of Justice (Case T-341/07, dated 30 September 2009).

Given our background and expertise in this area we submit that ECCHR has both a legitimate and sufficient interest, pursuant to Article 87(2) of the Special Law cited above, and is well placed to assist the Court in this important matter. For the Court's reference, we enclose the relevant statutes of our organisation and a short letter from ECCHR's General-Secretary confirming our intention and capacity to join the current proceedings as Annex A.

## Legal submissions

Our submissions focus on three fundamental rights which we argue are breached by the Agreement, namely:

- (i) *The right to respect for private life* - pursuant to Article 8 of the European Convention of Human Rights (hereafter, 'the European Convention') and Article 7 of the Charter of Fundamental Rights of the European Union (hereafter, 'the Charter').
- (ii) *The right to data protection* – pursuant to Article 8 of the Charter, read in conjunction with Directive 95/46/EC (hereafter, 'the Data Protection Directive') and the Council of

Europe Convention of 28 January 1981 for the Protection of Individuals with Regard to Automatic Processing of Personal Data (hereafter, 'the 1981 Convention'); and

- (iii) *The right to freedom from discrimination* – pursuant to Article 21 of the Charter and Article 14 of the European Convention.

### 1. The Right to Respect for Private Life

As is well known, Article 8 of the European Convention provides:

- (1) *Everyone has the right to respect for his private and family life, his home and correspondence.*
- (2) *There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

This right has been effectively mirrored by Article 7 of the Charter of Fundamental Rights which simply states:

*Article 7 Respect for private and family life*

*Everyone has the right to respect for his or her private and family life, home and communications.*

It is not in dispute that the PNR Agreement - which facilitates the collection, storage and analysis of 19 fields of personal passenger data for law enforcement purposes<sup>1</sup> - engages or otherwise interferes with the right to respect for private life<sup>2</sup>. The issue in this case is whether the interference is both "in accordance with the law" (that is, whether it satisfies the principle of legality) and "necessary in a democratic society" (that is, in satisfaction of the principles of legitimacy, necessity and proportionality) and it is to these two elements that our submission now turns.

#### (1) Accordance with the Law

##### (a) *Legality*

It is well established that in order to satisfy the principle of legality and be in compliance with the rule of law any restriction on a Convention right must be subject to effective control. Whilst a restriction which has a firm basis in either legislation (either primary or delegated<sup>3</sup>) or European Community law will ordinarily meet this requirement, other 'soft law' agreements which lack either binding capacity or enforceability can clearly fall short of this measure.

The current 2007 PNR agreement is composed of 3 interrelated but distinct elements: first; the short agreement signed by both parties, second; the letter from the Department of Homeland Security (DHS) to the EU and third, the letter from the EU to the DHS. Whilst the first part of the formal document is nominally an international agreement made pursuant to Articles 24 and 38 (Titles V and VI) of the Treaty on European Union, the legal basis, certainty and enforceability of the latter, 'letter exchange' part of the document is far from clear. We note that it is in the 'letter exchange', rather than in the body of the formal agreement itself, that the substantial clauses of the Agreement are contained and we question the veracity of concluding such a far-reaching international agreement by way of letter exchange in this way. In practice, such a method has effectively served to introduce

---

<sup>1</sup> As detailed in para. III of the DHS letter supplementing the 2007 EU-USA PNR Agreement

<sup>2</sup> In *Amann v Switzerland* [(2000) 30 EHRR 5], for example, the European Court of Human Rights (hereafter ECHR), drawing on earlier European Jurisprudence on this issue, clearly stated (at para. 65) that "the storing of data relating to the "private life" of an individual falls within the application of Article 8 § 1". See also, *Rotaru v Romania* (2000) Application No. 28341/95, (at paras. 42 – 44) and *Leander v Sweden* (1987) 9 EHRR 433

<sup>3</sup> *Barthold v Germany* (1985) 7 EHRR 383

unilateral amendment process whereby the DHS simply addresses 'DHS letters' to the EU who subsequently assess and respond accordingly<sup>4</sup>.

This issue of unilateral amendment is clearly and succinctly exemplified through the issue of privacy protections afforded under the current Agreement. In order to assuage EU privacy concerns, the DHS (at para. IV of the DHS letter):

made a policy decision to extend administrative Privacy Act protections to PNR data stored in the ATS regardless of the nationality or country of residence of the data subject, including data that relates to European citizens. Consistent with U.S law, DHS also maintains a system accessible by individuals, regardless of their nationality or country of residence, for providing redress to persons seeking information about or correction of PNR.

However, on 15 August 2007, less than two months after the PNR Agreement was signed, the DHS announced its "notice of a revised and updated system of records pursuant to the Privacy Act 1974 for the Arrival and Departure Information System (ADIS)". Under this proposal, the DHS sought to exempt ADIS information (which includes PNR and API data provided *inter alia* by "foreign governments") from disclosure on the basis of "criminal, civil and administrative enforcement requirements"<sup>5</sup> – thus unilaterally amending and effectively undermining the protections afforded by their earlier assurances in order to "counterbalance 'the set backs' for the US government in the [2007] EU-US PNR agreement"<sup>6</sup>.

It is clear, moreover, that the "assurances" contained in the DHS letter are not binding commitments – that is, the DHS "assures" but does not "warrant" or "undertake" to protect European PNR data<sup>7</sup>. Indeed, the penultimate paragraph of the DHS letter clearly states that "this Agreement does not create or confer any right or benefit on any other person or entity, private or public". Furthermore, there is no indication to suggest that the assurances have been incorporated into any type of enforceable, statutory form in the USA. We will discuss this issue in more detail below when considering the lack of procedural safeguards and the inadequacy of enforceability mechanisms available to Belgian citizens under current agreement. Suffice to say, it is questionable if anything apart from political or diplomatic considerations actually commits the US authorities who handle European PNR data to comply with the assurances supplementing this Agreement. Lacking judicially enforceable statutory regulation that allows for either criminal sanctions or the award of civil damages in the event of breach, it seems clear that the DHS is not bound by its assurances<sup>8</sup>. As a result, we submit that the interference with fundamental rights facilitated by the Agreement is not subject to "effective control" as required to meet the principle of legality and, as such, would be unlawful from the position of European human rights jurisprudence.

#### (b) Legal Certainty

---

<sup>4</sup> See Papakonstantinou, V. and de Hert, P. (2009) "The PNR Agreement and transatlantic anti-terrorism co-operation: no firm human rights framework on either side of the Atlantic" in *Common Market Law Review* 46(3): 885 – 919 (at p. 910).

<sup>5</sup> Federal Register: Aug. 22, 2007 (Volume 72, No. 162). For analysis see [www.statewatch.org/news/2007/aug/usa-adis-privacy-act-exemptions.pdf](http://www.statewatch.org/news/2007/aug/usa-adis-privacy-act-exemptions.pdf) and [www.statewatch.org/news/2007/sep/04eu-usa-pnr-exemptions.htm](http://www.statewatch.org/news/2007/sep/04eu-usa-pnr-exemptions.htm)

<sup>6</sup> See EDRI "US gains new advantages in the EU-USA PNR agreement", Newsletter No. 5.17, 12 September 2007. Available at <http://www.edri.org/book/export/html/1284>. Similarly, on 30 July 2007, DHS wrote to the EU Council formally requesting that all the documents concerning the negotiations that lead to the 2007 EU-US PNR Agreement be kept secret "for at least ten years after the entry into force of the agreements". See <http://www.statewatch.org/news/2007/sep/eu-usa-pnr-12305-07.pdf>

<sup>7</sup> *Ibid*, p.909

<sup>8</sup> See Ntouvis, I. (2008) "Case Comment: Air passenger data transfer to the USA: the decision of the ECJ and latest developments" in *International Journal of Law & Information Technology* 16(1): 73 – 95 (at 89). Whilst Ntouvis discusses the enforceability status of the 2006 Interim PNR Agreement, we submit that the same problems still underscore the current arrangement.

Furthermore, in order to satisfy the principle of legality, a law or rule which interferes with a fundamental right must be formulated with sufficient clarity to enable those likely to be affected to both understand the provision and accordingly regulate their conduct<sup>9</sup>. In European jurisprudence this requirement is known as the principle of 'legal certainty'. Whilst absolute certainty and foreseeability is not required<sup>10</sup>, there must nevertheless be "detailed rules setting out the basis upon which the activities [such as secret surveillance] can be carried out"<sup>11</sup> and/or "sufficient indication of the circumstances in which discretion will be exercised"<sup>12</sup>.

Thus in *Huvig v France* the ECHR found that telephone tapping by state authorities failed to meet the requirements of legal certainty, notwithstanding the fact that the surveillance was regulated by French Criminal Code, because, *inter alia*, the categories of persons liable to be subject to surveillance were insufficiently defined and no rules existed to govern the destruction of information obtained through intercept surveillance when no proceedings were pursued and/or the person was subsequently acquitted<sup>13</sup>. In *Kopp v Switzerland*<sup>14</sup>, the ECHR were asked to rule on the legality of state interception of telephone calls by a lawyer who was not himself suspected by the authorities of having committed any offence. Despite the fact that the Court Order authorising the interception expressly stated that "the lawyers conversations [were] not to be taken into account" in accordance with the Swiss law on legal professional privilege, the Court nevertheless found that the legal certainty provisions of Article 8(2) of the European Convention were breached because the law lacked sufficient clarity as to how professional privilege - and the discretion distinguishing privileged and non-privileged communications - was to be protected and exercised *in practice*<sup>15</sup>. Similarly, in *Govell v UK*<sup>16</sup>, the European Commission of Human Rights found that covert surveillance provisions were not "prescribed by law" because the guidelines governing their use were neither legally binding nor publically accessible.

In addition to the arguments outlined at pp. 15 – 20 of the Claimant's application for annulment, we submit that there are three ways that the current agreement is in breach of the legal certainty requirements outlined above.

First, there is insufficient legal certainty concerning the exercise of discretion over the executive use of "sensitive data" – defined (at para. III of the DHS letter) as "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and data concerning the health or sex life of the individual". According to the DHS letter: "Unless the data is accessed for an exceptional case, as described in the next paragraph, DHS promptly deletes the sensitive EU PNR data". In the following paragraph, however, "exceptional case" is broadly defined as one where "the life of a data subject or of others could be imperiled or seriously impaired". The potentially discriminatory effects of this provision are explored in further detail later in this submission. At this point, we simply observe that there are no further guidelines defining or otherwise limiting the scope of this important provision. Consequently, without further qualification, we submit that this provision is unduly broad, imprecise and *prima facie* fails to provide individuals with a sufficient indication of the circumstances which executive discretion to interfere with their fundamental rights will be exercised.

Second, we note that it is effectively impossible for an individual to know what use can be made of their private data within the PNR profiling system that is enabled by this Agreement. Data profiling

---

<sup>9</sup> *Sunday Times v UK* (1979-80) 2 EHRR 245

<sup>10</sup> *Ibid*, at para. 49

<sup>11</sup> *Huvig v France* (1990) 12 EHRR 528 (at para. 15.9)

<sup>12</sup> *Silver v UK* (1983) 5 EHRR 347

<sup>13</sup> *supra* note 11

<sup>14</sup> (1999) 27 EHRR 91

<sup>15</sup> *Ibid* (at paras. 72 – 73).

<sup>16</sup> No. 27237/95

surveillance systems operate by collecting and then analysing an individual's personal information against a combination of characteristics and behavioral patterns in order to create a risk assessment or profile. When a passenger fits within a given profile, they are accordingly identified as high-risk - that is, as someone who either is or could potentially be associated with persons involved in terrorism or serious transnational crime. The aim of data profiling, therefore, is to apply "data base technology and techniques - such as statistical analysis and modeling - to uncover hidden patterns and subtle relationships in data and to infer rules that allow for the prediction of future results"<sup>17</sup>. In this way, the capture and analysis of an individual's data functions to create "new, secondary information about that person"<sup>18</sup>.

There is no indication - either in the Agreement or in the 2010 Joint Review undertaken by the European Commission and the DHS - as to *how* this proactive process of profiling passengers and rendering them into suspects actually works. It is clear from the draft proposal for a Council Framework Decision on the use of PNR - which aims to set up an interrelated and comparable PNR profiling system within and beyond the EU - that such PNR profiling systems aim to "identify persons who are or may be involved in a terrorist or organized crime offence, as well as their associates", "to create and update risk indicators for the assessment of such persons" and "to provide intelligence on travel patterns and other trends"<sup>19</sup>. The objective is not, therefore, to simply identify known terrorists or individuals suspected of having committed an offence but rather to proactively link through association the data from such 'suspicious passengers' to other 'ordinary passengers' on the basis of both 'abstract profiles' and categories such as travel patterns and routes, credit card use and the use of particular travel agencies as revealed through PNR data<sup>20</sup>. On the one hand, this means that:

decisions on individuals will be taken on the basis of patterns and criteria established using the data of passengers in general. Thus decisions on one individual might be derived from the data of other individuals. It is thus in relation to an abstract context that decisions will be taken.

It is clearly not possible, therefore, for an individual to know what use will be made of their PNR data for the nominal 15 year duration of the retention period - an outcome which is arguably in breach of the legal certainty and foreseeability requirements of Article 8(2) of the European Convention as outlined above<sup>21</sup>. On the other hand, we submit that the filtering process itself, as well as the criteria against which each passenger is to be scanned and/or potentially rendered a suspect - both of which are material to the interference with private life in his matter - are so poorly defined and explained that the Agreement fails to meet the requisite degree of legal certainty outlined above. There are, for example, no rules outlining the basis and ways in which such profiling will be carried out nor are there any indications as to how executive discretion will be exercised (including against what criteria) to profile potential suspects to be targeted by state authorities. It is indeed because of the unjustifiable interference with citizens fundamental rights facilitated by the existing EU-USA PNR Agreement that the European Parliament have demanded - in their Resolution of 5 May 2010 on the Launch of Negotiations for Passenger Name Record (PNR) agreements with the United States,

---

<sup>17</sup> US General Accounting Office "Data Mining: Federal Efforts Cover a Wide Range of Uses: Report to Ranking Minority Member, Subcommittee on Financial Management, the Budget and International Security". *Committee on Governmental Affairs, US Senate, May 2004* (at p.1)

<sup>18</sup> Gunasekara, G. (2009). "The final privacy frontier? Regulating trans-border data flows" in *International Journal of Law & Information Technology* 17(2): 147 - 179 (at 158).

<sup>19</sup> Article 3(5) Proposal for a Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes. Available at:

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007PC0654:EN:NOT>

<sup>20</sup> See Opinion of the European Data Protection Supervisor on the draft Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes (2008/C110/01).

<sup>21</sup> See also Opinion of the European Agency for Fundamental Rights on the Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes (at para. 13).

Available at: [http://fra.europa.eu/fraWebsite/research/opinions/op-pnr\\_en.htm](http://fra.europa.eu/fraWebsite/research/opinions/op-pnr_en.htm)

Australia and Canada - that “in no circumstances may PNR data be used for data mining or profiling” and that “[the] use of data must be limited to specific crimes or threats, on a case-by-case basis”<sup>22</sup>.

## (2) Necessary in a Democratic Society

In order for an interference to a fundamental right to be considered “necessary in a democratic society” three basic requirements must be met – first, there must be a pressing social need for the interference (the principle of legitimacy); second, the restriction must correspond to the need and be necessary to achieve it (the principle of necessity); and third, the restriction must be a proportionate response to that need.

### (a) *Legitimacy*

We do not contend that the stated aims of the Agreement - that is, the prevention and combating of terrorism and serious transnational crimes - are illegitimate. Such objectives correspond to objectives of general interest recognised by the European Union and are consistent with the need to protect the rights and freedoms of others as stated in Article 52 of the Charter. However, following the approach of the European Data Protection Supervisor among others, we do submit that “the means used to reach this purpose leave room for discussion”<sup>23</sup>. Our criticisms of these means, however, are developed elsewhere throughout this submission.

### (b) *Necessity*

Necessity is a core principal of Article 8 compliance and is closely interrelated with the proportionality principle discussed below such that only an interference that is *necessary* to achieve a legitimate aim can be proportionate<sup>24</sup>. It is difficult to make an assessment, on the basis of the reviews undertaken by the relevant authorities or information otherwise currently in the public domain, as to the necessity of the restrictions facilitated this Agreement - that is, whether the collection, storage and subsequent analysis of European PNR data by the US authorities is actually useful or effective in combating terrorism and serious transnational crime. For its part, the recent EC - US review of the implementation of the PNR Agreement (dated 8-9 February 2010) states simply that:

As regards the question whether PNR serves the purpose of supporting the fight against terrorism and crime, the EU team has been satisfied that this is indeed the case. PNR provides DHS with the possibility of carrying out pre-departure assessments of all passengers which provide it with the opportunity of either taking steps to prevent a passenger from boarding an aircraft or giving DHS sufficient time to carry out all the background checks before the arrival of a passenger and prepare its response. It also provides DHS with the opportunity to perform risk assessments on the basis of scenario-based targeting rules in order to identify the unknown’ potential high-risk individuals. PNR provides a unique feature of being able to make associations between passengers and identify criminals who belong in the same organised crime group. PNR is also successfully used for identifying trends of how criminals tend to behave when they travel for example by understanding which routes they use<sup>25</sup>.

In our view, however, this report by the relevant competent authorities largely serves to restate the aims and potential capacities of the PNR surveillance system. It singularly fails to refer to or provide

---

<sup>22</sup> At para. 9(c). Available at: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2010-0144+0+DOC+XML+V0//EN&language=EN>

<sup>23</sup> *supra* note 20, at para. 16

<sup>24</sup> *supra* note 21, at para.14

<sup>25</sup> Report on the joint review of the implementation of the 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) 8-9 February 2010 (at p. 4 & 9). Available at: [http://ec.europa.eu/justice\\_home/news/intro/news\\_intro\\_en.htm](http://ec.europa.eu/justice_home/news/intro/news_intro_en.htm)

any robust or convincing evidence to demonstrate the actual effectiveness of the scheme or otherwise confirm the necessity of added value of the use of PNR data in combating terrorism and/or serious transnational crime – that is, that the interference with fundamental rights facilitated by PNR data capture, storage and analysis is actually *necessary* to achieve the Agreement’s stated aims. Whilst the EC may themselves be ‘satisfied’ that the restrictions are necessary, in the absence of further supporting evidence we submit that this is in itself insufficient to meet the necessity requirements imposed by Article 8(2) of the European Convention.

(c) *Proportionality*

Proportionality is the key principle for determining the ‘fair balance’ between the protection of individual rights and the interest of the community at large. Whilst there are a number of key elements that comprise the proportionality test, in this part of our submission we focus on two: first, whether there is adequate procedural fairness and safeguards against abuse and second, whether less restrictive alternatives for interference with fundamental rights exist.

(i) Procedural fairness and safeguards against abuse

The presence of procedural safeguards against abuse are a key component of the proportionality principle. Thus, in *Klass v Germany* - a challenge brought against secret surveillance and interception undertaken by the German state authorities – the ECHR held that:

the values of a democratic society must be followed as faithfully as possible in the supervisory procedures if the bounds of necessity, within the meaning of Article 8 para. 2, are not to be exceeded. One of the fundamental principles of a democratic society is the rule of law, which ... implies, inter alia, that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and a proper procedure<sup>26</sup>.

The possible avenues of redress for persons seeking information about, or correction of, their PNR data held by DHS are outlined at Sections IV – IV of the current agreement. We have already introduced the nominal extension of US Privacy Act protections under the Agreement and explained how such protections have been effectively undermined through a subsequent process of unilateral amendment by the US authorities. Section IV of the DHS letter expressly states that “DHS has made a policy decision to extend administrative Privacy Act protections to PNR data stored in the ATS regardless of the nationality or country of residence of the data subject, including data that relates to European citizens”. However, as Papakonstantinou and de Hert<sup>27</sup> point out, the letter clearly refers to “administrative Privacy Act Protections”, not all protections. The consequences of this distinction in terms of effective remedies are crucial:

Referring to the “three-pillar federal privacy law system”, we note that the Privacy Act of 1974 altogether grants: (a) access rights to American citizens or lawful permanent residents, (b) amendment rights only to American citizens, (c) four separate and distinct civil causes of action in American courts, two of which are injunctive (amendment and access) and two of which provide for monetary damages only to American citizens and American permanent residents. Of those three elements, it is believed that only (a) and (b) constitute “administrative protections” and have thus been extended to European citizens. *Recourse to American courts according to the Privacy Act of 1974 appears not to be granted to European citizens in cases where they believe that DHS processing has breached their rights [our emphasis added]*<sup>28</sup>.

Thus despite the appearance of additional rights of redress being granted to European citizens by the DHS under the 2007 agreement, and the subsequent unilateral diminishment of those rights by the

---

<sup>26</sup> *Klass v Germany* (1979-80) 2 EHRR 214, at para. 55

<sup>27</sup> *supra* note 4 (at p.913)

<sup>28</sup> *Ibid*

DHS in the months immediately following the agreement provisionally entering into force, in practice no such safeguards appear to actually exist. It is within this context that the European Data Protection Supervisor concludes that whilst “redress possibilities are foreseen in the agreement, the exercise of rights by the individual in practice, and especially the right of access to personal data, remains a challenge”<sup>29</sup>. Whilst the 2010 joint EU-US review of the Agreement concludes that “DHS ... implements its commitments in relation to passenger rights [including] implementing the right to access and redress”, it does not provide any substantive detail as to how European data subjects have effectively exercised such rights (if at all), as well as confirming that the DHS was “unable to specify how many ... requests were related to EU-originating PNR data” and that they “[do] not track the number of [FOIA and Privacy Act] requests related specifically to PNR”<sup>30</sup>. Without *effective* rights of redress available for European Citizens in either US or European Courts, we submit that the current Agreement is also disproportionate for want of appropriate procedural safeguards in its interference with the right to respect for private life.

(ii) Less restrictive means

The basis for this element of the proportionality test is that an interference with a fundamental right will be *prima facie* disproportionate where a less restrictive effective alternative exists. In *Campbell v UK*<sup>31</sup>, for example, the ECHR held that a blanket indiscriminate policy of opening all prisoners mail was disproportionate because the less restrictive means of opening only those letters reasonably thought to contain prohibited material was sufficient.

Within this context, we note the existence of two other key EU PNR Agreements - the EU-Canada PNR Agreement<sup>32</sup> of 2005 and the EU-Australia PNR Agreement<sup>33</sup> of 2008. The key provisions of these agreements are considerably less draconian and severe in scope than the comparable 2007 agreement with the US. Under the terms of the Canadian Agreement, for example, PNR data is retained for a maximum of 3.5 years for persons who *are not* subject to investigation<sup>34</sup> and 6 years (inclusive) for persons who *are* subject to investigation<sup>35</sup>, after which time the data is destroyed. The Agreement itself, moreover, is underscored by “commitments”, rather than “assurances”, which do not state (like the comparable US Agreement) that they confer no legal rights<sup>36</sup>. Similarly, under the EU-Australia Agreement, the Australian authorities agree to keep EU-sourced PNR data for no more than three years, with retention allowed for up to 5.5 years for investigative purposes in certain circumscribed circumstances<sup>37</sup>. The increased levels of compliance with fundamental rights protection in these two agreements have led to bodies - such the UK’s House of Lords European Union Committee and the European Data Protection Supervisor - to favorably conclude that the Canadian Agreement should be considered as a starting point for any agreement with the US on PNR

---

<sup>29</sup> *Supra* note 20, at p.1

<sup>30</sup> *Supra* note 25, at pp. 28 - 29

<sup>31</sup> (1993) 15 EHRR 137

<sup>32</sup> Council Decision of 18 July 2005 on the conclusion of an Agreement between the European Community and the Government of Canada on the processing of API/PNR data. Available at:

[http://ec.europa.eu/justice\\_home/fsj/privacy/thridcountries/index\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm)

<sup>33</sup> Agreement between the European Union and Australia on the processing and transfer of European Union sourced passenger name record (PNR) data by air carriers to the Australian customs service; OJ L213 of 08/08/2008. Available at: [http://ec.europa.eu/justice\\_home/fsj/privacy/thridcountries/index\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm)

<sup>34</sup> Commission Decision of 6 September 2005 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the Canada Border Services Agency. (2006/253/EC) Annex, Para. 8(a). Available at: [http://ec.europa.eu/justice\\_home/fsj/privacy/thridcountries/index\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm)

<sup>35</sup> *Ibid*, (at para. 9).

<sup>36</sup> *Ibid*

<sup>37</sup> Agreement between the European Union and Australia on the processing and transfer of European Union-sourced passenger name record (PNR) data by air carriers to the Australian customs service. (OJ L213 of 08/08/2008). Annex, Para. 12. See also: Council Decision 2008/651/CFSP/JHA of 30 June 2008. Available at: [http://ec.europa.eu/justice\\_home/fsj/privacy/thridcountries/index\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm)

transfer. In the abovementioned Report, for example, the House of Lords analyse the relative differences between the amount of data captured under the Canadian and US agreements (as either proposed or in place at that time) and conclude that:

What seems clear to us is that, if a country like Canada which takes its national security no less seriously than the United States is satisfied with only 25 data items, the United States must be required to produce for each and every additional item that it requires detailed and particular justification for the inclusion of that item. That justification must be made available to those negotiating on behalf of the EU, and we expect them to take a robust attitude in the negotiations before being satisfied that any additional data item is essential and therefore permissible<sup>38</sup>.

[.....]

The PNR agreement between the EU and Canada strikes the right balance between safety, security and privacy. The agreement being negotiated with the US must do the same<sup>39</sup>.

Whilst this comparison was made at a time when the EU-US agreement in force at the time captured 34 (rather than the current 19 fields), we submit that the same method of comparison could readily be applied to the current disparity in retention periods, for example, between the Agreement under challenge in this case and the comparable Agreements with the Canada and Australia. No justification has been provided - either in the Agreement itself or in any of the publicly available supporting documentation – as to why a routine retention period of 15 years is necessary under the US scheme, yet a reduced maximum period applies in other comparable EU PNR schemes<sup>40</sup>.

We note that under the Proposal for a Council Framework Decision on the use of PNR data for law enforcement purposes PNR data is to be first filtered by Passenger Information Units (PIUs) before being provided to Member States or transferred to third countries. According to the Impact Assessment accompanying the proposal, this filtering aims at providing the EU with the ability “to insist on certain standards and to ensure consistency in such bilateral agreements with third countries”<sup>41</sup>. As a result of this filtering process, it is envisaged that only the selected data of suspected individuals (rather than the PNR data of all passengers) would be transferable to Member States and third countries. It is entirely unclear why a similar filtering system and selection process is not, or could not, be applied to the transfer of data to other authorities or third countries under the current EU-US PNR Agreement. Such a mechanism would clearly increase the possibilities for the Agreement to comply with data protection standards in respect to third country and inter-agency transfers – which were highlighted in the recent 2010 joint EU-US review of the current Agreement as raising specific concerns.

We therefore submit that less restrictive, yet equally effective, means *are* available and currently in use by the EU in comparable PNR surveillance schemes. The current agreement was not preceded by any form of Impact Assessment that sought to identify or limit the extent of interference with fundamental rights. According to the European Union Agency for Fundamental Rights, this deficit can largely be explained by the origins and imperatives of the PNR surveillance systems themselves – which have been driven by commercial considerations such as the minimisation of costs and administrative burdens for air carriers rather than a clear understanding of the types of data actually

---

<sup>38</sup> House of Lords European Union Committee (21st Report of Session 2006–07) The EU/US Passenger Name Record (PNR) Agreement (published 5 June 2007). Available at: <http://www.libertysecurity.org/article1489.html>

<sup>39</sup> House of Lords Press Release. (13 June 2007) Lords EU Committee raise concerns over Passenger Name Record Agreement with US. Available at: [www.statewatch.org/news/2007/jun/eu-pnr-hol-report-prel.pdf](http://www.statewatch.org/news/2007/jun/eu-pnr-hol-report-prel.pdf)

<sup>40</sup> We discuss the proportionality and excessive nature of the retention period itself in further detail below (at s.2, Right to data protection, pp. 13 - 14).

<sup>41</sup> Impact Assessment. Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes. Chapter 5.2 (at p. 22)

needed to combat terrorism and serious transnational crime<sup>42</sup>. Whatever the historical reasons are for this development, we submit that the existence of less restrictive alternatives (as outlined above) serve to render the current Agreement *prima facie* disproportionate.

## 2. Right to data protection

The preamble to the current EU-US PNR Agreement explicitly states that it should be read “with regard to Article 6 paragraph 2 of the Treaty on European Union on respect for fundamental rights, and in particular to the related right to the protection of personal data”. This right is clearly enshrined in Article 8 of the Charter which provides that:

Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

This fundamental right needs to be read in conjunction with the provisions of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereafter, the Data Protection Directive) and its associated jurisprudence. Under Article 6(1)(b) of the Directive – a provision known as the ‘purpose limitation’ restriction - personal data must be “collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. One key interrelated aspect of the purpose limitation principle is that data should not be retained any longer than is necessary for the specified purpose<sup>43</sup>. Additionally, Article 6(1)(c) introduces a proportionality principle which overlaps in practice with Article 8(2) of the European Convention and provides that personal data must be “adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed”. Article 8(1) of the Directive prohibits states from processing personal data revealing sensitive information such as racial, ethnic or religious background and/or health or sex life except where “such processing is necessary to protect the vital interests of the data subject” as provided under Article 8(2)(c). Article 25(1) of the Directive provides that states can only transfer personal data to third countries which have an adequate level of data protection in place (known as the ‘adequacy’ provision).

As it made clear in paragraph 11 of its preamble, the rights to privacy contained within the Data Protection Directive “give substance to and amplify those contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with Regard to Automatic Processing of Personal Data” (hereafter, ‘the 1981 Convention’). The key provisions of the 1981 Convention that are engaged in this case – including the Article 5 restrictions on the quality of automatic data processing, Article 6 prohibitions on the automated processing of sensitive data and the procedural safeguards contained within Article 8 - are already outlined at pp. 7 – 9 of the current Application for annulment filed with the Court on 1 March 2010 and are accordingly not repeated in this submission.

Whilst the right to data protection is separate and relatively autonomous from the right to private life, it nonetheless overlaps with and maintains a close connection to Article 8 as discussed above. In

---

<sup>42</sup> *supra* note 21, (at para. 19)

<sup>43</sup> Brouwer, E. (2009). “The EU Passenger name Record System and Human Rights: Transferring passenger data or passenger freedom?” Centre for European Policy Studies Working Document No. 320/September 2009. Available at: <http://ssrn.com/abstract=1513243> (at p.19)

*Osterreichischer Rundfunk* (C-465/00), for example, the ECJ held that where national courts held that legislation regarding the processing of personal data was incompatible with Article 8 then that legislation would also be “incapable of satisfying the requirement of proportionality in Articles 6(1)(c) and 7(c) or (e) of Directive 95/46”.

In addition to the points already raised in the Application for annulment (notably at pp. 20-30), we submit that there are three key areas where the current PNR Agreement breaches the individual right to data protection.

First, the scope of the Agreement itself is so excessively broad that it arguably goes beyond the strict purpose limitation restrictions contained in the Data Protection Directive. The Agreement is not limited to the strict purposes of fighting terrorism or serious transnational crime but also extends to include other possible purposes such as “the protection of the vital interest of ...[any] person” or “as otherwise required by law”<sup>44</sup>. It is a key tenet of the purpose limitation principle contained in Article 6(1)(b) of the Directive that data can only be collected and processed for a *specific* purpose<sup>45</sup>. In addition raising serious legal certainty issues, we submit that the scope of the current Agreement as outlined above is so excessively broad that it arguably breaches the specificity requirements contained in Article 6(1)(b) of the Directive<sup>46</sup>. Notwithstanding the excessively broad scope of the Agreement, we observe that in practice the US authorities are currently using PNR data in ways that exceed the purpose limitation. In the February 2010 joint review of the implementation of the Agreement, for example, the EU team raised strong objections to the ‘function creep’<sup>47</sup> associated with US use of European PNR personal information for immigration and border control purposes:

### 3.3 Areas to be particularly monitored/areas of strong recommendation

The EU team has identified some areas where particular monitoring would be required.

- There are some concerns as regards the broad use of PNR data and in particular the matching of PNR against databases that have immigration and customs policy elements to them. The EU team is aware of the fact that these purposes also come under the responsibilities of DHS. However, all processing of PNR by DHS needs to respect the purpose limitation of the agreement<sup>48</sup>.

This point about the illegitimate misuse of PNR data was then developed by the EU team in the following terms:

The processing done on the basis of scenario-based targeting rules is consistent with the main purposes of the agreement. However, as regards the matching of PNR against law enforcement databases, the EU team has some concerns. Namely, the matching of PNR against ESTA denial and prior refusal records and visa refusal databases seem to have some immigration purposes to them. Even though ESTA and visa denials could be based on counter-terrorism and transnational serious crime reasons, they are also done for purely immigration policy related purposes. Further, the matching of PNR against border

---

<sup>44</sup> 2007 EU – US PNR Agreement, DHS Letter, Section I.

<sup>45</sup> Working Party on the Protection of Individuals with regard to the Processing of Personal Data. *Working Document: Transfers of personal data to third countries – applying Articles 25 and 26 of the EU data protection directive* (DG XV D/5025/98, WP12) 24 July 1998 (at p. 6). Available at: [http://ec.europa.eu/justice\\_home/news/information\\_dossiers/personal\\_data\\_workshop/documents\\_en.htm](http://ec.europa.eu/justice_home/news/information_dossiers/personal_data_workshop/documents_en.htm)

<sup>46</sup> This conclusion was recently supported by the European Data Protection Supervisor. See *Comments of the EDPS on different international agreements, notably the EU-US and EU-AUS PNR agreements, the EU-US TFTP agreement and the need of a comprehensive approach to international data exchange agreements*. 25.01.10 (at p.1). Available at: [www.edps.europa.eu/EDPSWEB/.../Comments/.../10-01-25\\_EU\\_US\\_data\\_exchange\\_EN.pdf](http://www.edps.europa.eu/EDPSWEB/.../Comments/.../10-01-25_EU_US_data_exchange_EN.pdf)

<sup>47</sup> ‘Function Creep’ refers to “the way in which information that has been collected for one limited purpose, is gradually allowed to be used for other purposes which people may not approve of” (Definition from [http://www.oup.com/elt/catalogue/teachersites/oald7/wotm/wotm\\_archive/function\\_creep?cc=global](http://www.oup.com/elt/catalogue/teachersites/oald7/wotm/wotm_archive/function_creep?cc=global))

<sup>48</sup> *supra* note 25 (at p. 11).

crossing information seems to be primarily focused on identifying visa overstayers. The EU team considers that this purpose was not intended to be covered by the agreement since it is an immigration based criminal offence which very possibly does not have a transnational element to it, since the overstaying takes place in the U.S. It is strongly recommended that DHS review these practices and use PNR data only for the purposes defined in the agreement. In this context also the notion of crimes that are transnational in nature should be revised. Not every criminal crossing the US border has committed a serious transnational crime<sup>49</sup>.

The EU team raised additional concerns about the US use of European PNR data in two further border control programs - the Immigration Advisory Program and the Regional Carrier Liaison Group. However, because DHS explicitly failed to provide them with sufficient information about these programs, the EU team were “[un]able to draw conclusions on the compliance of this program with the agreement” but made a strong recommendation that they be assessed as soon as possible “as regards the purpose limitation of the agreement and data protection”<sup>50</sup>.

In response to the serious concerns of the EU team, the DHS simply noted that “there are several references in the draft report that suggest DHS may be using EU PNR for purposes unrelated to serious transnational crime” but they considered that “this finding is premised on differing views between DHS and the EC review team on ... what constitutes a serious transnational crime; and ... what is considered a decision based on PNR”<sup>51</sup>. As a result, DHS stated that their belief that “all of its uses comply with the terms of the 2007 agreement” and that they were “happy to discuss differences in the two aforementioned items with the EC”<sup>52</sup>. Furthermore, DHS confirmed that the Immigration Advisory Program and the Regional Carrier Liaison Group *did* use PNR for border control purposes, simply stating that “PNR is not used as the sole basis to recommend to a carrier that a passenger not be boarded” as a mitigating factor. As such, DHS concluded that: “the use of PNR in this regard [is] consistent with the terms of the Agreement. However, we believe that the IAP and RCLG program fall outside the scope of the Agreement and respectfully request that conclusions and recommendations concerning the IAP and RCLG and the Agreement be provided since these issues were not discussed in detail during the joint review”<sup>53</sup>.

Thus, despite the clear evidence that the DHS are using European PNR data for border control reasons outside the scope of the purpose limitation of the Agreement and strong EU recommendations to urgently remedy the situation, US authorities are defiant in their response - by both refusing to acknowledge their breach and calling for the formal EU recommendations made on this issue to be withdrawn. From a data protection perspective, which adopts the fundamental rights of the individual as its starting point of analysis, this position is clearly unacceptable. It indicates that individual rights to data protection are being breached, contrary to Article 6(1)(b) of the Data Protection Directive, without the possibility of effective redress. DHS’s ‘happiness’ to informally discuss the issue with the EC within this context is patently insufficient.

Second, the duration of data retention facilitated under the Agreement is unduly excessive and potentially indefinite, thus further breaching the purpose limitation provisions of the Data Protection Directive. As we have stated earlier, the current agreement allows the personal data of European citizens to be retained in DHS (and other) databases for at least 15 years – eight years immediately accessible, followed by 7 years accessible in ‘dormant’ status – notwithstanding that the earlier EU-US PNR agreements had allowed a nominal retention period of 3.5 years. According to the European

---

<sup>49</sup> Ibid (at p. 16)

<sup>50</sup> Ibid (at p.16)

<sup>51</sup> Letter from DHS to European Commission (31 March 2010). *DHS response to the European Commission’s Report on the Joint Review of the US – EU Passenger Name Record Agreement* (at p.5). Available at: [http://ec.europa.eu/justice\\_home/news/intro/news\\_intro\\_en.htm](http://ec.europa.eu/justice_home/news/intro/news_intro_en.htm)

<sup>52</sup> Ibid (at p.5)

<sup>53</sup> Ibid (at p. 3)

Data Protection Supervisor, this retention period is “excessive”<sup>54</sup> and “without legal precedent” – indeed, the “extension of time that passenger data [is] kept – effectively from 3.5 to 15 years in all cases” is identified by the EDPS one of the key “grave areas of concern” of the Agreement<sup>55</sup>. The previous European starting point on this matter had been that:

Data must be retained for the period of time that is necessary for the purposes for which the data are collected. If, for example, identification of travellers posing a threat is the purpose, there would not be sufficient ground for retaining the data for longer than the retention period established under Directive 2004/82/EC. That Directive states that data should be deleted 24 hours after arrival. The retention of personal data of unsuspected individuals for possible future use for the given purposes has a substantial impact on human rights and would therefore need strong justification<sup>56</sup>.

Given the strict provisions of Directive 2004/82/EC and the prevailing view (as expressed by the Article 29 Working Party above) that retention of data of unsuspected individuals would require “strong justification”, the original 3.5 year retention period established under the earlier PNR agreements had been deemed excessive and a concession to the Americans during the negotiating process<sup>57</sup>. That this was then extended to a minimum 15 year period in all cases without the provision of “strong justification” or robust evidence as to necessity is both troubling and without legal foundation.

In any event, we note that the DHS do not even guarantee to destroy European PNR data after the specified 15 year period. Instead, the DHS letter simply states that “we *expect* that EU PNR data shall be deleted at the end of this [15 year] period; questions of whether and when to destroy PNR data collected in accordance with this letter will be addressed by DHS and the EU as part of future discussions”<sup>58</sup>. Furthermore, this nominal ‘commitment’ – which, in reality, lacks any binding effect or substance – would only apply to the PNR that is held in DHS’s own databases. Nowhere under the current EU-US PNR Agreement or its supporting documentation does DHS undertake to monitor and/or ensure deletion from other domestic databases to which it has already transferred PNR data during the initial 15 year period<sup>59</sup>. Indefinite retention of personal data is, we submit, clearly incompatible with the core purpose limitation principle contained in Article 6 of the Directive that personal data must not be retained any longer than is necessary for a specified purpose.

Finally, the *indiscriminate* nature of the PNR data collection and analysis arguably renders the Agreement illegitimate when measured against appropriate data protection standards including Article 6(1)(c) of the Data Protection Directive. Under the current Agreement the collection and analysis of data is not focused on individuals that present a risk. Instead, the Agreement facilitates the widespread and indiscriminate collection of personal data of innocent people - followed by the subsequent analysis, cross-matching, profiling and risk assessment of that data - in assist the targeting of individuals by law enforcement authorities. We concur with the view of the EDPS that “such a wide scale collection, analysis and storage of personal data could raise legitimacy and

---

<sup>54</sup> *supra* note 46 (at p.1)

<sup>55</sup> Letter from Peter Hustinx (EDPS) to Dr Wolfgang Schauble (Minister for the Interior) *New PNR Agreement with the United States of America*. 27 June 2007 (at p.1). Available at: [www.statewatch.org/news/2007/jun/eu-us-pnr-hustinx-letter.pdf](http://www.statewatch.org/news/2007/jun/eu-us-pnr-hustinx-letter.pdf)

<sup>56</sup> Article 29 Working Party. (2007). Common EU approach to the use of Passenger Name Record (PNR) data for law enforcement purposes. (at p.8). Available at: [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/others/2007\\_31\\_01\\_common\\_eu\\_approach\\_use\\_pnr\\_data\\_for\\_law\\_enforcement.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/others/2007_31_01_common_eu_approach_use_pnr_data_for_law_enforcement.pdf)

<sup>57</sup> *supra* note 4 (at 915)

<sup>58</sup> 2007 EU – US PNR Agreement, DHS Letter, Section VII.

<sup>59</sup> *supra* note 4 (at p.912)

proportionality issues in relation to the jurisprudence of the European Court of Human Rights<sup>60</sup>. In the recent decision of *S. & Marper v the United Kingdom*<sup>61</sup>, for example, the ECHR ruled that the indefinite retention of DNA the samples and profiles of those suspected (but not convicted) of committing an offence was disproportionate and in breach of Article 8 of the European Convention. In arriving at this conclusion, the Court declared that they were 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”<sup>62</sup>. Similarly, we submit that in this case the indiscriminate and potentially indefinite retention of the PNR data of innocent individuals facilitated by the 2007 Agreement is in breach of the proportionality principle contained within Article 6(1)(c) of the Directive and accordingly unlawful.

### 3. Right to non-discrimination

Article 14 of the European Convention provides that:

The Enjoyment of rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.

Similarly, Article 21 of the Charter of Fundamental Rights provides that:

Non-discrimination

1. Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited.

2. Within the scope of application of the Treaty establishing the European Community and of the Treaty on European Union, and without prejudice to the special provisions of those Treaties, any discrimination on grounds of nationality shall be prohibited.

Other international agreements – such as the UN Convention on the Elimination of all forms of Racial Discrimination<sup>63</sup> (hereafter, the UN Convention) – apply similar anti-discrimination provisions to state authorities (such as Belgium) who have ratified the convention. Significantly, Article 2(1)(a) of the UN Convention imposes a positive obligation upon states to amend, rescind or nullify any laws and regulations that have the effect of creating or perpetuating racial discrimination wherever it exists. Further to this provision, therefore, differential treatment by law enforcement authorities on the basis of ethnicity or national origin cannot be justified<sup>64</sup>.

When measured against this legal backdrop, we submit the 2007 PNR agreement raises considerable concerns. As we have already discussed, data profiling surveillance operates not only by identifying ‘known’ individuals who may be suspected committing an offence, but also by creating new, secondary information about individuals and proactively generating links between ‘known’ and ‘unknown’ individuals in order to *predict* those who may be involved in some future crime. We have

---

<sup>60</sup> *supra* note 46 (at p.2)

<sup>61</sup> 4 December 2008. Nos. 30562/04 and 30566/04

<sup>62</sup> *Ibid* (at para. 119 – 122)

<sup>63</sup> Adopted by the UN General Assembly Resolution 2106, 21 December 1965, entered into force 4 January 1969, ratified by Belgium on 7 August 1975.

<sup>64</sup> See, *inter alia*, *Timishev v Russia* (13 December 2005) Nos. 43577/98 and 55974/00 and *D.H v Czech Republic* (13 November 2007) ECHR 2008/5 on breaches of Article 14 of the European Convention. See also *R (European Roma Rights Centre) v Immigration Officer at Prague Airport* [2004] UKHL 55 on breaches of the UN Convention.

also noted that data profiling operates by mixing both *concrete* and *abstract* information (including patterns and profiles) to generate risk assessments and target individuals for increased surveillance and enforcement action and that the criteria used by states agencies (such as DHS and the other agencies with which they share European PNR data) to generate such patterns, profiles and risk assessments have not been publicly disclosed. Crucially, if law enforcement authorities build profiles upon untested generalisations or stereotypical assumptions that persons of a certain race, national or ethnic origin, religion, intellectual disabilities or mental illness are particularly likely to commit an offence, then such practices (and the enforcement action which follows) will arguably breach individuals rights to freedom from discrimination<sup>65</sup>.

As it stands, section III of the 2007 Agreement ostensibly seeks to limit DHS's use of "sensitive" data (that is, personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and data concerning the health or sex life of the individual) through the use of an automated filtering system which sifts the information out unless it needs to be accessed in an "exceptional case". In addition to our earlier comments about the lack of clear guidelines governing the exercise of executive discretion and the clear possibilities for abuse in this area, we make three further observations. First, even if "sensitive data" is automatically filtered out in the first instance, data profiles based on religious or ethnic background or health status can still be readily be constructed and deployed by state authorities on basis of 'ordinary' PNR data such as dietary requirements, use of medicines and/or passenger name<sup>66</sup>. The "OSI, SSI and SSR information" referred to in data field 17, Section III of the DHS Letter, for example, includes passenger details such as special meal requests which can readily be used to infer the religious background of passengers without recourse to the "exceptionality" provisions. Similar profiles can also be generated on the basis of an individual's name alone, when filtered using an appropriate profiling process. When properly correlated, 'ordinary' data can easily reveal sensitive information. Thus, according to Papkonstantinou and de Hert:

DHS could support that all these data, because they are not "included in the above types of EU PNR data" but they are rather inferred by its own software, do not formally fall under the sensitive data provisions of the Second PNR Agreement (or, rather, the DHS Letter) and thus do not benefit from the "exceptional case" filter; *ultimately, sensitive personal data of European citizens will be free for processing by the DHS*<sup>67</sup> [our emphasis added].

Second, unlike the draft Proposal for a European Council Framework Decision on the use of PNR data<sup>68</sup>, there are no explicit provisions within the current EU-US Agreement to prevent law enforcement action being taken against individuals solely on the basis of automated processing of PNR data or ultimately by reason of a person's racial, ethnic or religious background, political opinion or sexual orientation. As such, we assume that such processing is implicitly permitted under the current Agreement, thus clearly increasing the scope for discriminatory treatment on the basis of profiling built on stereotypical generalisations that certain ethnic or religious groups pose a greater terrorist risk than others.

The dangers and discriminatory effects of such automated, racial profiling were made readily apparent in recent decision of the *Bundesverfassungsgericht* (the German Constitutional Court) on the practice of 'Rasterfahndung' or data profiling undertaken by the German police to identify terrorist suspects<sup>69</sup>. In the immediate aftermath of the September 11 attacks in the USA, German federal police began a coordinated national dragnet investigation to identify potential Islamic terrorists using the following criteria: "Male, aged 18 – 40, (ex-) student, Islamic religious affiliation,

---

<sup>65</sup> *supra* note 21 (at para. 36)

<sup>66</sup> *supra* note 43 (at p. 23)

<sup>67</sup> *supra* note 4 (at p.915)

<sup>68</sup> See Recital 20 and Article 3.3 and 3.5 of the proposal

<sup>69</sup> BVerfG, 1 BvR 518/02, 4 April 2006, (hereafter, the *Muslim Sleeper* case).

native country or nationality of certain countries, named in detail, with predominantly Islamic population”<sup>70</sup>. This involved the collection of data from educational institutions, registry offices and the central register for immigrants which was then forwarded to the Federal Criminal Police Office who set up a national ‘Muslim sleeper’ file consisting of approximately 8 million pieces of information on up to 300,000 individuals. A final database of potential sleeper cell members was compiled containing almost 32,000 entries<sup>71</sup>. This figure was finally narrowed down in a final database. A legal challenge was brought by a Moroccan Muslim studying at the University of Duisburg who had been targeted by the surveillance, on the basis that the measures constituted an unlawful interference with his right to privacy and informational self-determination as reflected in Article 2(1) of the German Constitution. Significantly, the Court held that interference with this right could only be proportionate if certain conditions were met – namely, that there was a *concrete* danger to the survival or security of the state or to the person, or a sufficient probability that such a danger was imminent<sup>72</sup>. Thus, a “vague indication and mere assumption without any tangible evidence in the individual case is not sufficient”<sup>73</sup> and, as such, the general state of threat which had arisen after 11 September 2001 was insufficient to justify the data profiling and mining in question. Accordingly, the Court found that the transfer, storage and comparison of the data were specific violations and disproportionate interferences with the right to privacy. Crucially, the Court held that *additional comparison and analysis* of the data through profiling and data mining processes intensified the nature of the interference with fundamental rights and increased the possibility that certain groups could be stigmatised and disproportionately affected by such measures on the basis of their religious and ethnic background:

For those persons whose constitutional rights it affects, data profiling means a higher risk of becoming the target of further official investigative measures. This has been demonstrated to a certain extent by the outcome of the data profiling implemented since 11 September 2001. (...) Furthermore, the very fact of police data profiling having been carried out according to certain criteria – if it becomes known – can have a stigmatising effect on those who meet these criteria. (...) It is relevant, with regard to the intensity of the effects of the data profiling carried out since 11 September 2001, that it is targeted at foreigners of certain origins and Muslim beliefs, which always involves the risk of spreading prejudice and stigmatising these population groups in the public perception<sup>74</sup>.

Whilst the *Rasterfahndung* decision of the Bundesverfassungsgericht is not directly applicable in the instant case, we submit it is nonetheless of clear relevance because it is the only case (so far as we are aware) where the lawfulness of data profiling has been explicitly considered against the fundamental right to privacy by a European constitutional court. Significantly, the decision suggests that personal data which is acceptable for state authorities to collect in one way can readily become unacceptable (and unlawful) for recording and analysis in another, once factors such as the capacity for cross-referencing and aggregating the data to build data profiles for targeting individuals of specific groups is taken into account<sup>75</sup>. That is, the subsequent process of filtering, analysis and profiling of personal data constitutes a separate, relatively distinct and particularly severe form of interference with the right to private life that disproportionately affects individuals of certain ethnic,

---

<sup>70</sup> For a detailed description of the criteria, see *Bundesverfassungsgericht* 59 NEUE JURISTISCHE WOCHENSCHRIFT (NJW) 1939 (2006) [in German]

<sup>71</sup> Open Society Institute (May 2009) *Ethnic Profiling in the European Union: Pervasive, Ineffective and Discriminatory* (at p. 69). Available at: [http://www.soros.org/initiatives/justice/focus/equality\\_citizenship/articles\\_publications/publications/profiling\\_20090526](http://www.soros.org/initiatives/justice/focus/equality_citizenship/articles_publications/publications/profiling_20090526)

<sup>72</sup> *supra* note 69 (at para. 125)

<sup>73</sup> *supra* note 69, (at para. 145)

<sup>74</sup> *supra* note 69 (at paras. 110 – 112)

<sup>75</sup> Youngs, R. (2008) “Germany: shooting down aircraft and analyzing computer data” in *International Journal of Constitutional Law* 6(2): 331 – 348 (at p. 344).

national or religious groups and therefore requires its own justification. Absent such a justification, such interference should be considered unlawful.

It is clear that one of the primary rationales for the current EU-US PNR Agreement is to facilitate proactive data profiling of potential suspects. Such profiling takes place against undisclosed criteria for a period of up to 15 years, without sufficient guidelines regulating executive discretion and with a minimum amount of obstacles to prevent state agencies from effectively generating profiles and targeting individuals on the basis of sensitive criteria such as their ethnic or religious background. As such, we submit that the Agreement facilitates, rather than safeguards against, the risk of racial or ethnic profiling - a practice which the European Union Agency for Fundamental Rights has concluded constitutes unlawful discrimination and should therefore be explicitly banned<sup>76</sup> - and therefore could readily breach the provisions of Article 21 of the Charter. Furthermore, in facilitating such discriminatory activity, the Agreement also arguably engages<sup>77</sup> and breaches Article 14 of the European Convention - which permits differential treatment on the basis of nationality or ethnicity in certain circumstances, but only when "a reasonable and objective justification"<sup>78</sup> and "very weighty reasons"<sup>79</sup> are demonstrated, neither of which have been provided for under this Agreement.

## Conclusion

For the reasons outlined above, and in addition to the grounds pleaded in the application for annulment filed the Court on 1 March 2010 and published in the official journal on 21 April 2010, we contend that the 2007 EU-US PNR Agreement is in breach of three core fundamental rights – namely, the right to respect for private life (as protected by Article 8 of the European Convention and Article 7 of the Charter); the right to data protection (as protected by Article 8 of the Charter, read in conjunction with Directive 95/46/EC and the 1981 Strasbourg Convention) and the right to freedom from discrimination (pursuant to Article 21 of the Charter and Article 14 of the European Convention). Consequently, we submit that the law of 30 November 2009 that seeks to implement this Agreement ought to be annulled due to its incompatibility with fundamental rights.

We ask the Court to both join ECCHR as a party to these proceedings and accept our submissions in support of annulment. Furthermore, we enclose the relevant statutes of our organisation and a short letter from ECCHR's General-Secretary confirming our intention and capacity to join the current proceedings as Annex A. We are grateful for the opportunity of being able to provide our submissions in this case and, if it would assist the Court, we would welcome the opportunity to provide more detailed submissions on this matter in the future.

**European Center for Constitutional and Human Rights (ECCHR)**<sup>80</sup>

17 May 2010

Enc.

---

<sup>76</sup> *supra* note 21 (at para. 43)

<sup>77</sup> Whilst Article 14 of the European Convention is not free-standing, it is clearly engaged when facts "fall within the ambit" of one of the Convention rights set out in Articles 2 – 12 in this case, Article 8. See, for example, *Rasmussen v Denmark* (1985) 7 EHRR 371

<sup>78</sup> *Belgian Linguistics case* (1979-80) 1 EHRR 241

<sup>79</sup> *Schmidt v Germany* (1994) 18 EHRR 513

<sup>80</sup> This submission was prepared for ECCHR by Wolfgang Kaleck and Gavin Sullivan, with assistance from Dr Ben Hayes, Dan Squires (Matrix Chambers, London), Yveline Ruaud and Nicola Iburg.