EUROPEAN POLICY CENTRE

Policy Brief

June 2007

The King Baudouin Foundation and Compagnia di San Paolo
are strategic partners of the European Policy Centre

Up close and personal: data protection and EU-US relations

By Johnny Pring

Background

Since the terrorist attacks in the United States in 2001, Europe's role in the US-declared "war on terror" has been controversial, and the debate on the appropriate balance to be struck between individual rights and collective security has become more prominent.

This has certainly been the case on the issue of data protection: the row over granting American government security agents access to airline passenger data has highlighted the differences between EU and US standards in this area, and this circle has not yet been squared.

Following the attacks, the US introduced laws requiring airlines operating to, from and over America to provide access to their automated reservation systems – which contain data known as Passenger Name Records (PNR) – to its Bureau of Customs and Border Protection (CBP). This covered not only basic information such as name, date of birth and nationality, but also credit card details, address, telephone number, e-mail, medical data, and even meal choices and membership of frequent flyer programmes.

Failure to comply would result in serious penalties for the airlines, with a loss of landing rights and fines. However, compliance with the legislation would have put European airlines in conflict with the EU's Data Protection Directive.

The key provision here is Article 6.1, which obliges Member States to ensure that personal data processed in the EU is "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with these purposes".

There is a derogation under Article 25 which allows the transfer of data to a third country provided it "ensures an adequate level of protection". However, this "adequacy" is not well defined, and is to be determined "in the light of all the circumstances surrounding a data-transfer operation or set of data-transfer operations". If "adequacy" means the same or similar standards as in the EU, this is not explicitly stated.

Other notable provisions of the Directive include:

- a reference to Article 8 of the European Convention on Human Rights (ECHR), a non-EU instrument, which grants everyone "the right to respect for his private and family life, his home and his correspondence", and states that public authorities shall only interfere with this for reasons such as national security or public safety;
- Article 3.2, which states that the Directive does not apply to any processing of data which takes place outside Community law (i.e. first pillar), such as activities relating to security, defence or crime;
- Article 8, which prohibits the processing of sensitive data such as racial origin, religious or political beliefs, or health, although Member States may make exemptions for reasons of "substantial public interest".

An analysis of the *legality* of the proposed transmission of European PNR data to the US was given in October 2002 by the Article 29 Working Party on Data Protection, an independent European advisory committee set up under the Directive. Regarding Article 25, it said the processing of data transferred to the US federal authorities fell short of the adequacy requirement, as

the relevant US law only protected American citizens' data. It recommended negotiating to establish a system ring-fenced with conditions and guarantees for the processing of European PNR data.

The first deal and its critics

The European Commission and the CBP negotiated throughout 2003 to reach an agreement: in return for access to 34 PNR categories on European airlines' reservation systems, the CBP gave a 48-clause Undertaking (i.e. a non-legally binding promise) on data protection. This agreement was open to criticism on several counts.

Firstly, it was made under the first pillar (EC) rather than third pillar (cooperation in justice and home affairs), with Article 95 of the EC Treaty (the establishment and functioning of the Internal Market) as its legal basis, contrary to the Article 29 Working Party's advice.

Secondly, the content of the agreement and Undertaking provided ample scope for controversy. For example, the 34 data categories, while fewer than originally demanded by the US, exceeded the 19 recommended by the Article 29 Working Party; the number of other agencies to which the CBP could pass the data was apparently open-ended; and EU citizens were not granted data protection rights under US legislation.

The method of data transfer was particularly controversial. The EU granted the CBP direct access to reservation systems to collect this data itself (a 'pull' system) until the airlines established a satisfactory system for them to collect and provide it to the CBP (a 'push' system).

The Article 29 Working Party clearly preferred the 'push' system, as did many MEPs, who regarded US standards as insufficient to protect EU air passengers. Yet the Commission sidelined them during the negotiations and, once these were completed, only asked the European Parliament for a non-binding opinion. In March 2004, the Parliament responded by adopting a resolution which sharply criticised the legal basis for the accord, its non-binding nature on the US authorities and the 'pull' system, and called for a new agreement to be negotiated.

However, the Commission stuck to its guns and the Council approved the negotiated agreement, with some Member States more enthusiastic than others but all generally willing to cooperate with Washington on this issue.

Parliament goes to Court

As it had threatened to do, the Parliament then sought redress in the European Court of Justice (ECJ), and launched twin complaints against the Commission and the Council, on procedural and substantive grounds.

In a joint ruling on both cases in May 2006, the ECJ found in favour of the Parliament and annulled both the Council and Commission Decisions, although it prolonged the EU-US agreement until the end of September 2006. However, in doing so, the Court made only two substantial findings:

- firstly, that the processing of personal data in this case was outside the scope of the Data Protection Directive (as defined in Article 3.2), and therefore the Commission's decision on "adequacy" was as well;
- secondly, because this data processing was not covered by the Directive, Article 95 of the EC Treaty was not an appropriate legal basis for the Council decision.

The Court did not address the rest of the Parliament's complaints, particularly the alleged breach of provisions of the Directive and the ECHR. These therefore remain unanswered legal and political issues, and potential sources of further dispute.

While the ECJ ruling was undoubtedly a short-term political victory for the Parliament, it did not settle the matter. The Commission, supported by the Council, remained determined to press ahead on a similar basis, mindful of the potential legal uncertainty for European airlines operating transatlantic services. Their solution was therefore to conclude an interim agreement with the US, signed in October 2006, which was substantially similar in content but on a different legal basis (third pillar). This agreement runs until the end of July 2007.

The Parliament was excluded from these negotiations too, and a resolution adopted in September 2006 again criticised the Commission's approach.

State of play

The limited nature of the ECJ's ruling means that it remains unclear whether continued transfer of passenger data to the CBP would infringe European citizens' rights under the Data Protection Directive. The Commission has used this uncertainty to argue that there is no infringement.

However, when the Commissioner for Justice, Freedom and Security Franco Frattini spoke at a European Parliament plenary session in December 2006, he adopted a more reassuring tone, stressing that, in future negotiations, the Commission would ensure that the standards agreed were in line with the EU's Charter of Fundamental Rights. Yet this Charter will not be

binding unless it is included in the EU treaty which replaces the ill-fated Constitution (of which it is part) and is ratified. The Commission has also remained silent on Article 8 of the ECHR, which is referred to in the Directive and was one element of the Parliament's complaints to the ECJ.

Other developments have done little to assuage European criticisms of the PNR agreement. In an EU-US Joint Review of the Undertakings in September 2005, EU officials concluded that the CBP had not substantially complied with its commitments until May 2005, and the CBP wanted to maintain some elements of a 'pull' system even after the 'push' system was put in place.

MEPs have also been concerned about the apparent escalation in US demands, such as the length of data retention and the expansion of the purposes for which PNR data may be used to include disease control. In January 2007, they adopted another critical resolution.

While the Commission may have the upper hand – the Parliament cannot negotiate with the Americans – it is ultimately in the more difficult position, as it has to balance its EU commitments with the demands of the US authorities. In February 2007, it began negotiations on the new agreement with Washington, again without involving MEPs.

The bigger picture

Aside from data protection itself, the dispute has brought several broader issues into focus.

Firstly, the EU's credibility as an international negotiating partner has suffered a setback, as the pillar system makes it difficult to conclude legally-watertight agreements. In the PNR dispute, the Commission must take some of the blame for choosing the wrong legal basis.

Secondly, the Parliament has shown itself to be a more awkward transatlantic partner than the Commission and many EU governments, and its reluctance is not just a passing phase. It may not have the legal means to prevent a new agreement, but it can certainly raise the political profile of an issue and stir up European concerns about sovereignty and the protection of rights.

Finally, the whole PNR debate has arguably been as much about EU inter-institutional power play as about the issue itself. It has given the Parliament an opportunity to assert its role as the defender of EU citizens' rights and raise its own profile.

By contrast, the Member States have hidden behind the Commission, which is perceived to have focused much more on accommodating the US than on defending rights.

However, it is doubtful whether the Commission could have done things differently in the face of intense lobbying from European airlines afraid of losing landing slots in the US.

On two other issues, not entirely unrelated, the Parliament has again criticised the EU's attitude towards the US.

The first concerned the allegations of collusion by 14 Member State governments with CIA 'rendition' flights (the extradition of terrorist suspects in EU countries to the US or even, it was claimed, to countries where torture was practised). The Parliament set up a temporary committee to investigate these allegations in January 2006, and narrowly adopted a highly critical resolution in February 2007.

The second was the transfer of data to the US authorities from the Belgium-based SWIFT banking network, which facilitates international financial transfers. In June 2006, it emerged that SWIFT had allowed the CIA access to its data, including transactions involving EU citizens, which appeared to contravene its obligations under the Data Protection Directive. In the face of Parliament protests, the Commission began talks with the US in January to reach a similar agreement as for PNR which would allow the transfer of SWIFT data to continue.

Prospects

The political and legal uncertainty over PNR is set to continue.

The Commission faces an end-of-July deadline to negotiate a new, more permanent agreement with the US, and is in a very difficult position: on the one hand, US Homeland Security Secretary Michael Chertoff sees the current agreement as only a starting point; on the other, the European Parliament has, if anything, hardened its stance, with Mr Chertoff's appearance at a Parliamentary PNR hearing in May 2007 failing to convince many MEPs to support the American approach.

Although MEPs have shown they can make plenty of noise on this issue, it is uncertain whether they would risk another appeal to the ECJ, as there is no guarantee that the Court would support them in a second ruling.

Politically, the Parliament also could find itself at a dead-end if the US authorities start threatening sanctions against European airlines, such as abrogating their

landing rights. If that happens, airlines might simply transfer the data with no agreement in place and therefore with no data protection guarantees for European passengers.

The wider challenge

The data protection controversies over PNR and SWIFT do not stand alone. There are a growing number of security-related initiatives taken at European level with similar implications.

The Prüm Treaty on cooperation in police and criminal matters allows signatory Member States to grant each other automatic access to their police files, creating 'pull' systems between themselves. In February 2007, the Council agreed to incorporate this into the EU's legal framework.

The Council is also discussing a Commission proposal to convert Europol into an official EU agency, which would also enhance its role as a data coordinator; and in November 2006, Eurojust, the EU's judicial cooperation unit, signed an agreement with Washington allowing exchanges of information on cases under investigation.

The existing Schengen Information System (SIS) is being upgraded to include biometric identifiers and link national passport databases, due to be operative by the end of 2008. By this time, nine of the EU's 'new' Member States will have joined the Schengen zone, thus extending the geographical reach of the new database. The parties allowed access to the data will also be expanded.

In December 2006, the Council adopted a Framework Decision on exchange of information between Member States in criminal investigations or intelligence operations, and the Commission has proposed another Council Framework Decision in this area to harmonise access to data in another Member State and the grounds for refusal.

The Data Retention Directive, due to be implemented by March 2009, allows national authorities access to lists of connections made by suspects through mobile phones or the Internet.

Finally, Commissioner Frattini has expressed an interest in 'positive' profiling, whereby passengers would voluntarily submit personal identifying information in advance to avoid more onerous security checks at airports. The Commission has also indicated that it would like to set up a European version of the PNR system.

Options and dilemmas

Such increased cooperation in security matters between EU Member States highlights the different national data protection standards within Europe.

As the EU Directive only covers first-pillar activities, a common third-pillar approach on data protection will be important to avoid similar objections to data exchange between Member States as those raised over PNR transfers to the US.

In October 2005, the Commission therefore proposed a Council Framework Decision on the protection of personal data transferred in the third pillar.

This refers in particular to the Charter of Fundamental Rights' provisions on respect for private and family life and the protection of personal data, and follows, "wherever possible", the principles of the Data Protection Directive. It would effectively allow a 'pull' system to operate between Member States, but in this case, all parties would be subject to the same data protection standards, including judicial guarantees under the relevant national legislation.

Both the Parliament and data protection authorities throughout Europe support this proposal, which is still being discussed by the Council.

More broadly, national and European authorities will continue to face the challenge of dealing with serious threats to security for the foreseeable future.

Access to relevant data is an invaluable tool in combating terrorism and organised crime. Perhaps the inevitable lack of transparency in security-related work inevitably breeds mistrust among those who see their role as protecting the citizen from an overzealous state.

Polarised debate

In the PNR case, Washington's heavy-handed attitude and the exclusion of MEPs from the negotiations, while perhaps a wise decision from the point of view of concluding an agreement rapidly, have only served to polarise the debate.

The increase in intra-European and international cooperation in security matters will, however, keep data protection issues on the front burner.

Johnny Pring is a qualified English lawyer with more than four years of EU public affairs' experience, and holds a summa cum laudae MA in European Studies from the Catholic University of Leuven.

European Policy Centre ■ Résidence Palace, 155 rue de la Loi, 1040 Brussels, Belgium
Tel: + 32 (0)2 231 03 40 ■ Fax: +32 (0)2 231 07 04 ■ Email: info@epc.eu ■ Website: www.epc.eu

With the support of the European Commission