



Hellenic Data Protection Authority
Kifisias Av. 1-3, PC 11523
Ampelokipi Athens, Greece

Tuesday, January 9, 2007

Privacy International
6-8 Amwell Street
London
EC1R 1UQ
GB

Dear Commissioner,

RE: EU-US PNR agreement in light of 'Automated Targeting System'

ACLU
125 Broad Street,
New York, NY 10004
USA

We are writing to you on behalf of Privacy International and the American Civil Liberties Union to raise concerns about recent disclosures by the United States Department of Homeland Security regarding the 'Automated Targeting System' relating to passenger entry into the US.¹ We believe that this system violates the EU-US agreement on transfers of personal data, and in turn, breaches both American law and the EU Directive 1995 on Data Protection. In particular, the system breaches the EU Directive by using 'passenger name record' (PNR) data from EU carriers and reservations systems,² consisting of personal information on both European and foreign nationals, including American citizens, for the purpose of generating a risk assessment score. In addition, it violates a specific Congressional prohibition on the use of U.S. funds to develop or test risk-assessment and profiling systems on passengers.³

According to the U.S. Department of Homeland Security (DHS) and in particular Customs and Border Protection (CBP) branch, the ATS is part and parcel of a larger system called the Treasury Enforcement Communications System. Originally used for tracking cargo, this system is now designated as the "cornerstone for all CBP targeting efforts."⁴ It combines data from CBP mainframe systems with PNR received from foreign carriers,⁵ along with data from foreign governments 'and certain express consignment services in conjunction with specific cooperative programs'.⁶ ATS then generates a risk assessment score for all passengers:

"ATS provides equitable treatment for all individuals in developing any individual's risk assessment score, because ATS uses the same risk assessment process for any individual using a defined targeting methodology for a given time period at any specific port of entry."⁷

¹ DHS, Office of the Secretary, Privacy Act of 1974; System of Records - Notice of Privacy Act system of records, November 2, 2006, Volume 71, Number 212. Hereafter 'DHS ATS Register Statement'.

² This data is 'pushed' by carriers to the U.S. Government, but it may also be 'pulled', where the U.S. authorities log into the reservation databases to gain access to the information they are seeking.

³ For example, the Department of Homeland Security Appropriations Act, 2007, P.L. 109-295 (H.R. 5441), provides in Title V, Sec. 514 (e), "None of the funds provided in this or previous appropriations Acts may be utilized to develop or test algorithms assigning risk to passengers whose names are not on Government watch lists."

⁴ DHS, Privacy Impact Assessment of the Automated Targeting System, November 22, 2006. Hereafter 'PIA'.

⁵ According to the Privacy Act notice, the full PNR is used in the ATS-P system.

⁶ DHS PIA.

⁷ DHS PIA.

The score and the PNR are kept for 40 years.⁸

The scheme directly contravenes the EU-US agreement on the transfer of passenger data.

1. The DHS has exempted ATS from the 1974 Privacy Act by preventing individuals from exercising any right of access to this profile and any right to modify or correct information. According to the Privacy Impact Assessment published by DHS, "There is no procedure to correct the risk assessment and associated rules stored in ATS."⁹ This directly contravenes the EU-US agreement, which specified a number of actionable rights for Europeans to appeal against the mis-use and abuse of their personal data.
2. CBP and DHS may use this profile for any number of purposes. According to the DHS, the driving purpose behind ATS is "to perform targeting of individuals, including passengers and crew, focusing CBP resources by identifying persons who may pose a risk to border security, may be a terrorist or suspected terrorist, or may otherwise be engaged in activity in violation of U.S. law." It may also be used "to assist in the enforcement of the laws enforced or administered by DHS, including those related to counterterrorism."¹⁰ This directly contravenes the EU-US agreement, which limited the use of PNR to combating terrorism and serious trans-national crime.
3. This data, which includes information on tens of millions of people, is kept for 40 years. This directly contravenes the EU-US agreement, which requires the data to be deleted after a three-year period.

Privacy International
6-8 Amwell Street
London
EC1R 1UQ
GB

ACLU
125 Broad Street,
New York, NY 10004
USA

Most importantly, it appears that ATS was kept more or less a secret until recently. Until the November 2006 statement that publicly acknowledged its existence, reviews of ATS by the Department of Homeland Security Inspector General and the Government Accountability Office did not identify the processing of personal data through data-mining. The joint EU-US review in 2005 never identified this additional processing and thus enthusiastically supported the treatment of the data by U.S. authorities. And throughout the re-negotiation of the agreement in the summer of 2006, ATS was never mentioned.

During the drafting of the original agreement a great amount of concern was expressed regarding the use of PNR for the purpose of profiling and data mining. According to the Article 29 Working Party, passenger risk-assessment systems, such as the now-defunct Computer Assisted Passenger Pre-Screening System (CAPPS II), should never be applied:

"In fact, these [risk-assessment] systems are qualitatively different from the mere transfer of passenger PNR data and involve wide-ranging issues which should be clarified and specifically addressed by the Working Party, in consideration of the more pervasive effects that would affect the fundamental rights of the data subjects concerned. In particular, the CAPPS II system raises a number of peculiar issues that require not only specific consideration by the Working Party, but also different, higher safeguards."¹¹

Instead of gaining stronger safeguards, Europe now faces a situation where the EU-US agreement on PNR has been fundamentally undermined by this additional processing by the Department of Homeland Security.

⁸ DHS ATS Register Statement.

⁹ DHS PIA.

¹⁰ DHS ATS Register Statement.

¹¹ Article 29 Working Party, Opinion 2/2004 on the Adequate Protection of Personal Data Contained in the PNR of Air Passengers to Be Transferred to the United States' Bureau of Customs and Border Protection (US CBP), adopted on 29 January 2004.

In addition, these actions of the U.S. government violate both EU and a number of national laws. Privacy International notes that ATS likely violates national privacy and data protection laws, particularly if national carriers are submitting data to the U.S. authorities. The ACLU also notes that the U.S. Congress specifically prohibited the Department of Homeland Security from engaging in this sort of airline passenger profiling.¹²

The ATS is a clear threat to privacy and human rights. We would like to remind you that the TEC system of which ATS is a key component of, was the system that flagged Maher Arar, a Canadian citizen, and led to his rendition to Syria, as was recently uncovered by the Canadian inquest into his case.¹³ Without adequate safeguards and review these systems are prone to error and abuse.

Privacy International
6-8 Amwell Street
London
EC1R 1UQ
GB

ACLU
125 Broad Street,
New York, NY 10004
USA

We call on your office to:

- Work with the Article 29 Working Party to conduct a full and open review of the PNR agreement.
- Conduct an investigation into the status of the data transferred on both your nationals and foreign nationals, including American citizens, data sent from your jurisdiction that are now residing under the jurisdiction of the CBP.
- Conduct an inquiry into why both the joint EU-US review never voiced any concern over the status of ATS and how the EU review team was able to conclude: "The EU team also found that at some instances CBP went significantly beyond, or intends to go beyond, what is necessary in order to comply with the Undertakings. CBP namely installed technology that will track disclosure of PNR data and monitor manual access to such data."¹⁴

We are surprised that the promised safeguards of open review and actionable rights are being undermined with great ease through secret systems and inadequate reviews.

We look forward to hearing your responses on these matters.

Yours sincerely,

Simon Davies
Director
Privacy International

Barry Steinhardt
Director
Technology and Liberty Project
American Civil Liberties Union

¹² For example, see The Department of Homeland Security Appropriations Act, 2007, P.L. 109-295 (H.R. 5441), Title V, Sec. 514 (e).

¹³ See 'Report of the Events relating to Maher Arar', Commission of Inquiry into the Actions of Canadian officials in Relation to Maher Arar, Factual Background, Volume I, September 2006, pages 57, 61-65, 114-115, available at <http://www.ararcommission.ca/>.

¹⁴ Commission Staff Working Paper on the Joint Review of the implementation by the U.S. Bureau of Customs and Border protection of the Undertakings set out in Commission Decision 2004/535/EC of 14 May 2004, Redacted version, Washington 20-21 September 2005, Brussels, December 12, 2005.