Written Testimony of Edward Hasbrouck
before the LIBE Committee of the European Parliament and the
Article 29 Working Party

TRANSFERS OF PNR DATA FROM THE E.U. TO THE U.S.

Public debate about Passenger Name Record (PNR) data, as well as the work of the LIBE Committee, the European Parliament, and the Article 29 Working Party, have all focused on PNR data collected by and in the possession of airlines, and the transfer of that data directly from data controllers in the European Union to the government of the United States. This is the subject of the previously annulled "agreement" and finding of "adequacy" of protection for PNR data transferred to the U.S. government, as well as the current interim agreement and the new agreement being negotiated between the E.U. and the U.S.

But the problems of misuse of PNR data, violations of human rights and civil liberties, and interference with the free movement of persons are much more extensive than has generally been realized.

PNR data has been, and could be, transferred to the U.S. government, and used in ways that violate fundamental principles of human rights and civil liberties, through commercial intermediaries and through legal and operational mechanisms that bypass the E.U./U.S. PNR agreement.

Here are some of the problems related to PNR data that cannot be addressed within the current proposals for a new E.U./U.S. agreement, and that call for additional action by the LIBE Committee, the European Parliament, the Article 29 Working Group, and the European commission:

1. COMMERCIAL TRANSFERS OF TRAVEL DATA TO THE U.S. IN VIOLATION OF THE DATA PROTECTION DIRECTIVE AND THE CODE OF CONDUCT FOR CRS'S

In most cases, PNR data are collected, stored, and transferred to U.S. territory by commercial intermediaries, not directly by airlines. Most data about passengers is entered into PNR's by travel agencies (including Internet-based travel agencies) and tour operators, and stored and transferred to U.S. territory by Computerized Reservation Systems (CRS's). These commercial transfers of PNR data to the U.S. are thus in flagrant violation of both the E.U. Data Protection Directive and the E.U. Code of Conduct for CRS's. These violations happen even if the data isn't passed on to the U.S. government.

Since there is no data protection law in the U.S. applicable to PNR data, as soon as this data is transferred or accessible to commercial entities in the U.S. it is subject to both commercial and governmental misuse.

Even if the CRS or other intermediary in the U.S. is not considered to be the owner or "controller" of the data it stores, it is subject to demands for this data by Federal, state, and local government and law enforcement agencies. These demands can be made by agencies other than the division of Customs and Border Protection or the Department of Homeland Security, and would not be regulated by the E.U./U.S. agreement. These demands could be made by secret national security letters or by court orders, and those orders could require the CRS not to reveal that it has received such an order. As the experience of the Electronic Frontier Foundation (EFF) and the ACLU in attempting to challenge other secret U.S. government demands for personal data have shown, judicial review of these types of demands can be blocked by the assertion of the "state secrets privilege" – even when the secret orders become publicly known, which they usually don't.

In addition, the CRS has the right under U.S. law to provide any of the data in its possession "voluntarily" to government agencies or other third parties in the U.S. or other countries. There is no requirement that the airline or the data subject be notified of such disclosures, even if they specifically request such notice. So it is possible that CRS's have provided PNR data to government agencies or other entities in the U.S. or other countries without the knowledge or consent of the airline, the travel agency who made the reservation, or the travellers and other data subjects.

This problem is not limited to flights that touch the U.S. If a travel agency, tour operator, or airline utilizes a CRS based in the U.S., its PNR's and customer profiles are created and stored in a CRS in the U.S., even for flights within the E.U. or in other parts of the world than the U.S.

This outsourcing of data storage and transfer of data to CRS's in the U.S. is almost never disclosed to passengers by airlines, travel agencies, or tour operators. This lack of notice and consent violates the general requirement of the Data Protection Directive, and the specific requirement of the Code of Conduct for CRS's for notice of the CRS being used and for consent for any transfers of PNR data by the CRS to third parties. The consent requirement of the Code of Conduct has no exceptions: it requires consent even for transfers of data to government agencies or for law enforcement purposes.

Finally, API and other PNR data provided under government mandate – such as name, address, and other identifying information – is open to commercial use and abuse. Use of this data is not limited to government purposes. Travel companies are permitted by U.S. law to retain this information indefinitely, and to use or disclose it without notice or consent of the data subjects. This data can be, and is, passed on and used by third parties, including CRS's own data-aggregation, data warehousing, and data mining operations such as Sabre's "Vistrio" joint venture and the Amadeus Revenue Integrity division (formerly "Airline Automation, Inc.").

2. BYPASSING THE PNR AGREEMENT AND THE RIGHTS OF TRAVELLERS THROUGH THE "OPEN SKIES" AGREEMENT

The latest draft of the so-called "Open Skies" agreement on air transport between the E.U. and the U.S. fails to respect the rights of travellers. It would override portions of the PNR agreement, and create new mechanisms by which other provisions could be overturned without adequate public participation in those future decisions.

The "Open Skies" agreement incorporates obligations under law enforcement treaties, but fails to mention any of those treaties limiting the powers of law enforcement or protecting the rights of travellers. In particular, it fails to mention the International Covenant on Civil and Political Rights, which guarantees freedom of movement – including international movement – under its Article 12. The "Open Skies" agreement thus might be interpreted to take precedence over the ICCPR or any restrictions in the PNR agreement, especially if the "Open Skies" agreement is ratified as a treaty, while the PNR agreement is not, but remains a non-binding "undertaking" not enforceable through any judicial process in the U.S.

The "Open Skies" agreement requires compliance with all "recommended practices" of the International Civil Aviation Organization (ICAO). By making ICAO recommendations mandatory, the "Open Skies" agreement effectively delegates to ICAO the legislative power of the E.U. and the US. This is especially problematic because national delegations to ICAO have never included data protection, civil /liberties, or human rights authorities.

The "Open Skies" agreement requires compliance with "security measures" adopted by the parties to the agreement, but sets no standards for the manner in which they should be adopted, or can be reviewed. The "Open Skies" agreement thus requires compliance with even secret, unreviewable, orders adopted without due process or democratic decision-making procedures.

3. CURRENT REVIEW OF POSSIBLE REVISION OR REPEAL OF THE CODE OF CONDUCT FOR CRS's FAILS TO CONSIDER DATA PROTECTION, CIVIL LIBERTIES, AND HUMAN RIGHTS.

The Code of Conduct for CRS's currently requires (A) consent of the passenger for any transfer of data in PNR's to entities (including government agencies) not involved in the reservation, and (B) notice by each system user (airline, travel agency, tour operator, etc.) of the CRS used.

Because all major global CRS's do business in the E.U. and are subject to the E.U. Code of Conduct, these provisions are the de facto global standard for the protection of PNR's and other travel data.

As noted above, these rules are widely and flagrantly violated. Compliance is extremely rare, perhaps because there has been no enforcement by the European Commission of these provisions of the Code of Conduct.

The EC is currently conducting a public consultation on the possibility of revising or repealing the Code of Conduct for CRS's. But the terms of reference for that consultation make no mention of the data protection, notice, and consent provisions of the current Code of Conduct.

4. RECOMMENDATIONS

To address these problems and the ongoing, systematic, and illegal violations of the rights of travellers to freedom of movement and protection of personal data about them and their movements, Irecommend that the LIBE Committee, the European Parliament, and the Article 29 Working Party:

A. Insist on the inclusion of representatives of national data protection and human rights authorities and experts innational delegations to ICAO plenary meetings and ICAO task forces and working groups, such as ICAO's facilitation division and its New Technologies Working Group.

B. Insist on the inclusion of national data protection and human rights authorities and the LIBE Committee in the current European Commission consultation on the Code of Conduct for CRS's. Insist that the current consent and notice requirements for disclosure of CRS usage and of data transfers to commercial or governmental third parties be retained, and that the EC begin to enforce them.

C. Insist that the "Open Skies" agreement explicitly recognize the right to freedom of movement t guaranteed by Article 12 of the ICCPR and other instruments of international law, and that the "Open Skies" agreement not preempt the PNR agreement or require compliance with national "security" measures not subject to meaningful independent judicial review to assure their compatibility with principles of human rights and civil liberties.

D. Enforce the requirements of the Data Protection Directive and national data protection laws with respect to transfers of PNR data to the U.S., in light of the lack of adequate protection for PNR data in commercial hands, once it is transferred to the U.S. This enforcement effort should begin from a recognition of the reliance of airlines, travel agencies, tour operators, and other travel companies on CRS's as aggregators and processors of travel data, and should therefore focus on the obtianing compliance by the CRS's.

E. Ensure that the use of any PNR or APIS data collected from travellers or other data subjects inresponse to government mandates is limited to government purposes. Airlines, CRS's, and other travel companies should not be given a "free pass" to retain, use, disclose, or transfer this data commercially after it has been obtained by government coercion.

Brussels, 26 March 2007

Edward Hasbrouck

Edward Hasbrouck

+1-415-824-0214

edward@hasbrouck.org

http://www.hasbrouck.org
http://hasbrouck.org/articles/PNR.html

Travel expert, consumer advocate, and author of, "The Practical Nomad: How to Travel Around the World" and "The Practical Nomad Guide to the Online Travel Marketplace".

Consultant and technical and policy analyst for the Identity Project on travel-related human rights and civil liberties issues.

ABOUT THE IDENTITY PROJECT

The Identity Project (IDP), http://www.PapersPlease.org, provides advice, assistance, publicity, and legal defense to those who find their human rights and civil liberties infringed, or their legitimate activities curtailed, by demands for identification, and builds public awareness about the effects of IDrequirements on fundamental rights. IDP is a program of the First Amendment Project, a nonprofit organization inthe United States providing legal and educational resources dedicated to protecting and promoting rights protected by the First Amendment to the U.S. Constitution.