BNA International

World Data Protection Report

International Information for International Businesses

Monthly news and analysis of data protection and privacy issues from around the world

The Transfer Of Airline Passenger Data to the U.S.: An Analysis of the ECJ Decision

By ***Henriette Tielemans***, ***Kristof Van Quathem***, ***David Fagan***, *and* ***Amalie Weber***
Covington & Burling.

Reprinted from the June 2006 issue of BNA International's
World Data Protection Report

www.bnai.com

Personal Data

The Transfer Of Airline Passenger Data to the U.S.: An Analysis of the ECJ Decision

By Henriette Tielemans, Kristof Van Quathem, David Fagan, and Amalie Weber, Covington & Burling.

Henriette Tielemans and Kristof Van Quathem are Partner and data protection advisor, respectively, in the Brussels office of Covington & Burling. David Fagan and Amalie Weber are associates in the Washington, D.C. office of the firm. The authors may be reached at htielemans@cov.com; dfagan@cov.com; kvanquathem@cov.com; and aweber@cov.com

In a much anticipated decision,[1] the European Court of Justice (ECJ) annulled on May 30, 2006, an agreement between the European Union and the United States providing for flights departing from E.U. Member States and destined for the U.S. to transfer upon departure, certain airline passenger information to the U.S. Homeland Security Bureau of Customs and Border Protection (CBP). Some observers hailed the decision as a triumph of E.U. privacy law for protecting passenger information and beating back the United States' post-September 11 efforts to extend its jurisdictional reach in the name of national security. Others, however, have portrayed the ECJ as deciding the case on a mere technicality, laying the groundwork for the Commission and U.S. negotiators to tweak the agreement only slightly – or the Commission simply to alter the legal grounds for entering into the agreement – and for the data transfer to continue as planned.

In reality, the true impact of the ECJ decision likely lies beyond the particulars of passenger data – the United States is likely to get the passenger data that it requires either through a revised agreement at the E.U. level or via bilateral negotiations. The greater meaning of the ECJ case might be first, that the scope of E.U. privacy rules are much narrower than many believed; and, secondly, that other data-related Directives, such as the recent Data Retention Directive,[2] may be on shaky legal footing.

The U.S. Statutory and Regulatory Framework for Passenger Data

Following the terrorist attacks of September 11, 2001, the United States overhauled the statutory and regulatory landscape with respect to a range of domestic security issues, including aviation security. The overhaul of aviation security began specifically with the enactment of the Aviation and Transportation Security Act (ATSA) in November 2001.[3] ATSA created the Transportation Security Administration within the Department of Transportation.[4] It also established a series of requirements to increase flight safety, such as the requirement that the door to the cockpit be locked during flight[5] and the requirement that airlines provide seats for air marshals.[6] New forms of infrastructure protection for critical national assets, such as airports, were also introduced.[7]

In addition to these measures, ATSA mandated that both foreign and domestic airlines that operate flights to the United States provide passenger and crew manifests and, for either inbound or outbound foreign air flights, passenger name records (also known as PNR data) to the CBP.[8] PNR data is the reservation information contained in an air carrier's electronic reservation system that sets forth the identity and travel plans of each passenger or group of passengers in a reservation record.[9] Under ATSA, an airline carrier must provide CBP with electronic access to its PNR information when requested to do so. The airline carrier must allow CBP to interface directly with the airline's electronic reservation systems and provide CBP with the commands necessary to properly access the information.[10]

Importantly, the law places no restriction on which elements of PNR data CBP may request to receive. CBP may share any PNR data that it does receive with other federal agencies, upon request, for national security or other lawful purposes that comply with the requirements of the Privacy Act governing federal inter-agency sharing of personal information.[11] PNR data collected by CBP is protected from disclosure to non-governmental third parties by the Freedom of Information Act (FOIA), which, among other things, limits the public disclosure of personal information where such disclosure of the information would constitute a clearly unwarranted invasion of personal privacy, or where the information is complied for law enforcement purposes, to the extent that disclosure may reasonably be expected to constitute an unwarranted invasion of personal privacy.[12]

The U.S./E.U. Agreement

Pursuant to ATSA and the implementing regulations, CBP sought the compliance of European airlines with its requirements to receive access to PNR data, resulting in a protracted negotiation with the European Commission to reach a pan-European accommodation that would put European carriers on an equal footing, consistent with E.U. law, while allowing the U.S. government access to the information it desired.

The U.S. requirements posed a number of problems for European authorities. First of all, the E.U. imposes strict limits on the processing and international transfer of personal data under the Data Protection Directive and the Member State implementing laws. Among other things, the Data Protection Directive restricts the transfer of personal data to countries without data protection laws similar to those in the European Union. The United States does not have a privacy regime similar to that of the E.U. Moreover, PNR data is collected by airlines in connection with the service that the airlines provide for passengers. Under the Data Protection Directive, airlines would be required to justify any alteration of that use to serve the purposes of law enforcement – and it was questionable whether such a legal basis existed under E.U. law at the time the U.S. laws came into effect.

Against this background, representatives of the E.U. data protection authorities of the 25 E.U. Member States, assembled in the so-called Article 29 Working Party (WP29), voiced strong

 WDPR ISSN 1473-3579

opposition to the envisioned transfer of passenger information soon after the United States adopted ATSA and issued the initial implementing regulations on PNR. In particular, the WP29 challenged the disproportionate nature of the measures, the excessive retention times, and the lack of legal basis for the transfer.[13] The European Parliament, and in particular its left wing and liberal members, also took up the issue and adopted several resolutions against the envisioned transfers.

At the same time, the terrorist attacks of September 11 remained fresh in the minds of government leaders, and the interests of commerce – access to the U.S. market is vital to Europe and Europeans are the largest group of foreigners travelling to the United States[14] – dictated that a compromise be reached. The European Commission, therefore, set out to negotiate a solution that would provide for protection of passenger information and formalise the PNR requirements to give legal certainty to the E.U. airlines. The Commission's solution was ultimately comprised of three elements:

- a set of Undertakings adopted by CBP;
- a Commission adequacy determination; and
- the ultimate E.U./U.S. Agreement.

The Undertakings

Following intensive negotiations with the European Commission, on May 11, 2004, the CBP adopted a set of Undertakings related to how it would use the PNR data it collects from airlines. The Undertakings apply for a period of three and a half years, and clearly follow the general data protection principles, most of which can also be found in the E.U./U.S. Safe Harbor Agreement. The key elements of the Undertakings are as follows:

- *Purpose "limitation"*: CBP pledged that PNR data would be collected solely for preventing and combating terrorism and related crimes, including "other serious crimes" that are transnational in nature.[15]
- *Categories of data*: The Undertakings contain an Annex of 34 PNR data fields on which CBP can request information.[16] The 34 fields – which range from name, address and billing information to seat and ticket number – were negotiated from a potential 60 fields that are contained in some airlines PNR systems.
- *"Sensitive" data*: CBP pledged not to use any "sensitive" data, defined as "personal data revealing racial or ethnic origin, political opinions, or religious or philosophical beliefs" among other things.[17] CBP also pledged to implement an automated system that would filter such sensitive data from PNR codes.
- *Onward transfers*: PNR data can be shared with other U.S. agencies pursuant to the protections of U.S. law and agencies. PNR data can also be shared with "foreign government authorities" for the limited purposes described under the agreement (*e.g.*, combating terrorism and other law enforcement purposes).[18] The Undertakings provide that any other entity receiving PNR data from CBP must agree to terms of disclosure that restrict the purpose for which the PNR data can be used, ensure the disposal of the data, and require CBP's authorisation before any further disclosures take place.
- *Method of access*: While obtaining the right to initially "pull" PNR data, CBP relented on making this right permanent and agreed that it would ultimately be willing to receive data that is "pushed" by the airlines.
- *Notice, access, and rectification*: CBP has agreed to inform passengers of the collection and use of their information, and passengers have a right of access to their information on the basis of FOIA, subject to the limitations set out in the Act. CBP has also agreed to rectify data at passengers' request.
- *Security*: CBP has agreed to keep the PNR data in encrypted form on a closed intranet system, with access limited only to authorised and trained personnel.
- *Retention*: The CBP agreed to limit the retention of PNR data to three and a half years. If the data has been "manually processed", it may be retained for up to eight years.
- *Remedies and verification*: Passengers can lodge complaints with their national Data Protection Authorities or with the CBP. If the complaint cannot be resolved by the CBP, passengers can turn to the Privacy Officer of the Department of Homeland Security. In addition, the CBP will undertake a review of the implementation of the Undertakings every year, in cooperation with the Commission and representatives of European enforcement authorities.
- *Reciprocity*: The United States agreed that it will provide future assistance if the European Union or its Member States introduce similar requirements for U.S. airlines to transfer PNR data to E.U. authorities.

Adequacy Determination

Following the negotiation of the Undertakings, the Commission launched a "comitology" procedure under the Data Protection Directive to declare that the Undertakings offered an "adequate" level of protection to PNR data transferred to the United States.[19] The European Parliament reacted by adopting a Resolution against the adequacy determination and calling on the Commission and Council of Ministers to stop the procedure and to first seek an opinion from the European Court of Justice. The request was rejected and, on May 14, 2004, the Commission formerly decided that the Undertakings provide adequate protection under the Data Protection Directive.[20] As a result of this decision, the restrictions on transfers of PNR data to the United States lapsed.

The Agreement

An adequacy determination does not in and of itself suffice to legalise the overall processing of PNR data by airlines for law enforcement purposes – it only legalises the international transfer aspect. Therefore, on May 17, 2005, the European Council of Ministers approved a bi-lateral Agreement with the United States, pursuant to which both parties agreed that the CBP would have access to PNR data in line with its Undertakings and within the limits set out in the adequacy determination.[21] The Agreement explicitly required airlines to make PNR data available to CBP in the United States, thereby providing a legal basis for European carriers to process requests received from CBP.

The Council approved the Agreement on the basis of Article 95 and 300 of the E.U. Treaty, which govern, respectively, measures for the establishment and functioning of the Internal

Market, and international agreements. Under this combined basis the European Parliament's role was limited to adopting non-binding resolutions. The European Parliament, however, refused to perform any consultative role in the Council's determination, claiming that the Agreement violated the Treaty rules. At the same time, the WP29 also adopted a critical report on the Undertakings, principally attacking the overly broad purpose definition and the potential disclosures of information to other U.S. agencies and other foreign governments.[22]

Parliament's Challenge and the ECJ Decision

On July 27, 2005, the European Parliament filed its formal challenge in the European Court of Justice to both the Agreement and the adequacy determination. The European Parliament challenged the legal basis of the Agreement and the legality of the adequacy determination, and claimed that the Council had violated the fundamental right to privacy enshrined in the European Convention on Human Rights. On the basis of these arguments, Parliament asked the Court to annul both texts.

Legal Basis for the Agreement and Adequacy

Parliament's arguments related to the invalid legal basis for the Agreement and the adequacy determination are best framed in terms of the historical evolution of the European Union. Launched as an European Economic Community, the Union has by now entered almost every aspect of the economic and monetary policy to eventually create an Internal Market and a monetary union – the so-called "first pillar" of E.U. competency. However, in other areas, such as cooperation in foreign policy (the "second pillar") and police and judicial cooperation in criminal matters (the "third pillar"), the establishment and acceptance of E.U. competency has been slower to form. As a result, different procedures and even different legal instruments have developed for decisions in different "pillars". For example, in the case of Internal Market issues, the European Parliament acts as an equal partner and Member States can be outvoted in the Council of Ministers. By contrast, in matters of criminal law, Parliament's role is often reduced to that of non-binding resolutions and in the Council, Member States often have to agree unanimously on a text.

Against this background, the ECJ considered Parliament's argument that both the Agreement and the adequacy determination were based on the wrong legal basis. On the adequacy determination, the European Parliament noted that the Data Protection Directive was adopted under the first pillar (Internal Market) – to ensure the free flow of personal information among Member States (a commerce-related view of data) – and, therefore, may only govern processing operations that fall within the scope of the first pillar. Article 3 of the Directive moreover explicitly provides that the Directive does not apply to the processing of personal data in the course of an activity that falls outside the scope of Community law, such as to processing operations concerning public security, defence, and state security. The ECJ agreed with the arguments developed by the European Parliament, and further agreed CBP's use of personal data and the transfer of data to CBP are matters that, in fact, concern principally public security and relate to State activities in the areas of criminal law – not the Internal Market. Based on this reasoning, the ECJ decided that the adequacy determination is null and void.

On the Agreement, the Council of Ministers took the position that the Agreement in fact related to the first pillar (Internal Market) because it impacted how airlines could be treated by the Member States. The Council argued that unless the Member States agreed on a common manner to deal with the transfers of data to the CBP, some airlines could be fined by their home country regulators for complying with the U.S. data transfer mandates while others would not. Likewise, some airlines could be subject to U.S. fines for failing to comply with CBP requests while others would just allow for the transfer of data. In the Council's view, these differences in treatment could impact competition among the airlines. As a result, according to the Council, the Agreement was justified under Article 95 of the E.U. Treaty, which allows the Council of Ministers to adopt measures to establish the Internal Market. The Court rejected the Council's argument. It decided that the primary objectives of the Agreement are combating terrorism and protecting the privacy of E.U. passengers, and that the use of an Internal Market basis for such objectives is not appropriate. The ECJ therefore, also decided that the Agreement is null and void.

In terms of transition, the Court pointed out that the Agreement can be terminated by the European Union at any time, with the termination taking effect 90 days from the notification. That brings us to September, 2006. Because the Agreement can have effect only in combination with the adequacy determination, the Court decided to also uphold the adequacy determination until September 30, 2006. The Commission and the Member States thus have until that date to come up with an alternative mechanism for the PNR transfers.

Human Rights and Proportionality

As a result of its decision to annul the case, effectively, on procedural grounds, the ECJ was able to avoid addressing any of the substantive arguments on human rights and proportionality that the Parliament had raised. The Parliament specifically claimed that the Agreement with the United States and the Commission's adequacy determination violated the human right to protection of personal data as enshrined in Article 8 of the European Convention on Human Rights, and, in particular, breached the principle of necessity and proportionality contained in the Convention.

These questions technically remain open in light of the ECJ's disposition of the case. However, it is worth noting that in his opinion to the Court, the advocate-general, who prepared the Court decision, analysed the Agreement and the Undertakings terms in light of the Human Rights Convention and concluded that the documents did not violate the Convention.[23] The advocate-general specifically concluded with respect to Parliament's many complaints arising out of the Agreements and Undertakings – *e.g.*, the excessive retention time, the disproportionate amount of data, the overly broad uses and disclosures, and the lack of rights and remedies for passengers – that the protection of passenger data had received sufficient consideration in each case. The advocate-general also found that Member States, in areas concerning public security, have considerable latitude in deciding what is a proportionate measure.

Consequences of the ECJ Decision and the Likely Next Steps

For the United States, the ECJ decision, while noteworthy, is perhaps less momentous than for its counterparts across the Atlantic. CBP is statutorily authorised to collect PNR information without the accommodations contained in the Undertakings, such as the limited number of data fields requested by CBP and the restrictions on the use of sensitive data. The U.S. government is unlikely to back away from what it views as requests for information that will make its aviation and homeland security screening efforts more efficient and that, moreover, the U.S. Congress has clearly authorised the Executive Branch to seek. There is a sense, in public statements from U.S. government officials so far, that CBP will stay on course in its information requests and that how the E.U. complies with the requests is primarily a concern for the European Union – although U.S. officials might reasonably be expected to help their European counterparts develop a solution that will withstand another challenge before the ECJ.

In the European Union, the impact of the ECJ decision is greater, at many levels. First, at a practical level, the ECJ annulled the airlines' legal basis for processing PNR data for law enforcement purposes and for transferring the data. Thus, European airlines are again facing the prospect of having to grapple with two possibly conflicting regulatory regimes on this issue. Their plight will presumably be a source of pressure to reach an alternative basis for the Agreement.

Secondly, the likely solution to the ECJ decision is for the Council to conclude a new Agreement with the U.S. Government, this time under the third pillar. This Agreement would have to be unanimously approved by the Council of Ministers. In a recent press conference, Commissioner Fratinni, the E.U. Commissioner responsible, indicated that he was confident that the E.U. institutions would meet the September 30, 2006 deadline. If a "third pillar" solution is reached, the European Parliament would only have the authority to adopt a non-binding resolution addressing the Agreement and would not have the authority to challenge the new decision in Court.

Thirdly, in turn, the ECJ decision may have unexpected results for the European Parliament. Although it was technically the victor in the ECJ decision, the Parliament will likely see its authority reduced by any subsequent E.U.-level solution. Moreover, the Court did not consider whether the Agreement and the Undertakings violate human rights. As a result, the Commission and the Member States have no obligation to change the content of the annulled measures – a point of concern for the Parliament.

Fourth, the ECJ decision will be of greater impact across Europe if an E.U. level agreement cannot be reached. In that case, each Member State may separately conclude a bilateral agreement with the United States. The risk of bilateral agreements, of course, is that different rules could apply across the European Union, with the E.U. airlines affected differently depending on the bargaining power and interests of each individual Member State. Because of the potential disparate impact of different rules, most observers believe a solution will be found at E.U. level.

Finally, unrelated to the PNR debate, the Court decision may touch on other E.U. measures that have attracted attention of late. For example, the recent Data Retention Directive mandates the retention of communications traffic data by electronic communications service providers for law enforcement purposes. The Directive was adopted on the same basis as the PNR Agreement (Article 95 of the Treaty) and likewise clearly obligates commercial entities to process personal data for law enforcement purposes, which now seem to fall outside the scope of the Internal Market and the Data Protection Directive. For Member States on the fence about whether to challenge the Data Retention Directive, the ECJ analysis of the PNR Agreement may well provide the final push to make a challenge.

1 *European Parliament v. Council of the European Union*, C-317/04 ; *European Parliament v. Commission of the European Communities*, C-318-04.

2 Directive 2006/24/EC of the European Parliament and of the Council of March 15, 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. (Official Journal, *L 105, 13/04/2006).*

3 Aviation and Transportation Security Act, Public Law No. 107-71, 115 Stat. 597 (2001).

4 Id. at § 101.

5 Id. at § 104.

6 Id. at § 105.

7 Id. at § 106.

8 Id. at § 115 ; *see also* 49 U.S.C. § 44909(c)(3).

9 19 C.F.R. § 122.49d.

10 19 C.F.R. § 122.49d.

11 See 5 U.S.C. § 552a.

12 Freedom of Information Act, 5 U.S.C. § 552(b).

13 WP29, Opinion 6/2002 of October 24, 2002 on transmission of Passenger Manifest Information and other data from Airlines to the United States. WP29, Opinion 4/2003 of June 13, 2003 on the level of protection ensured in the United States for the transfer of Passengers' data.

14 Nicola Clark, E.U. Court Bars Giving Passenger Data to U.S., International Herald Tribune, May 31, 2006 (noting U.S. Department of Commerce data on travel by Europeans to the U.S.), available at *www.iht.com/articles/2006/05/30/news/fly.php*.

15 Undertakings of the Department of Homeland Security Bureau of Customs and Border Protection, ¶ 3 (2004), *www.dhs.gov/interweb/assetlibrary/CBP-DHS_PNRUndertakings5-25-04.pdf*.

16 Id. at Attachment "A".

17 Id. at ¶ 9.

18 Id. at ¶ 29.

19 This procedure – which consists of a simple proposal from the Commission to be approved (or rather, not rejected) by the E.U. Member States, with the possibility of Parliament to opine on the text – is common under E.U. law for the adoption of implementing measures. For example, the same procedure has been used for the adequacy determination of the Safe Harbor Agreement and the standard contractual clauses.

20 Commission Decision of March 14, 2004 on the adequate protection of personal data contained in the PNR of air passengers transferred to the United States' Bureau of Customs and Border Protection. (Official Journal, L235, 6.7.2004).

21 Council Decision (2004/496/EC) of May 17, 2004 on the Conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection. (OJ L183, 20.5.2004).

22 WP29, Opinion 2/2004 of January 29, 2004 on the protection of personal data contained in the PNR of air passengers to be transferred to the United States' Bureau of Customs and Border Protection.

23 Opinion of the Advocate General Léger of 22 November 2005 on Case C-317/04 and case C-318/04.