CEPS Policy brief
No. 109 • July 2006

The Political Life of Data

The ECJ Decision on the PNR Agreement between the EU and the US

Elspeth Guild & Evelien Brouwer

On 30 May 2006, the European Court of Justice (ECJ) held that the Passenger Name Records (PNR) Agreement between the EU and the US on the processing and transfer of personal data by air carriers to the US was unlawful. Headlines in the UK's Daily Telegraph indicate the seriousness with which industry has taken the judgment: "EU privacy ruling threatens chaos on flights to US" (31 May 2006). The Financial Times was even more alarmist: "EU airline ruling puts terror deal in doubt". Clearly something important had happened, notwithstanding the fact that the ECJ preserved the application of the two contested measures until 30 September 2006, in order to provide time for a new agreement to be negotiated.

The EU institutions also acted with alacrity: on 19 June the European Commission proposed to the Council that the institutions send a joint letter to the US authorities denouncing the PNR agreement as of 30 September 2006 and enter into a new agreement in the same form but under a new legal base, no longer subject to the European Parliament's effective scrutiny. Anyone who has followed EU affairs will be familiar with the contrast here to the normal, fairly slow approach of the Commission to a perceived need to change a law. Such a rapid reaction indicates the seriousness of the situation.

However, the PNR agreement has not been the only route by which the US authorities have been seeking ways to obtain personal information about EU citizens. The US authorities have also bilaterally negotiated measures to gain access to banking information about EU citizens' transactions and actively opposed further EU measures to protect data subjects. All this activity around personal data evidences serious political differences about the relationship of the individual and the state between the EU and US regarding the collection, storage, use and manipulation of data. So what is the political life of data which has so galvanised both EU and US institutions?

In this briefing paper we will outline:

1. The EU-US agreement – its extent and scope
2. The ECJ judgment – its meaning
3. The wider implications for the architecture of the EU
4. The data protection question
5. Remedies for the aggrieved individual
6. Some recommendations to resolve the structural problems raised by the decision.

We address three critical issues in this note. The first is how the current architecture of the EU is failing to deliver the legal certainty that is critical to the EU's foreign relations and international standing and what needs to be done to improve it; secondly, the European legal norms on data protection and how they should be reconciled in the light of very different US considerations; and thirdly the right of the aggrieved individual to a remedy in the case of illegal data processing.

The EU-US agreement

Since January 2003, European airlines flying into the United States are obliged to provide the US customs authorities with electronic access to the data contained in their automated reservation and departure control systems, referred to as 'Passenger Name Records' (hereinafter 'PNR data'). Based on US laws adopted following the terrorist attacks of 9/11, airline companies should submit these data before or immediately after the airplane takes off. If they fail to do so, they can be fined a maximum of $5,000 for each passenger whose data have not been appropriately transmitted. The PNR data comprise 34 fields of data, including not only name and address, but also contact details such as telephone numbers, email address, information on bank numbers and credits cards, and also on the meals ordered for the flight.

Initially, based on information of the European Commission that this requirement would be in breach of national laws and Community legislation, including the EC Directive 95/46 on data protection and the code of conduct for computerised reservation systems, the US authorities were willing to postpone the entry into force of the new provisions. However, after 5 March 2003, they refused to waive the right to impose penalties on airlines failing to comply with the legislation on electronic access to PNR data. After this date, the European airline companies

Elspeth Guild is Professor at Radboud University Nijmegen and CEPS Senior Research Fellow. Evelien Brouwer is a researcher at Radboud University Nijmegen. They express their thanks to Dr Biao Xiang of Compas of Oxford University for coining the phrase in the title, ' the political life of data'.

found themselves, as expressed at that time by a Member of the European Parliament, 'between a rock and a hard place'. If they conform to the applicable EC rules and refuse US authorities access to the PNR data, they would risk a fine from the US authorities and if they transmit the data in breach of data protection laws, they would risk a fine by the national data protection authorities in the EU. The European Commission tried to escape from this dilemma by adopting, after having negotiated with the US officials, a decision on adequacy based on Article 25 of the EC Directive on data protection. By taking this decision, the Commission expressed its conviction that the US would ensure an adequate level of data protection. This decision enabled the Council to adopt the Agreement of 17 May 2004 between the European Community and the United States of America.

The adoption of this agreement was highly disputed not only because of the disregard of the Council and Commission for the position of the European Parliament, but also because of the widespread concerns for the data protection rights of EU passengers. For example, the European Data Protection Working Party (based on Article 29 of the EC Directive 95/46) repeatedly raised its doubts on the proportionality of transfer of PNR data and on the level of protection as guaranteed in the undertakings of the US Bureau of Customs and Borders Protection (CBP). Other concerns dealt with the fact that the transfer of data was based on a 'pull' instead of 'push' system, which means the US authorities have immediate access to the electronic systems of the airline companies, instead of being dependent on the companies to provide them with the information.[1]

In September 2005, a US-EU team conducted a joint review in Washington, D.C. on the implementation by the US CBP of the Undertakings as set out in the Commission Decision 2004/535 of 14 May 2004.[2] The EU team was composed by Commission officials, a member of OLAF, two representatives of national data protection authorities (Germany and the UK) and law enforcement authorities.[3] In the report on the Joint Review, the EU team expressed its disappointment at the fact that based on "understandable concerns about law enforcement sensitivities", limitations were imposed on the number of records that could be accessed by the EU team and on the provision of hard copy versions of certain staff procedural guidance. This meant, according to the EU team, that the review report was written "in the context of those limitations" and thus should be read in this perspective. The EU team found these limitations particularly regrettable as, according to the report, "all the members of the EU team were required to sign confidentiality agreements exposing them to criminal sanctions for any breach". In general, the EU team found a "substantial" compliance with the Undertakings as of the date of the Joint Review (20 and 21 September 2005). However this has been described as a "late compliance" as the PNR Agreement already entered into force on 28 May 2004. Until mid-May 2005, the EU team concluded that there was not a sufficient degree of compliance. According to the report, the Privacy Office of the Department of Homeland Security could not provide the EU team with concrete reasons why it took CBP such a long time to implement the Undertakings. For example, the EU team found that only on 15 March 2005 the CBP implemented a filtering system for sensitive data and data beyond the maximum of 34 permitted PNR data elements. The EU team recommended to delete permanently the PNR data which were collected by CBP between 28 May 2004 and the date the CBP started to 'filter' the data. The EU team further recommended to provide clearer guidance to CBP officers as to the meaning and interpretation of "serious crimes that are transnational in nature" that form part of the purposes for which the CPB may collect PNR data.

During the Joint Review, the US authorities submitted their intention to retain a sort of 'pull' system even after the change to a 'push' system was agreed upon in the Undertakings. On the basis of this report on the Joint Review, one can conclude that compliance of the US authorities with the agreements as adopted between US authorities and the EC is not a matter-of-course. This is particularly worrying in light of the fact that EU officials assessing the level of US compliance of the Undertakings were not allowed to have full access to the relevant information and were forced to sign confidentiality agreements exposing them to US criminal sanctions for any breach.

The ECJ judgment and its meaning

The European Parliament, which has been marginalised in the rush to adopt the EU-US agreement, commenced proceedings before the ECJ to annul both the agreement between the European Communities and the US on the transfer of PNR data and also the Commission decision on the adequate protection of these data transferred to the Bureau of Customs and Border Protection (the adequacy decision). It had already adopted a strongly worded report by MEP Boogerd-Quaak to this effect expressing doubts about the effectiveness of US data protection norms, but this opinion did not have any apparent effect.[4] In support of the Council, the Commission and the UK intervened. In support of the Parliament, the European Data Protection Supervisor participated formally in the proceedings.

The judgment is very interesting for a number of reasons. The first is that at the very beginning, at paragraph 3, the first effective paragraph of the judgment the Court sets out the provision of the European Convention on Human Rights which states: "everyone has the right for respect for his private and family life, his home and his correspondence". It continued with the second paragraph of Article 8 ECHR – the circumstances in

[1] In the Undertakings between the Commission and US officials, it has been agreed that the 'pull' system would only persist until such time as air carriers are able to implement a system to 'push' the data to CBP. According to promises made to the Commission a full functioning of the 'push' system would be in place by the end of 2005.

[2] Commission Staff Working Paper on the Joint Review, 12.12.2005, revised version (see http://www.statewatch.org/news/2006/jun/eu-usa-pnr-com-review-2005.pdf).

[3] In the delegation list annexed to this document, all the names of these officials have been deleted.

[4] CNS/2004/64, 6 April 2004.

which a state may intervene with the right.

To our knowledge it is unprecedented that the European Court of Justice, the court of the European Union, commences one of its judgments with a reference not to the law of the EU but to an international human rights agreement to which the EU is not even a party (nor has the power to become one at the moment). This is even more surprising in view of the fact that the ECJ does not then return to Article 8 European Convention on Human Rights at all in the judgment! Only one further reference is made to it at paragraph 62 when the ECJ sets out the Parliament's claim in favour of annulment of the EU-US Agreement. One must ask then, what is the Court's intention in setting its whole judgment in the framework of the human right to privacy yet never refers to it specifically?

The European Parliament's key complaint, couched in the words of competence and respect for its prerogatives, is that the EU-US agreement is too wide and constitutes an interference with the individual's right to protection of his or her data. Further, it considers that the Commission's adequacy decision was misguided at best. However, the Court chose to decide the whole case on a much more limited ground – the legal base on which the agreement and decision were founded. It never addressed the issue of the right to privacy and its application to the PNR arrangements, other than by commencing the whole ruling with that right!

The Court held that both the EU-US agreement and the adequacy decision could not have their legal base in EU transport policy (a first pillar provision). Instead, on the basis of a careful reading of the preamble to the EU-US agreement, it found that its purpose is:

a) to enhance security;

b) to fight against terrorism;

c) to prevent and combat terrorism, and related crimes, other serious crimes , including organised crime; and

d) to prevent flight from warrants or custody for those crimes.

On this basis the Court held that the transfer of PNR to the US authorities is a operation concerning public security and the activities of state authorities in the area of criminal law. Thus the Court held that the transfer of data falls within a framework established by the public authorities that relates to public security. For this reason the Court determined that the EC Directive 95/46 on the protection of personal data was not relevant as the two acts are excluded by its Article 3(2), which states that it does not apply to activities in the second and third pillars and "in any case processing operations concerning public security, defence, State security and the activities of the State in areas of criminal law". In view of the fact that the data would only be available to US law enforcement authorities and not EU authorities, this ground is difficult to reconcile with EU competences, the only ones that the ECJ is charged to protect.

So, the EU-US agreement is annulled as is the Commission's adequacy decision, but both on the ground that they are not first-pillar activities within the transport sector but belong elsewhere in the constitutional architecture of the EU. The question then is where do they belong?

The wider implications for the architecture of the EU

The current disarray in EU-US relations on PNR in part arises from the inadequacy of the current EU constitutional structure to provide a clear, precise and transparent legal base for the agreement. The attack by the European Parliament on this ground has resulted in the annulment of the agreement and the adequacy decision. Had the EU Constitutional Treaty been in force, the collapsing of the pillars of the Union would have meant that the incorrect legal base would have been less dramatic. While the Court would still have found that the provision on which the agreement was incorrectly based, a correct legal base would have been present in the same treaty (i.e. the Constitutional Treaty) and the substitution of one legal base for another would have been much easier. The participation of the European Parliament, the application of the EC Directive on data protection and access for the aggrieved individual to a remedy would have remained similar. The 'black hole' of democratic deficit, accountability and protection of the individual would have been more limited.

The PNR problem is a classic example of the extraordinarily complicated and ultimately untenable structure under which the EU currently operates. That an international agreement and adequacy decision could be founded on the wrong part of the EU structure and thus, after two years of operation be held to be illegal is highly frustrating for all involved, including the US. It bites at the principle of certainty of law and the effectiveness of the EU as a negotiating partner in international relations.

However, the lack of support for the EU Constitution expressed by the negative referenda results in France and the Netherlands in May and June 2005, has meant that the reconstruction of the EU architecture has not gone ahead. The latest decision of the Council has been to extend the period of reflection for a further 12 months for the member states to consider the future. Notwithstanding this period of reflection, however, a number of member states have ratified the Constitutional Treaty since the French and Dutch referenda, indicating a positive approach at least in some parts of the Union.

The choice of the third pillar – matters of policing and criminal law – for the new PNR agreement is not without problems. For one, in the third pillar the Parliament has even less voice than in the first pillar, so the result would be that the Parliament is effectively cut out of the picture. In the third pillar, there is highly heterogeneous control by the ECJ as its jurisdiction over third-pillar matters depends on whether each member state has made a declaration permitting its national courts (and not necessarily courts at the same level) to refer questions to the ECJ on third pillar issues. Some member states permit even first instance courts to refer third pillar questions to the ECJ (for instance Italy) whereas others permit no access to the Court (for instance the UK).[5] In any

[5] See the table on declarations of EU Member States accepting the jurisdiction of the ECJ in the third pillar in: Elspeth Guild and Sergio Carrera, *No Constitutional Treaty?*

event, the ECJ's finding that the exclusion provision in Article 3(2) of the data protection directive applies to the PNR agreement and the adequacy decision also has the effect of cutting the ECJ itself out of the picture, notwithstanding the heterogeneous rules of access to that court.

No matter how one looks at it, the current situation is rather messy and unsatisfactory. The President of the Commission, Barroso has mentioned in an increasing number of speeches from May 2006, that the EU needs to use the passerelle provision of Article 42 Treaty on European Union to transfer the whole field of the third pillar into the first pillar (at Title IV EC). It remains to be seen whether this proposal will be taken up and if so by whom. The Commission has also used the possibility of bringing actions before the Court challenging measures on the ground that the legal base use is unlawful as regards various Council acts in the second and third pillars, claiming that since there is competence for them to be adopted in the first pillar, they must be adopted there. The most surprising of these actions is that in respect of the second pillar, where the Commission claims that a measure on small arms and light weapons adopted in the common foreign and security policy should have been adopted under the provisions of the ACP Agreement with countries in Africa, the Caribbean and Pacific.[6]

By itself, though, the collapsing of the first and third pillar might not be enough. While it would bring any future PNR decision within the first pillar and thus subject to the data protection directive, as the Court stated, the exception in that directive on public security, defence, State security and activities of the State in areas of criminal law applied, so the individual's data might still not be subject to data protection. But, the Constitutional Treaty is not limited to the collapsing of the pillars; it also introduces the EU Charter of Fundamental Rights as a legally binding part of the EU framework. This means that the right to data protection as included in the Charter would be part of EU law and provide the individual with a right against unlawful data collection, transmission and manipulation. Thus, in order to resolve the PNR issues regarding protection of the individual's data, in addition to the collapsing of the pillars, the EU also needs to give legally binding effect to the Charter in order to overcome the obstacles that the PNR decision has raised.

Data protection

The final choice for the legal basis of the PNR decision is extremely important, because in instances where there is an error or illegal activity, the data protection rights of the individual whose information has been collected, transferred, manipulated, and further transmitted depend critically on the legal status of the acts. If the European settlement on the right of the individual in respect of his or her personal data is higher than the US counterpart (which all parties agree), the individual in Europe will want to have European protection against manipulation of his or her data and not US protection which will be much lower. But this will depend on whether EU law which regulates the transmission of data is subject to European norms which the individual can access.

It is disappointing that in this judgment, the ECJ on the one hand concluded that the collection of PNR data by the airlines falls within the scope of Community law and on the other hand seemed to accept that if the same data are to be transferred for public security reasons they no longer need the protection of the EC data protection directive. This conclusion, if accepted, will have much broader implications. For instance, it would mean that the transmission of information to third countries or organisations from the future Visa Information System or data on third-country nationals stored in SIS II (Schengen Information System) would escape the applicable rules of the EC directive on data protection, as long as this transmission is intended for police or public security use. In his initial reaction to the PNR judgment, the European Data Protection Supervisor, Mr. Hustinx, appropriately concluded that this reasoning of the ECJ would create a loophole in the protection of citizens. In this light, the PNR judgment contrasts with the more liberal approach of the ECJ in its earlier judgment in the Österreichischer Rundfunk case.[7] In this judgment, the ECJ explicitly declared that the applicability of the data protection Directive has to be interpreted broadly and should not be limited to data processing which is directly linked to the freedoms of free movement as protected in the EC Treaty.

The paramount importance of data protection for every individual has been confirmed by its insertion as a fundamental right in the EU Charter on Fundamental Rights. In its explanatory memorandum to the proposal for a Framework Decision on third pillar data protection, the European Commission affirmed this by stating that the EC Directive 95/46 on data protection contains fundamental rules on the lawfulness of data processing as on the rights of data subjects.[8] According to the Commission, these fundamental principles should apply to data processing in the first and in the third pillar. Member states cannot simply circumvent principles, such as purpose limitation and the procedural guarantees as included in the EC Directive, by adopting rules that permit the use of first pillar information for third pillar purposes.

In the Österreichischer Rundfunk case, the ECJ also referred to the applicability of Article 8 ECHR in relation to data processing in general. This means that the lawfulness of those decisions should be considered against the background of Article 8 ECHR. It is to be doubted whether the transmission of the extensive list of personal data to US authorities and the uncertainty about the future use of this information will pass the test of the criteria which have been developed by the European Court of Human Rights on the basis of Article 8 ECHR.[9] So here the start of the judgment becomes somewhat clearer. If the EU data protection Directive does not apply to the PNR agreement because the directive is first pillar and the agreement is somewhere in a

Implications for the Area of Freedom, Security and Justice, CEPS, October 2005.

[6] C-91/05.

[7] Joined cases C-465/00, C-138/01 and C-139/01.

[8] COM (2005) 475.

[9] See for example Rotaru v Romania, 4 May 2000, appl. no. 28341/95 and the recent Segerstedt-Wiberg & ors v Sweden, 6 June 2006, appl.no. 62332/00.

common foreign and security policy (second pillar) or policing and cooperation in criminal matters (third pillar), the norm that applies will be the European human rights norm of the right to privacy contained in Article 8 of the ECHR.

What about the individual?

At the heart of the concerns about the transfer of data within the structure of the EU and EU-US relations is the justified concern of the EU to protect its citizens' and residents' rights. How can the individual make sure that his or her data are properly collected, transferred and only used for lawful purposes in accordance with EU (and ECHR) standards of the right of privacy and data protection? The problem raised by the PNR decision of the ECJ is what will happen to the aggrieved individual? Let us take the imaginary example of Mr Ali Mohammed, a Spanish national who seeks to board a plane from Madrid to New York. Let us say Mr Mohammed was born in Morocco and naturalised as a Spanish citizen five years ago. His data are transmitted to the US authorities in accordance with a new PNR agreement, made on the basis of the third pillar as it correctly stands. The US authorities, erroneously confusing Mr Mohammed with another Mr Mohammed who is on one of their terrorist lists, advise the airline to refuse him access to the plane which it does. As a result, the business meeting he was to have attended is cancelled and the multi-million euro deal falls through. Does Mr Mohammed have any remedy against what has happened to him, which (again let us suppose) all agree is the result of a negligent mistake?

Under the rules applicable to air travel, it is very unlikely that he will have a cause of action against the airline on the basis of breach of contract. Because his data were transmitted in accordance with the agreement, the airline company is protected against a breach of contract claim.[10] It would be a matter of US law as to whether he would have an action against the US authorities. He might potentially have the possibility to sue the EU institutions (within the time limits) under Article 230 EC claiming that his individual rights are directly affected by the agreement with the US. However, the scope of Article 230 has been very narrowly interpreted by the ECJ and it is very much of a long shot, considering that in any event he would have to sue within two months of the publication of the measure.

Finally, Mr Mohammed would be able to take his case to the European Court of Human Rights in an action against Spain for permitting the transmission of his data unlawfully and contrary to his right to respect for his private life under Article 8 ECHR. Should the European Court of Human Rights find in his favour, then the whole EU-US system would once again be condemned, this time for a failure to protect human rights. Such a decision would be even more problematic for the architecture of the EU than the ECJ's decision on PNR. However, this possible legal action is the only one that is not surrounded by question marks as to whether Mr Mohammed could in fact access it. But, this remedy is outside EU law. The lack of clear accessible EU remedies for passengers against the transmission and use of their personal information is difficult to reconcile with the generally accepted principle that everyone whose rights under EU law have been violated should have an effective remedy: a principle that is repeatedly confirmed in the judgments of the ECJ and inserted in Article 47 of the EU Charter on Fundamental Rights.[11]

An isolated issue?

The issue of the transfer of PNR data to US authorities is not unique. US authorities obtain, or are trying to obtain, access to personal data of EU citizens and persons residing in the EU in more than one way. Of course, the most recent example is the revelation of the fact that since 2001, US authorities, including the CIA, have been allowed access to confidential information on international banking transfers of EU customers held by the Belgian bank consortium SWIFT.[12] The initial statements from a spokesperson of the European Commission and the Belgian government that this transfer of personal data does not fall either within the ambit of the EC Directive or the Belgian data protection law constitute a clear and alarming example of the actual gap in data protection.

During the EU-US informal High Level meeting on Freedom, Security and Justice on 2-3 March 2006, in Vienna, the US officials mentioned, in the context of fighting terrorists' use of the Internet, that they were "considering approaching each Member State to ensure that the data collected on the basis of the recently adopted Directive on data retention would be accessible to them".[13] During the same meeting the US officials warned against the adoption of the draft framework decision on the protection of personal data in the third pillar. The US delegation expressed its concerns about the "negative impact of the draft framework decision on data protection on its bilateral relations with Member States if it was to be adopted in its present form". This concern regarded the draft Article 15 of the proposal which includes special requirements with regard to the transfer of data to authorities in third countries or to international bodies. This example in fact demonstrates the need for the EU legislator to provide uniform and stringent rules with regard to the transmission of personal data to third countries and that the level of this protection should not be determined by US counterparts.

The framework decision on data protection in the third pillar is a step forward in providing a certain level of protection in the field of police and judicial cooperation. Still, it is questionable whether the 'loophole' of data protection, as described above, will be solved by a swift adoption of this proposal. Instead of reinforcing the rights of individuals, this proposal still seems more focused on extending the possibilities for transmitting personal information to other authorities and authorities in third countries. Further, the adoption of this Framework

[10] It may be open to the individual, however, to start an action with the purpose of seeking the national judge to make a preliminary reference to the ECJ on whether the data transmission and effects were lawful.

[11] Johnston v Chief Constable of the RUC, C-222/84; Panayotova, C-327/02.

[12] Eric Lichtblau and James Risen, "Bank Data Sifted in Secret by U.S. to Block Terror", *The New York Times*, 23 June 2006.

[13] EU Council, Report of the EU-US informal High Level meeting on Freedom, Security and Justice on 2-3 March 2006 in Vienna (http://www.statewatch.org/news/2006/apr/eu-us-jha-7618-06.pdf).

Decision will not change the lack of competence for the ECJ to assess the lawfulness and proportionality of the data processing involved. A more appropriate solution would be to extend the applicability of the EC Directive on data protection to the whole field covered by EU law by amending Article 3(2) to provide more strictly for the exceptions. It might be necessary to provide for more specified rules for concrete situations, but the basic principles as provided in the EC Directive should be considered as a minimum level of data protection. The rights contained therein should only be restricted in accordance with these principles and the criteria as developed on the basis of Article 8 ECHR. Finally, the EU Charter needs to be given legal effect so that the rights of privacy and data protection contained in it can provide a legal basis for the balancing of the individual's rights against the state's interest in access to and use of the data.

Some recommendations to resolve the problems raised by the decision

Architectural solutions

The best option is for the member states to ratify the Constitutional Treaty immediately. This would both collapse the pillar structure and insert the Charter of Fundamental Rights into the heart of the EU structure as legally binding, thereby protecting data as a fundamental right. The next best option would be for the Council to agree to a rapid use of Article 42 TEU to move the third pillar into the first pillar and thus create one streamlined structure for the two pillars. Whether this will be possible remains to be seen. This action would solve both the problem of the legality of the measure and the applicability of the data protection Directive. It would not solve the problem of the adequacy of the data protection Directive, for which, a legally binding EU Charter on Fundamental Rights would be necessary as well.

Remedies for the individual

If the architectural solutions are adopted (either the ratification of the Constitution or the collapsing of the pillars combined with legal force to the Charter), the individual would come within the normal rules of EU legal remedies. He or she would be able to start an action in the national court against the national authorities on the basis of the data protection Directive which requires that the individual has a legal remedy for any breach of the rights guaranteed by the applicable national law. Alternatively, if the matter still falls within the Directive´s exceptions, his claim could be based on the right to privacy and data protection in the Charter. If the national judge was in doubt about the use of the data at stake, then he or she could refer the matter to the ECJ via the preliminary proceedings based on 234 EC. Without the Constitution, the narrow interpretation of Article 230 EC makes a direct action of the individual before the ECJ against the decision of the Council and the Commission not a likely solution. However, the ECJ could widen its interpretation of that provision to permit a recourse in this situation. A solution within the EU, however, is highly desirably as the alternative is the potentially very damaging possibility of a judgment from the European Court of Human Rights striking down an EU-US agreement on human rights grounds.

However one looks at the PNR issue and beyond it to the different philosophies of the EU and US on data protection, the issue is now firmly on the political agenda. The legal constraints of the EU, tied up with a European understanding of human rights as encompassing the right of the individual to control of his or her data, lead inexorably to conflict with the US authorities, which consider data as the property of the individual or authority which collects them. Data have acquired a political life of their own, which has opened new fissures in EU-US relations.