

ECCHR Third-Party Submission to the Belgian Constitutional Court

- Summary -

The European Center for Constitutional and Human Rights (ECCHR) last week filed third-party submissions in a Belgian Constitutional Court challenge against the EU-USA Passenger Name Record (PNR) Agreement and mass surveillance system.

Background

In July 2007 the EU signed an Agreement with the US Department of Homeland Security to facilitate US access to European PNR data for the purposes of combating terrorism and serious transnational crime. The Agreement - which has been widely criticized by bodies such as the European Parliament, the European Data Protection Supervisor, the European Agency for Fundamental Rights as well as civil liberties, privacy and anti-racist activists – allows US law enforcement authorities to collect and store European personal data for at least 15 years, subjecting all passengers to potentially far-reaching surveillance irrespective of whether they are suspected of having committed any offence. Controversially, the Agreement enables US authorities to engage in *data profiling*, linking innocent passengers to ‘suspicious’ passengers based on factors such as travel patterns, credit card use and (potentially) religious or ethnic background.

On 1 March 2010 the Belgian branch of the *Ligue des Droits de L’Homme* (the Human Rights league) filed a legal challenge in Belgium’s constitutional court against the domestic legislation of 30 November 2009 implementing the EU-USA PNR agreement. On 21 May ECCHR filed a third party submission in support of this application and requesting to be joined as a party to the proceedings – available on the homepage.

Legal Submission

ECCHR’s submission argues that the PNR Agreement breaches three key fundamental rights - including the *right to respect for private life* (pursuant to Article 8 of the European Convention of Human Rights and Article 7 of the Charter of Fundamental Rights of the European Union), the *right to data protection* pursuant to Article 8 of the Charter, read in conjunction with the Data Protection Directive 95/46/EC and the *right to freedom from discrimination* (pursuant to Article 21 of the Charter and Article 14 of the European Convention). The key arguments of ECCHR’s submission include:

- The Agreement lacks adequate enforcement mechanisms by which citizens can enforce their rights in the event of a breach, in contravention of the *legality principle* required by Article 8 of the European Convention.

- The Agreement interferes with fundamental rights in ways that lack the requisite degree of *legal certainty* required under Article 8. There is insufficient certainty over the discretion enjoyed by state authorities to access ‘sensitive data’ revealing racial, religious, political or sexual information about individuals. Furthermore, because the Agreement fails to disclose how data profiling actually works, it is impossible for an individual to know what use can be made of their personal data.
- The Agreement *disproportionately* interferes with individuals’ Article 8 rights. It has not been demonstrated that the mass surveillance facilitated by the Agreement is actually an effective (and therefore, necessary) means of combating terrorism. There are less restrictive alternatives available - for example, the similar EU PNR Agreements with Australia and Canada have comparable aims yet retain passenger data for significantly shorter periods. Furthermore, the current Agreement lacks appropriate procedural safeguards and avenues for redress. The protection nominally afforded under the US Privacy Act 1974 does not actually extend in practice to Europeans wishing to enforce their individual rights against US authorities.
- The PNR surveillance system is already being used by the US authorities for purposes that go *beyond the scope* of the Agreement in breach of Article 6(1) (b) of the Data Protection Directive. Recent reviews of the system by the EU, for example, clearly show that PNR personal data is being misused by US authorities for immigration and border control purposes rather than for combating terrorism or serious transnational crime.
- The Agreement allows US authorities to retain personal data for an excessive, and potentially indefinite, period. Previous PNR agreements kept the data for 3.5 years. Under the current agreement, data is kept for at least 15 years in all cases. Furthermore, no commitment is made by the US to actually destroy the data after that 15 year period nor to ensure the destruction of data by the other agencies that the DHS share PNR information with. This is clearly incompatible with Article 6 of the Data Protection Directive which requires that *personal data must not be kept any longer than is necessary* for a specified purpose.
- The current PNR Agreement allows for the widespread collection and storage of personal data of innocent people by law enforcement authorities. This data is then further subjected to subsequent analysis, cross-matching, modeling against unknown criteria over a potentially indefinite period to build ‘high risk’ or ‘suspect’ profiles. The *indiscriminate* nature of this mass surveillance system breaches the proportionality requirements of Article 6(1)(c) of the Data Protection Directive.

- Despite the use of automatic filtering, the Agreement still allows US authorities to access sensitive data (both in ‘exceptional cases’ and through analyzing, for example, ordinary PNR information concerning dietary/medical requirements and/or passenger name) that enable the construction of data profiles based on untested generalizations or stereotypical assumptions that persons of a certain race, ethnic origin or religious background are particularly likely to engage in terrorist offences. The Agreement facilitates and fails to adequately safeguard against the discriminatory effects of racial or ethnic profiling, potentially *breaching anti-discrimination provisions* contained in Article 21 of the Charter and Article 14 of the European Convention as a consequence.

Conclusion and next steps

The ECCHR is currently awaiting the Court’s decision on our application in this important matter. We anticipate being able to provide more detailed submissions on these issues before a hearing date is set by the Court for later in 2010.