Notes and Commentary

The Agreement on Passenger-Data Transfer (PNR) and the EU-US Cooperation in Data Communication

Kay Hailbronner*, Vagelis Papakonstantinou**
and Marcel Kau***

I. INTRODUCTION

Although individual privacy is a much-esteemed right on both sides of the Atlantic, in practice its protection has engendered, within the last ten years, some serious legal and socio-economic conflicts between the United States and the European Union. Its elusive context only constitutes part of the problem's explanation. After all, regardless whether "privacy", "information privacy" or "data protection", individuals in the Western hemisphere broadly understand the same thing when it comes to infringements of their privacy rights. Part of the same explanation also relates to different backgrounds: in the United States, the state is admittedly viewed in opposition to individuals, as something whose powers must be kept under control; in Europe, different historical experiences have led to a similar concept of checks and balances as in the United States, though public interests and common goods foster the government's positions toward the

* Professor of Law at the University of Konstanz/Germany (Chair for Public Law, International and European Law) and Director of the Center for International and European Law on Immigration and Asylum.
** PKpartners Law Firm, Athens Greece and lecturer at the University of Patras, Greece, Department of Computer Engineering and Information.
*** University of Konstanz, Germany.

Published by Blackwell Publishing Ltd.,
9600 Garsington Road, Oxford OX4 2DQ, UK, and
350 Main Street, Malden, MA 02148, USA.

International Migration Vol. 46 (2) 2008
ISSN 0020-7985

individual. Consequently, this setting has led to a stronger need for data protection in Europe, and a more lenient protection framework in the United States.

These reasons, and perhaps many more ranging from economics to sociology and politics, have led to today's situation where, when it comes to the protection of privacy, we are faced with two rather different systems. Problems occur when these two systems intersect, which is unavoidable given the breadth of relationships at all levels between Europe and the United States. One of the recent examples of transatlantic conflicts is the demand of the US government that air carriers operating flights from Europe to the United States have to transfer the passenger's name records in advance.

On 11 December 2006, an expert meeting supported by the German Marshall Fund dealt with the Agreement on Passenger Data Transfer between EU Member States and the United States in the context of transatlantic cooperation in data communication. The participants of the meeting came from both Europe and the United States, and included academics as well as representatives of the US government, the EU Commission, and the Electronic Privacy Information Center (EPIC), a Washington-based non-governmental organization. The focus of the discussions was the existing Agreement of European airlines to provide data on arriving passengers and the different data protection traditions in the United States and Europe.

II. DATA PROTECTION AND THE PNR AGREEMENT

Passenger Name Records (PNR)

The term passenger name record denotes "the travel record for a person, as used by airline and travel agency databases". In effect, the PNR is the information required by an airline to sell an airplane ticket; this information nowadays include the passenger's full name, date of birth, home and work address, telephone number, e-mail address, passport details, credit card details or method of payment, the names and personal information of emergency contacts, as well as details of any special meal requirements or seating preferences or any other similar requests. According to information released during the negotiations of the PNR issue, each record actually includes some sixty fields pertaining to personal information of the respective passenger.

Even from a preliminary point of view, the significance per se of creating a database with sixty fields on each and every individual can hardly be overlooked;

in effect, the PNR system creates a database with comprehensive information on all basic individual data.

The treatment of PNR data as something more important than what they really are – information in order to make a booking – began with the terrorist attacks of September 11th. In the obvious belief that through adequate processing of PNR terrorists could have been kept out of the country the US Bureau of Border and Customs Protection (CBP) started asking international air carriers for access in their passenger data. Evidently, access by CBP of PNR data meant access to information on who traveled to the United States before that person landed on US soil.

European airlines were at that point faced with a dilemma: if they did not comply with CBP they would not be able to fly to the United States, while if they did comply, they would very probably break the law in their homeland, since according to a basic principle of data protection law, personal information may not be transmitted to any third country that does not afford an "adequate" level of protection in comparison to that within the EU. The United States notoriously fails the European "adequacy" test; therefore, by law no personal information may travel from any EU Member State to the United States. European airlines ultimately were only left with the choice of which law to break.

Background and invalidation of the first PNR Agreement

In order to resolve the deadlock European airlines were facing the European Commission intervened and began negotiations with the United States in order to resolve the PNR matter centrally, for all Member States. A legal basis for the Commission was therefore urgently needed; given that the only data protection law at that time was the EU Data Protection Directive, the legal basis had to lie within it. Indeed, the Commission decided to consider PNR as commercial information, and began negotiations with the United States in 2003. From a US perspective, the new instrument was intended to build upon the Aviation and Transportation Security Act of 2001.

Negotiations went on for most of 2003. Evidently, the most difficult problem was to overcome the generally known "inadequacy" of the US legal scheme for the protection of privacy, at least in comparison with European standards.

The first PNR Agreement was entered into on 28 May 2004 in Washington. Prior to that, Commission and Council respectively issued their decisions on the "adequate protection of personal data" and the "Agreement between the European Community and the United States of America on the processing and

transfer of PNR data". All of this did not sit well with the European Parliament, mostly since it was eager to play a more important part in European policy. As a result on 27 July 2004, a couple of months after the first PNR Agreement was concluded, the Parliament filed two actions in front of the European Court of Justice, each one aimed at the Council's and Commission's decisions, upon which the first PNR Agreement was based, respectively. The Parliament claimed, among other things, that adoption of the decision on adequacy was ultra vires, that the legal basis for the decision approving the conclusion of the agreement was not appropriate, and that fundamental rights had been infringed. Additionally, the newly established European Data Protection Supervisor intervened in support of the Parliament in both cases.

The Court reached its decision two years later, on 30 May 2006 (C 317/04). It did not go into the substance of the Parliament's claims, because it found that because the first PNR Agreement did not pertain to commercial communications but rather to security matters, the legal basis of the first PNR Agreement could not be the Directive; therefore the first PNR Agreement had to be annulled. The Court subsequently set a deadline for a new PNR Agreement to be entered by 30 September 2006.

Negotiations for conclusion of the second PNR Agreement started in July 2006, again centrally for all EU Member States but this time by the Council, because the Court's decision put a lid on the Directive's application when it came to PNR information once and for all. However, given the tight deadline and the tense feelings that the Court's decision raised within the EU, its conclusion by September 2006 seemed unrealistic. In accordance with new European processes (so-called "Third Pillar"), negotiations between the United States and the Finnish Presidency, assisted by the Commission, were completed on 6 October 2006 and an interim PNR Agreement was finally entered into on 18 October 2006. The interim agreement expressly refers to the Undertakings by the Department of Homeland Security (DHS) incorporated in the first PNR Agreement, which therefore also remains in effect, but is amended by a later side agreement.

Since the current interim Agreement on the transfer of passenger data is only valid until 31 July 2007,[1] it is of a provisional nature and both sides are bound to agree on permanent rules governing the exchange of passenger data.

Provisions of the interim PNR Agreement

From a first point of view, the interim PNR Agreement by itself does not differ substantially from its predecessor of 2004. It is, nevertheless, its reading in combination with a side letter by the DHS, which is officially annexed in the Council's decision, which has raised substantial concerns on its actual effectiveness in protecting individual privacy.

The interim PNR Agreement alone does not stray from notions and mechanisms implemented by its predecessor: at its core lies the basic provision that "in reliance upon DHS's continued implementation of the aforementioned Undertakings as interpreted in the light of subsequent events, the European Union shall ensure that air carriers operating passenger flights in foreign air transportation to or from the United States of America process PNR data contained in their reservation systems as required by DHS." In parallel, DHS has the right to "electronically access the PNR data from air carriers' reservation systems located within the territory of the Member States of the EU (pull system) until there is a satisfactory system in place allowing for transmission of such data by the air carriers (push system)." Therefore, according to the interim PNR Agreement, the DHS has the right to instruct European airlines which PNR data to collect and to access to them. Naturally, all this stands under the condition that DHS continues to adhere to the Undertakings of 2004. The Undertakings are essentially provisions of a technical nature that regulate the details of DHS' processing.

Among the few differences of the interim PNR Agreement from its 2004 predecessor is the expansion of the catalogue of US agencies that may process PNR data: this time it is not only the DHS, and in particular the CBP, that are designated processors of PNR data, but rather "CBP, US Immigration and Customs Enforcement and the Office of the Secretary and the entities that directly support it", explicitly excluding certain "components of DHS."

Another point that has raised criticism refers to the interim PNR Agreement allowing DHS to change the standards of processing, if US laws change to this end. Additionally, a side letter of the United States side amends the Undertakings of 2004, upon which the interim PNR Agreement is based. In brief, EU PNR data are now openly shared among any US agency that undertakes some, even remote "counter-terrorism function". According to the side letter, the DHS alone may decide which PNR data it requires to be transmitted for an indicative period of 72 hours before the respective flight; the limitation to only accessing 34 out of some 60 PNR fields became indicative; and PNR data must be stored for periods over 3.5 years since collection. Finally, no implementation review shall be performed as long as the interim PNR Agreement remains in effect.

Altogether, the interim PNR Agreement is neither a text substantially different from its predecessor, nor one that could cause more problems to individual privacy than the previous regulatory framework already did; nevertheless, the situation is practically reversed by the DHS' side letter to the interim Agreement, that the Council decided to, in a confusing way from a law-making perspective, annex to its Decision on the adoption of the interim PNR Agreement.

Given the reversing effect of the side letter to the PNR status as known until today, it comes as no surprise that the Parliament has fiercely attacked the final wording of the interim PNR Agreement, and requested amendments and clarifications from the Council. The power struggle that led to the Parliament's actions and brought the situation this far shall also presumably add to the intensity of reactions, which will probably increase when negotiations for the second PNR Agreement begin in the very near future.

Data protection concerns

The interim PNR Agreement as amended by the DHS side letter cannot stand any data protection evaluation because it too obviously constitutes a product of negotiations in which data protection was found at the wrong end of the power struggle.

What could prove of use in this analysis is reference to certain inherent concerns that pertain to the notion of a PNR Agreement per se, when examined from a data protection perspective. In the case of beforehand processing, while a passenger is still trying to cross the Atlantic or is even packing back home, PNR-related processing can only refer to either flagging individuals that are not welcome in the United States but have obviously not committed any criminal acts thus far, or mass profiling. In the first case, the measures taken can from an intelligence or police perspective be expedient, but must not remain totally uncontrolled. The second case, however, is the one that is potentially problematic and raises human rights concerns: given that PNR data afford profiling based on sensitive personal information, for instance, sorting out Muslims on any flight on the basis of their meal preferences, one cannot help but wonder whether such persons will not be treated differently when they land in the United States, based solely on their religion or nationality.

In this context, there appears to exist little difference between "push" and "pull" methods when it comes to PNR data processing. Although the EU demonstrates a strong preference towards a "push" system, whereby air carriers shall forward

filtered PNR data to the DHS, as opposed to a "pull" system where DHS reaches out itself to the reservation database of air carriers, the essence of the PNR Agreement abolishes in practice any significance to that distinction from a data protection perspective, since DHS controls what kind of PNR data are collected and which categories are transmitted.

III. DIFFERENT APPROACHES TO THE PROTECTION OF PRIVACY

Common backgrounds – different approaches

The different approaches to privacy between the EU and the United States may come as a surprise to many, given the common roots of both systems. Indeed, data protection emerged on both sides of the Atlantic, sharing origins both in the United States and in those European states that were technologically advanced enough to afford it. The 1960s and 1970s witnessed a series of publications on the protection of privacy from emerging information technology, primarily by US scholars. The first privacy or data protection regulatory texts emerged almost simultaneously: German states, Sweden, and the United States were the first to acquire legislation protecting private life, only to be closely followed by France, Germany at a federal level, and, only in the early 1980s, the United Kingdom and other European states.

It could be said, and is indeed often maintained, that data protection or the protection of information privacy from the then emerging information technology developed within a small international circle of scholars on both sides of the Atlantic, who practically imposed the introduction of such legislation on their own jurisdictions. Once that happened in certain technologically advanced countries, data protection became a trend and was followed by other technologically advanced countries. By the early 1980s, all countries in whose jurisdictions computers meant anything had dealt in one way or another with the issue of protecting individual privacy from related infringements.

Notwithstanding this common basis, the EU and the United States developed differently with respect to privacy protection. Regardless of the reasons behind such choice, the fact remains that Americans opted for a laissez faire approach, whereas in Europe, data protection became institutional. And, as years passed, the respective institutions became deeper in Europe which still constitutes a strong contrast between the two models.

In any event, the European data protection system is institutional, meaning that an agency is in charge of data protection at the national level (state or federal agencies). This agency runs controls over enterprises and the public sector, and issues fines, regulations, guidelines and codes of conduct. While doing so, it applies a law, usually the Data Protection Act, that primarily has two aims: first, it sets basic data protection principles for private and public processing, and, second, affords certain rights to individuals. Among such principles is listed the finality principle, which provides that a database may only serve the purpose it was created for. Equally important is the principle of fair and lawful collection and processing. Individual rights include the right to information, and access and rectification of erroneous entries in personal information databases.

In contrast to this, the United States seems to have opted for sector-specific legislation such as the Video Surveillance Act or Data Matching Act accompanied by self-regulatory attempts, plus the Privacy Act of 1974 that only applies at federal level. No data protection agency operates in the United States, nor is any of the basic European data protection principles applicable there. Even though the legislative rules on data protection are less developed in the United States, constitutionally-based privacy rights have been accepted for many decades. Additionally, the DHS offers some kind of administrative redress, although there are no judicial remedies to safeguard law infringements in data protection matters. Eventually, the DHS' division in charge of privacy matters will constitute an institutional framework that is nevertheless different from the institutional basis of the European data protection agencies.

A lot of alternatives to institutional data protection have been proposed (e.g. self-regulation) and many justifications have been put forward, but the striking difference remains that the EU Member States have institutions with more than thirty years of experience and production on this task, whereas the US system has deliberately avoided introducing comparable institutional frameworks to the same end.

The "adequacy" criterion

After some forty years of persistent implementation, both the Americans and Europeans will be reluctant to admit its own model's shortcomings. The problem that also led to this analysis is the "gunboat diplomacy" in data protection matters implemented by the EU on this issue. According to a basic EU data protection principle, no personal information may be transmitted from the EU to a third country that does not afford "adequate" protection. This, by all measures, constitutes a problematic approach, whereby Europe practically forces every other country of the world to implement data protection legislation, obviously

along the lines of its own legislation. Such an approach, although it has perhaps failed against such strong opponents as the United States, did not fail in a series of other countries with less negotiating power.

The PNR Agreement is only a minor part in the whole of transatlantic security processing and personal information sharing. The conclusion of any PNR Agreement was, in a way, forced by the United States: unless a text was adopted, European air carriers would probably have lost all of the transatlantic market. It is this pressure that led, and still leads, to the acceptance of a PNR Agreement. The same, however, is not expected to be the case where no pressure exists, where both negotiating parties will be looking back into their own countries and the political heat they will face if any one of them betrays their own models and notions of privacy protection.

IV. CONCLUSIONS FROM THE EXPERT MEETING

During the meeting of experts on 11 December 2006, three issues proved particularly difficult for the EU and United States to agree on. In the context of the transatlantic cooperation in data communication the principles of 1) adequacy, 2) reciprocity and 3) their political underpinnings created serious conflicts among the prospective parties.

Adequacy

The "Adequacy Requirement" as established by the Commission Decision 2004/535/EC demands adequate data protection standards in countries to which the European air carriers' passenger data may be transferred. As seen above, the United States and EU both have rules for data protection, but different legal traditions. Therefore, the European "Adequacy Requirement" constitutes a serious obstacle to the data sharing with the United States. However, it is generally admitted that the former visa procedures requiring Europeans to apply for visas provided almost the same information on the incoming passengers as the current PNR Agreement. Notwithstanding the detriment legal schemes, abandoning the "Adequacy Requirement" can be assessed as a promising measure to enhance the transatlantic cooperation in data communication, especially since the United States would have serious difficulties matching the European adequacy standard.

Reciprocity

Additionally, there is a basic principle of reciprocity in international law, suggesting that the EU could demand the same data from US airlines flying to Europe that the United States demands from European airlines to the United States. However, while the United States wants data on arriving passengers, it does not have a registration requirement for citizens and legal foreign residents, as most European countries do. Therefore, the US legal tradition of a more liberal approach toward personal records could stand against an exchange of data. Consequently, the principle of reciprocity could constitute a serious domestic obstacle for the US government to enter in a mutual data exchange Agreement.

Political Underpinnings

Finally, it has to be emphasized that political reservations rather than substantive legal differences impede a new Agreement on passenger data transfer. Leaving aside the technological development of computer-based data analyses, the former visa procedure stipulated a strict legal regime demanding a full set of personal data in advance of travel to the United States. In fact, the current passenger data transfer is not very different from that. However, the political environment has changed since September 11th. As a result of the US-led war on terror, EU-US relationships have deteriorated, and some European countries question the United States' commitment to human rights. In order to change this, the United States could, for example, show goodwill by including the principles of fundamental human rights and data protection in the preamble of a new Agreement and offer a reciprocal transfer of data to the EU. For European countries, the restrictions on sharing data within the US government conspicuously conflict with the international law principle of reciprocity. This is especially the case, since the European Court of Justice's decision invalidating the first PNR Agreement has led the European public opinion to the conclusion that the missing data protection devices of the Agreement contravened European law (even though the Court did not address this issue in its judgement). Symbolic activities could considerably increase the acceptance of a new Agreement, while the European Union could reconsider the principle of an "adequate" data protection standard as a basis for the Agreement, especially since there are also different data protection standards within the EU. The principle of reciprocity and the Adequacy Requirement constitute two major legal and political obstacles to a revised Agreement on data transfer between the United States and the EU.

In any event, and in view of the forthcoming negotiations between the EU and the United States on a second PNR Agreement, some point of compromise could be achieved that would respect European data protection principles and the need

of American security agencies for as much personal data processing as possible. Such a solution could begin with the wording of the Data Protection Directive, but could then deviate from it, introducing exceptions in those cases where US agencies find this necessary. European law by no means prohibits data processing by security agencies. On the contrary, such processing is allowed but is placed under stricter controls than in the United States. The PNR Agreement need not break new legal grounds; it could place the acquis communautaire at its basis and introduce on top of it those exceptions that shall be deemed necessary during negotiations.

NOTES

1 Council Doc. 13668/06 of 6 October 2006.