

TACD

TRANS ATLANTIC DIALOGUE TRANSATLANTIQUE
CONSUMER DIALOGUE DES CONSOMMATEURS

Secretary Michael Chertoff
U.S. Department of Homeland Security
Washington, D.C. 20528, U.S.A.

Franco Frattini
European Commissioner for Justice, Freedom and Security
Rue de la Loi 200, B-1049 Brussels, Belgium

September 12, 2006

Dear Secretary Chertoff and Commissioner Frattini,

Re: Passenger Name Records (PNR)

We are writing to you regarding the issue of privacy and access to Passenger Name Records. In light of the decision of the European Court of Justice, the U.S.-EU PNR Agreement must be annulled or renegotiated by the end of this month. The TransAtlantic Consumer Dialogue (TACD), a network of more than sixty EU and U.S. consumer organizations that acts as a consultative forum to the EU and U.S., is therefore writing to give you the consumer perspective on the implications for privacy, and the questions of efficacy, related to a transatlantic agreement that might jeopardize the privacy and security of passenger name records.

The importance of adequate security measures is beyond any doubt. TACD believes that security measures should be proportional and effective. TACD issued the attached resolution on PNR in May 2004 (www.tacd.org/docs/?id=254) urging the U.S. and the EU to (1) stop the disclosure of the traveler information until privacy concerns are addressed, and (2) suspend the PNR agreement until the Court of Justice has considered the matter. TACD further urged the U.S. Congress to develop comprehensive privacy safeguards for air traveler information and encouraged all authorities participating in the PNR discussion to consult with consumer protection groups.

The European Court of Justice ruled in May 2006 that the PNR Arrangement lacked an adequate legal basis and held that the agreement would be annulled unless it could be renegotiated prior to September 30, 2006. Subsequently, the Secretary of the U.S. Department of Homeland Security called for the expanded disclosure of air traveler information to the United States.

As set out in the resolution of May 2004, TACD aims to protect EU and U.S. travelers from violations of their privacy as consumers through the extensive disclosure of their passenger name records (PNR) and Advance Passenger Information (API) data from airline carriers, travel agencies, computerized reservation systems (CRS), and data aggregators to U.S. law enforcement authorities and commercial entities.

We have a particular concern about the failure of the present PNR agreement and any future agreements that would violate the privacy rights of consumers or subject air travelers to unnecessary and intrusive profiling and searching. We believe that it is vitally important to explore alternative approaches to air travel safety that are less intrusive and more likely to protect the security of travelers. We note for example, the ongoing problems in the United States installing necessary safety equipment and the recent decision of the Transportation

Security Administration to suspend the installation of the only airport checkpoint device that automatically screens passengers for hidden explosives.

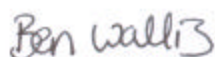
The recent decision of the European Court of Justice and the ongoing concerns in the United States about the accuracy, reliability, and privacy protection for air traveler databases underscore the importance of the TACD position on this matter.

TACD therefore urges the governments of the United States and the European Union:

1. To abide by the decision of the European Court of Justice and establish an adequate legal basis, consistent with EU and U.S. privacy law, to protect the privacy of air traveler information.
2. To undertake a comprehensive study on the effectiveness of air traveler profiling and the alternative techniques that could be pursued to promote air travel safety and protect the privacy of passengers.
3. To publish on an annual basis a report on the implementation of any PNR transfer arrangements established, which includes a reporting of complaints received and resolution procedures.

We would be interested to discuss our concerns and ideas with you, and thank you in advance for taking account of the vital perspective of consumers in Europe and the United States regarding the privacy of their air travel records.

Yours sincerely,



Ben Wallis, TACD Coordinator
On behalf of the TACD Steering Committee

Benedicte Federspiel, Chief Counsel, Forbrugerrådet (Danish Consumer Council)
Jean Ann Fox, Director, Consumer Protection, Consumer Federation of America
Klaske de Jonge, Director, Consumentenbond (Dutch Consumers Association)
Rhoda Karpatkin, President Emeritus, Consumers' Union
Ed Mierzwinski, Director, Consumer Program, Public Interest Research Group
Jim Murray, Director, BEUC (European Consumers Organisation)
Karel Pavlik, International Relations, SOS (Czech Consumer Defence Organisation)
Lori Wallach, Director, Global Trade Watch, Public Citizen

Cc:

Peter Schaar, Article 29 Working Group
Peter Hustinx, EU Data Protection Supervisory Authority
Graham Watson, Member of the European Parliament
Ted Stevens, Chair, Senate Committee on Commerce, Science and Transportation
Daniel Inouye, Co-Chair, Senate Committee on Commerce, Science and Transportation
Conrad Burns, Chair, Senate Commerce Subcommittee on Aviation
John D. Rockefeller, Senate Commerce Subcommittee on Aviation
Susan Collins, Chair, Senate Homeland Security and Governmental Affairs Committee
Joseph Lieberman, Senate Homeland Security and Governmental Affairs Committee
Don Young, Chair, House Committee on Transportation and Infrastructure
Jim Oberstar, House Transportation and Infrastructure
John Mica, Chair, House Transportation Aviation Subcommittee
Jerry Costello, House Transportation Aviation Subcommittee
Peter King, Chair, House Select Committee on Homeland Security
Bennie Thompson, House Select Committee on Homeland Security

TACD

TRANS ATLANTIC CONSUMER DIALOGUE DIALOGUE TRANSATLANTIQUE
DES CONSOMMATEURS

DOC NO. INTERNET-30-04

DATE ISSUED: JUNE, 2004

RESOLUTION ON PASSENGER NAME RECORDS

The Issue

The Trans Atlantic Consumer Dialogue (TACD) has strong concerns about how the current disclosure of personal data in airline reservations for flights from the EU to the US will affect travelers' privacy rights.

It is an issue of particular interest to TACD because the manner in which it is being handled by EU and US authorities indicates a lack of concern for the opinions of the public and the European Parliament (the only elected body of the EU) and a willingness to bypass the democratic debate. This is an issue that could have a major impact on travelers of both economic entities, on the future of the EU-US trade relationship, and on the way travel information will be shared among, and disclosed by, law enforcement authorities and commercial entities in the future.

Risks for Consumers

TACD aims to protect EU and US travelers from violations of their privacy as consumers through the extensive disclosure of their passenger name records (PNR) and Advance Passenger Information (API) data from airline carriers, travel agencies, computerized reservation systems (CRS), and data aggregators to US law enforcement authorities and commercial entities.

- We do not oppose sound security measures designed to ensure aviation safety. However, we believe that passenger profiling and monitoring programs, such as the US CAPPs II system, present risks for the privacy of passengers flying from the European Union, and should therefore be subject to the strongest privacy safeguards
- The use of PNR data from air travelers from the EU in the CAPPs II program has 'mission creep' potential, as this data could be used by US law enforcement authorities for purposes beyond aircraft safety and combating terrorism
- The disclosure by the US government of European passengers' data to governments and authorities outside the EU and the US could put at risk the privacy of those passengers if foreign governments do not have adequate privacy protections in place in the public and private sectors
- The lack of strong access, correction and deletion rights with respect to the personal information collected and used by US authorities, as well as the lack of legally enforceable and truly independent redress mechanisms and compensation rights, makes the risks of abuse more likely

- Regarding the method of transfer of data, the sole acceptable system of transfer is the “push” system whereby the data is first selected, then transferred to U.S. authorities, rather than the “pull” system, which allows U.S. authorities direct access to the airline reservation systems
- There have been recent and widespread disclosures of a sweeping amount of travel data between US private sector entities (airlines, CRS, and data mining companies), and by them to US law enforcement authorities without proper legal authority and for dragnet purposes. These show the lack of adequate safeguards to prevent passengers’ data, including information collected from EU travelers, from unwarranted disclosures and potential abuses
- The US-VISIT program may present risks to many travelers’ privacy when it gains the power to establish links to the passenger data collected by US authorities from travelers flying from the European Union to the United States. The processing of data within the US-VISIT system is not protected by the same EU data protection requirements (as embodied in the EU-US PNR agreement of May 2004) that would apply to the disclosure, and further processing, of passenger data to the US Bureau of Customs and Border Protection
- International Civil Aviation Organization (ICAO)’s proposals for new and revised standards for travel documents, combined with laws and proposals in both the US and the EU to require compliance with ICAO standards, would raise serious privacy implications. These proposals would require the mandatory collection and inclusion of PNR beyond that required for airlines’ commercial purposes; the mandatory collection by airlines and/or travel agents of API data beyond that required for commercial purposes; and mandatory forwarding of PNR and API data to government agencies and sharing of this data between governments, despite the lack of legal protections for data shared with those governments or commercial entities.

Resolved

The TACD urges the governments of the United States and the European Union:

- To stop the disclosure of personal data of US-bound passengers flying from the EU, and its use by the US government, *inter alia* for testing of passenger pre-screening systems such as the CAPPS II program, until:
 - all privacy issues regarding the implementation of this program have been addressed in a satisfactory manner as recommended by the US General Accounting Office report of February 2004; and
 - EU-specific concerns have been addressed pursuant to the recommendations of the European Parliament and the Article 29 Data Protection Working Party
- To suspend implementation of the EU-US PNR agreement of May 2004 until the Court of Justice of the European Communities has examined the compatibility of the Commission’s adequacy decision and of the EU-US PNR agreement with EU rules, and until it has ruled on whether the European Parliament’s assent is necessary before the agreement can enter into force
- To encourage the US Congress to assess the specific privacy risks related to passengers’ personal information and passenger pre-screening programs, and determine whether they warrant any specific legislative measures
- Not only to question the adequacy and purposes of the regime surrounding the transfer of passenger data, but also the reality of its implementation. This is because it may lead to a system of global surveillance for general law enforcement purposes, as well as to increased cooperation between the US government and commercial entities to work on data mining projects without proper privacy safeguards. The purposes for which

passenger data are collected have to be strictly defined and their use limited to the fight against terrorism and terrorism-related crimes

- To establish a strong legal framework for transferring airline data to government authorities in the US in a way that is compatible with strong data protection principles. This entails:
 - limiting the data elements to what is proportionate to the aims sought;
 - ensuring the accuracy of the records, and of the matching of passenger records against suspects’;
 - making the data retention periods short and proportionate;
 - providing clear and comprehensive information to passengers, including about the content and scope of the data required, the purpose of collection and the data recipients before their travel information is collected;
 - providing passengers with a judicially enforceable right to access, correct, modify and/or delete their personal data.
 - providing consumers with truly independent redress, compensation and appeal mechanisms in case of governmental abuse and infringement of passengers’ rights;
 - determining the US agencies and authorities to which PNR data would be disclosed
- To make the EU-US PNR agreement and the US Undertakings legally binding in the United States in order to enable air travelers to obtain redress before US courts
- To prohibit transfers of passenger data when they are made to non-EU government agencies or law enforcement authorities, unless they comply with the EU-US PNR agreement, or other existing third -party information-sharing rules with equivalent data protection requirements
- To suspend the implementation of the EU-US PNR agreement until the technical mechanisms to put in place a “push” system of data transfer are available
- To assess passenger data transfer schemes, new standards for travel documents, as well as passenger pre-screening and biometric identification systems, such as CAPPS II, US -VISIT programs, together when negotiating agreements to protect travellers’ privacy. Common data protection rules should apply to interconnected programs that use or will use the same personal data
- To modify the privacy policy applicable to the US -VISIT Program in order to provide travelers, covered by both the EU-US PNR agreement and the US-VISIT program, with the same level of privacy protections
- To encourage all authorities involved in the PNR discussion to consult with consumer protection groups, as well as to include representatives of consumer organizations and data protection authorities in discussions of ICAO and other relevant standards proposals, and in government delegations to ICAO meetings and working groups, in particular in any cases where proposed standards would override or alter national or EU consumer protection or data protection laws or regulations.