Passenger Name Record Agreement

European Court of Justice

Annulment of Commission Adequacy Decision and Council Decision Concerning Conclusion of Passenger Name Record Agreement with US Grand Chamber Judgment of 30 May 2006, Joined cases C-317/04 and C-318/04, *European Parliament* v. *Council and Commission*

Mario Mendez*

Introduction

On 30 May 2006, the European Court of Justice handed down a significant judgment, which, amongst other things, attests to the continuing complications posed by the European Union's Byzantine pillar structure. At issue was a Commission adequacy decision, in the Data Protection Directive framework,[1] which recognised the US as providing an adequate level of protection for the transfer of Passenger Name Record (PNR) data and the related first pillar international agreement. The adequacy decision and the Council decision concerning conclusion of the agreement both were annulled because the personal data processing at issue was outside the Directive's scope, concerning as it did public security and State activities in the areas of criminal law. The judgment thus offers important clarification as to what is subject to first pillar data protection standards, and its ramifications will be felt well beyond the PNR field. The European Union now has concluded a new international agreement with the US under the third pillar which, to the discredit of the European negotiators, is even more questionable on fundamental rights grounds than its predecessor. Whilst the standards of the Data Protection Directive do not apply to this third pillar measure, ECHR standards remain applicable, and it is possible that, unlike in its first judgment, the European Court of Justice may find itself unable to avoid pronouncing on whether this new Agreement meets the standards articulated by the Strasbourg Court.

* Researcher, European University Institute, Florence.

[1] Directive 95/46/EC, *OJ* [1995] L 281/31.

European Constitutional Law Review, 3: 127–147, 2007

doi: 101017/S1574019607001277

Legal and factual background

In the wake of the 11 September attacks, the US passed legislation requiring airlines flying into US territory to transfer various types of data concerning passengers and crew to the Bureau of Customs and Border Protection (CBP).[2] An implementing regulation followed requiring the airlines to provide CBP with electronic access to PNR data,[3] a particularly expansive category, which can include amongst other things payment information, e-mail address, frequent-flyer information, meal preferences and special health requirements. Failure to comply could lead to substantial fines and the potential loss of landing rights.

The Commission informed the US in June 2002 of the possible conflict these rules would create with, *inter alia*, the Data Protection Directive, which subject to various exceptions only permits data transfers to a third country which 'ensures an adequate level of protection'.[4] The US takes a radically different approach to privacy and data protection, which is characterised in the private sector by its sectoral and piecemeal nature and its heavy reliance on industry self-regulation.[5] In October 2002, the Data Protection Working Party, a body composed of national data protection authority representatives set up under the Data Protection Directive, issued an Opinion pointing to numerous compatibility problems.[6] Commission and US officials met in Brussels in February 2003 and produced a 'joint statement' containing 'undertakings' as to data handling as well as several 'understandings'.[7] It specified that they would work towards a bilateral arrangement under which an 'adequacy decision' – a Commission finding within the Data Protection Directive framework that a third country ensures an adequate level of protection[8] – would be adopted. It also stated that the Commission 'considered that EU data protection authorities may not find it necessary to take enforcement actions against airlines complying with the US requirements.' It thus appeared to give the green light to airlines to ignore any incompatibility that US requirements, due to apply from 5 March 2003, would pose with respect to data

[2] *See* the Aviation and Transportation Security Act, 19 Nov. 2001, Public Law 107-71, Title 49 US Code, section 44909(c)(3)) and the interim implementing regulation Passenger and Crew Manifests Required for Passenger Flights in Foreign Air Transportation to the United States, *Federal Register*, 31 Dec. 2001.

[3] Passenger Name Record Information Required for Passengers on Flights in Foreign Air Transportation to or from the United States, *Federal Register*, 25 June 2002.

[4] *Supra* n. 1, Art. 25(1).

[5] For an overview *see* G. Shaffer, 'Globalization and social protection: the impact of EU and international rules in the ratcheting up of U.S. privacy standards', 25 *Yale Journal of International Law* (2000) p. 1 at p. 22-28.

[6] Opinion 6/2002, 24 Oct. 2002.

[7] *See* <http://ec.europa.eu/comm/external_relations/us/intro/pnr-joint03_1702.htm>.

[8] *Supra* n. 1, Art. 25(6).

protection obligations and to indicate that national data protection authorities should not pursue any resulting breaches. That the guardian of the Treaties put its name to such a document is striking indeed, not least since the Charter of Fundamental Rights contained an express provision on data protection (Article 8), and the Convention was busy reproducing it in the draft Constitution. It is not surprising that the European Parliament responded with a resolution chiding the Commission.[9]

The ongoing negotiations produced a set of 'undertakings' in May 2003,[10] which were the subject of critical evaluation by the Data Protection Working Party.[11] A censorious European Parliament resolution also followed in October 2003.[12] In December, the Commission issued a Communication emphasising the many concessions gained and stated that the procedures for adopting an adequacy decision and concluding an international agreement would be launched.[13] The concessions, however, did not satisfy the Data Protection Working Party, which issued a very critical opinion on the updated undertakings asserting, amongst other things, that without a 'push system', whereby the airlines transfer the data as contrasted with the 'pull system' that gives CBP direct access to airline databases, no adequacy could be assumed.[14]

On 1 March 2004, despite the stance of the Data Protection Working Party and a strong rebuke from a European Parliament committee,[15] the Commission placed a draft adequacy decision and draft undertakings before the Parliament, which was soon followed by a proposal for a Council decision concerning conclusion of the Agreement. The Parliament responded with a resolution calling upon the Commission to withdraw the draft decision and underscored its willingness to pursue legal action,[16] which it put into practice on 21 April 2004 by seeking an Article 300(6) opinion. Notwithstanding the absence of the Parliament's opinion, the Council adopted the decision concluding the Agreement on 17 May 2004,[17] the Commission having adopted the adequacy decision three days earlier.[18] The Agreement was signed on 28 May 2004 and entered into force that day. The

[9] P5_TA(2003)0097, *OJ* [2004] C 61E/381.

[10] Available at <http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2003_en.htm>.

[11] Opinion 4/2003, 13 June 2003.

[12] P5_TA(2003)0429, *OJ* [2003] C 81E/105.

[13] COM(2003)826, 16.12.2003.

[14] Opinion 2/2004, 29 Jan. 2004.

[15] A5-0104/2004, 24 Feb. 2004, a resolution adopted on 9 March, P5_TA(2004)0141, *OJ* [2004] C 102E/147.

[16] P5_TA(2004)0245, 31 March 2004.

[17] Decision 2004/496/EC, *OJ* [2004] L 183/83.

[18] Decision 2004/535/EC, *OJ* [2004] L 235/11.

Parliament accordingly withdrew its request for an Opinion and brought legal challenges under Article 230.[19] The cases were joined with the UK supporting the Council and Commission and the European Data Protection Supervisor supporting the European Parliament.[20]

Opinion of Advocate-General Léger[21]

In addressing the first plea that the adequacy decision infringed the Data Protection Directive, the Advocate-General held that only if a third country transfer concerns personal data processing falling within the Directive's scope can an adequacy decision constitute an implementing measure.[22] It was underlined that:

> 96. … [t]he first indent of Article 3(2) of Directive 95/46 provides that the directive does not apply to the processing of personal data 'in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and *in any case to processing operations concerning public security*, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and *the activities of the State in areas of criminal law*'. [footnote omitted]

The Advocate-General considered that the consultation, availability and CBP use of data located within member states' territory constituted personal-data processing operations concerning public security and related to State activities in areas of criminal law excluded from its scope and invoked several recitals of the adequacy decision as demonstrating the aforementioned purpose.[23] The adequacy decision concerned a data processing operation 'regarded as necessary to safeguard public security and for law-enforcement purposes' and the fact that the data were collected in the course of a business activity could not justify applying the Directive in an area excluded from its scope.[24] Accordingly, the Commission did not have the power under Article 25 'to adopt a decision on the adequate protection of personal data transferred *in the course* and *for the purpose* of a processing operation expressly excluded from the scope of that directive' and the decision must be annulled.[25]

[19] Cases C-317/04 and C-318/04, 27 July 2004.

[20] The leave granted to the European Data Protection Supervisor is significant because of the Council arguments that were rejected: *see* Orders of the Court, 17 March 2005.

[21] Opinion of Advocate-General Léger, delivered 22 Nov. 2005.

[22] Ibid., para. 95.

[23] Paras. 97-99.

[24] Para. 103.

[25] Paras. 104-105.

The analysis of the Council decision began with a lengthy section finding the first plea, alleging that Article 95 EC was an incorrect legal basis, well founded in the light of the agreement's aim and content.[26] Looking first at the aim, he found, relying on preamble recitals, that it simultaneously pursued two objectives: on the one hand, combating terrorism and other serious crimes and, on the other, respecting fundamental rights.[27] Turning to its content, several paragraphs were found to confirm this analysis.[28] Equipped with these conclusions, he rejected the arguments advanced in defence of Article 95 as the correct legal basis.[29]

Having concluded that the Council decision should be annulled, the Advocate-General made some remarks as to an appropriate legal basis and the nature of the PNR regime.[30] He noted that a measure providing for consultation and the use of personal data by an entity tasked with ensuring a State's internal security could be treated as an act of co-operation between public authorities and that, in this context, the third pillar is sometimes mentioned. It was underlined that '[i]t is the compulsory disclosure of data for security and law-enforcement purposes that is important, and not the specific form it takes in any given situation.'

The Advocate-General then dispensed with the alleged infringement of Article 300(3),[31] and turned to the pleas concerning a breach of fundamental rights and proportionality, which also were invoked in the adequacy decision challenge and which he opted to assess together.[32] The right to protection of personal data was considered to constitute an aspect of the right to respect for private life protected by Article 8 ECHR via the prism of the general principles of law in the Community legal order.[33] Applying the two-fold approach stemming from Article 8 ECHR, the conclusion that there was an interference with private life was reached in a few sentences.[34]

The first two prongs of the due justification test, whether the interference is in accordance with the law and whether a legitimate aim is pursued, were quickly dealt with.[35] With respect to the first, he found that airlines and their passengers – by reading the Council decision, the annexed agreement, the adequacy decision and the annexed undertakings – 'can be informed with sufficient precision for the purpose of regulating their conduct'. As to the second prong, the interference was

[26] Paras. 126-156.
[27] Paras. 129-133.
[28] Paras. 134-138.
[29] Paras. 141-155.
[30] Paras. 157-161.
[31] Paras. 177-190.
[32] Paras. 193-262.
[33] Para. 209.
[34] Paras. 211-213.
[35] Paras. 215-224.

https://doi.org/10.1017/S1574019607001277 Published online by Cambridge University Press

considered to pursue a legitimate aim particularly with regard to combating terrorism, whilst combating other serious crimes also was considered to fall within several legitimate interests.

Turning to the crucial third prong – whether the interference is necessary in a democratic society for the purposes of achieving the legitimate aims – Advocate-General Léger commenced by proffering some thoughts as to the scope of review.[36] ECHR case-law was invoked in support of the proposition that where the aim of interference is to maintain national security or combat terrorism, States are allowed a wide margin of appreciation. The Council, he continued, should have a wide margin of appreciation given the nature and importance of the objective of combating terrorism and the politically sensitive context in which the negotiations were conducted. Accordingly, review should be limited to determining whether there was a manifest error of assessment.

The actual review began with the Advocate-General invoking several provisions of the Agreement and adequacy decision in rejecting the assertion that the undertakings are not binding.[37] He then addressed the argument that the amount of data is excessive and also may include sensitive data.[38] Three observations were made in support of the proposition that the Commission did not agree to a manifestly inappropriate measure:

1) The importance of intelligence activity in counter-terrorism.
2) The fact that other EU information exchange instruments provide for less data disclosure is not sufficient to demonstrate the PNR regime is excessive.
3) The undertakings strictly limit access to, preclude use of, and filter sensitive data.

The argument that the data retention period is excessive fared equally badly.[39] The period was considered not manifestly excessive 'bearing in mind … that, as the Council points out, investigations which may be conducted following terrorist attacks or other serious crimes sometimes last several years.' It was necessary 'to consider the period of storage of data from PNR in light of their usefulness, not only for purposes of preventing terrorism but, more widely, for law-enforcement purposes.'

As to the alleged absence of judicial review, the Advocate-General responded that the undertakings provided a series of safeguards (in terms of information, data access and remedies), which rendered the interference in private life proportionate to the legitimate aims.[40] He also rejected the argument that the discretion

[36] Paras. 225-233.
[37] Paras. 235-236.
[38] Paras. 237-239.
[39] Para. 242.
[40] Paras. 245-254.

to transfer the data to other public authorities, including foreign government authorities, goes beyond what is necessary to combat terrorism and other serious crimes.[41] Advocate-General Léger stressed that such a transfer can only be carried out on a case-by-case basis for limited purposes 'largely linked to the legitimate aim pursued by the PNR regime' and that there are a number of safeguards.

Finally, the Advocate-General dispensed with the pleas alleging an infringement of the duty to state reasons and that the Council acted in breach of the duty under Article 10 to co-operate in good faith in the procedure for adopting the Agreement.[42]

Judgment of the European Court of Justice

With respect to the adequacy decision, the Court commenced with the alleged infringement of the first indent of Article 3(2). It recalled the subject-matter excluded from the Directive's scope and continued:

> 55 The decision on adequacy concerns only PNR data transferred to CBP. It is apparent from the sixth recital… that the requirements for that transfer are based on a statute enacted by the United States …. According to the seventh recital … the United States legislation in question concerns the enhancement of security and the conditions under which persons may enter and leave the country. The eighth recital states that the Community is fully committed to supporting the United States in the fight against terrorism within the limits imposed by Community law. The 15th recital states that PNR data will be used strictly for purposes of preventing and combating terrorism and related crimes, other serious crimes, including organised crime, that are transnational in nature, and flight from warrants or custody for those crimes.
>
> 56 It follows that the transfer of PNR data to CBP constitutes processing operations concerning public security and the activities of the State in areas of criminal law.

The Court recognised that the data were collected initially in the course of an activity falling within the scope of Community law, but the data processing taken into account in the adequacy decision was quite different in nature concerning 'data processing regarded as necessary for safeguarding public security and for law-enforcement purposes.'[43] The Court reiterated the finding in *Lindqvist,*[44]

[41] Paras. 255-260.
[42] Paras. 263-281.
[43] Para. 57.
[44] Case C-101/01 *Lindqvist* [2003] *ECR* I-12971, para. 43.

that the activities mentioned in the first indent of Article 3(2) are 'activities of the State or of State authorities and unrelated to the fields of activity of individuals', but held that:

> 58 …. this does not mean that, because the PNR data have been collected by private operators for commercial purposes and it is they who arrange for their transfer to a third country, the transfer in question is not covered by that provision. The transfer falls within a framework established by the public authorities that relates to public security.

The adequacy decision was held to concern data processing within the first indent of Article 3(2) and thus outside the Directive's scope, it was therefore annulled without it being necessary to address the other pleas.[45]

Turning to the Council Decision, the European Court of Justice promptly accepted the first plea and annulled the Decision again without considering it necessary to address the remaining pleas:

> 67 Article 95 EC, read in conjunction with Article 25 of the Directive, cannot justify Community competence to conclude the Agreement.
>
> 68 The Agreement relates to the same transfer of data as the decision on adequacy and therefore to data processing operations which…are excluded from the scope of the Directive.
>
> 69 Consequently, Decision 2004/496 cannot have been validly adopted on the basis of Article 95 EC.

The Court however went on to limit the effects of its judgment.[46] It noted that the Agreement provided that either party could terminate at any time and this would take effect 90 days after notification, but that CBP's right of access to PNR data and the airlines processing obligation only existed for as long as the adequacy decision was applicable. The Court continued:

> 73 Given, first, the fact that the Community cannot rely on its own law as justification for not fulfilling the Agreement which remains applicable during the period of 90 days from termination thereof and, second, the close link that exists between the Agreement and the decision on adequacy, it appears justified, for reasons of legal certainty and in order to protect the persons concerned, to preserve the effect of the decision on adequacy during that same period. In addition, account should be taken of the period needed for the adoption of the measures necessary to comply with this judgment.

[45] Paras. 59-61.
[46] Paras. 71-74.

The European Court of Justice therefore preserved the adequacy decision's effect until 30 September 2006 but not beyond when the agreement comes to an end.

Commentary

Consequences for EU data protection

The PNR judgment will have serious ramifications for data protection in the European Union. This follows from what it tells us about the scope of the Data Protection Directive. A data processing operation outside its scope, as laid down in Article 3(2), remains so even if the data were initially processed within the scope of Community law. And although Article 3(2) has been held to be unrelated to the field of activity of individuals, where data processing takes place within a framework established by public authorities pertaining to an area excluded from the Directive's scope, then it will be caught by Article 3(2). This is the essence of what the Court has to say on the Directive's scope, and the alternative on both counts would have emptied Article 3(2) of meaning.

To be sure, in the run up to the conclusion of the Agreement, few would have suspected that the outcome of this case would actually turn on Article 3(2), as direct references were non-existent and references to the third pillar were few and far between.[47] The Data Protection Working Party did underline the need for the third pillar context to be incorporated in its Opinion 6/2002,[48] but this was not pursued in later Opinions. It was not until the litigation stage that the European Parliament saw fit to invoke Article 3(2). There was of course little incentive to run such an argument during the negotiations. If a third pillar international agreement rather than the Data Protection Directive were viewed as the applicable framework, the European Parliament and the Commission would see their roles reduced and the European Court of Justice's jurisdiction curtailed. More concessions were no doubt obtained precisely because the negotiations took place on the assumption that the Data Protection Directive was the operating background norm. Admittedly, the US was uncompromising, and the end product was riddled with data protection shortcomings, but the US surely would have been even more intransigent had it not been faced with the rules in the Directive. This could well explain why it does not seem possible to find any discussion of Article 3(2) prior to the European Parliament bringing the legal challenges.

In terms of the consequences of the judgment, first and foremost, it constitutes a rejection of the EU approach to bilateral PNR negotiations. The Commission

[47] *See* however M.V. Pérez Asinari and Y. Poullet, 'Données des voyageurs aériens: le débat Europe – Etats-Unis', 113 *Journal des Tribunaux – Droit Européen* (2004) p. 266 at p. 269.

[48] *Supra* n. 6.

https://doi.org/10.1017/S1574019607001277 Published online by Cambridge University Press

has noted that it will take due consideration of the judgment in its ongoing negotiations with Australia.[49] As for the PNR Agreement concluded with Canada shortly before the judgment, this is no longer legally sound given that it also was based on an adequacy decision and a Community Agreement, which has Article 95 EC as its legal basis.[50] The Agreement allows for unilateral termination,[51] but as of late October, this does not appear to have been exercised.

The judgment also calls into question the legal base employed for the Data Retention Directive,[52] and may well have provided the impetus for Ireland's challenge.[53] It is useful briefly to recall the background to its adoption. In April 2004, France, Ireland, Sweden and the UK introduced a proposal for a draft framework decision under Title VI EU Treaty, which, essentially for the purposes of crime prevention and prosecution, would impose harmonised data retention obligations on electronic communications service providers.[54] But first the Commission, and then the European Parliament Committee on Legal Affairs,[55] later joined by the Council legal service,[56] responded that harmonisation of data to be retained and the retention period should be adopted under Article 95 EC, and that the proposed framework decision would affect the provisions of the Directive on Privacy and Electronic Communications[57] which would constitute a breach of Article 47 EU Treaty. Harmonisation accordingly took place via a Directive with Article 95 EC as its legal basis. The Court in the PNR judgment simply ruled out Article 95 as a legal basis for data processing outside the Data Protection Directive's scope. If we transpose this reasoning then even if the data were initially collected in the course of an activity falling within the scope of Community law, namely the provision of services, the retention obligation arguably requires further processing operations that are 'quite different in nature', concerning as they do 'data processing regarded as necessary for … law enforcement purposes'. The directive relates to data processing operations that, to use the combined language of Article 3(2) of the Data Protection Directive, Article 1(3) of the Directive on Privacy and Electronic Communications and the PNR judgment, fall within a framework established by the public authorities that relates to the activities of the State in areas of criminal law. This is the type of argument that is likely to be employed and if

[49] COM(2006) 333, 28.6.2006.

[50] Decision 2006/230/EC, *OJ* [2006] L 82/14.

[51] Ibid, Art. 9(3).

[52] Directive 2006/24/EC, *OJ* [2006] L 105/54.

[53] Case C-301/06 *Ireland* v. *Council and European Parliament*, pending.

[54] 8958/04 CRIMORG 36 TELECOM 82, 28.04.2004.

[55] *See* respectively SEC(2005) 420, 22.3.2005, and Committee on Legal Affairs Opinion 31 March 2005 attached to A6-0174/2005, 31.5.2005.

[56] 7688/05 JUR 137 COPEN 62 TELECOM 21, 05.04.2005.

[57] Directive 2002/58/EC, *OJ* [2002] L 20/37.

successful may lead to the Directive having to be replaced with a third pillar measure that will potentially be even less sensitive to data protection concerns.

The PNR judgment is therefore certain to be criticised for creating a loophole in the protection offered by Community law data protection standards. However, this is a shortcoming that is not of the Court's making but is rather a consequence of the current constitutional architecture of the Union. The inapplicability of Community law data protection standards to matters outside the scope of Community law[58] has become an especially controversial issue in the wake of the terrorist attacks in the US and Europe, which have given rise to the adoption of measures with negative repercussions for data protection.[59] This has generated ever more forceful calls for the adoption of an overarching third pillar data protection measure based on the Data Protection Directive standards, which eventually led to a Commission proposal for a framework decision on personal data processing in the police and judicial co-operation framework.[60] It was welcomed by the European Parliament,[61] the European Data Protection Supervisor,[62] and the Conference of European Data Protection Authorities,[63] all of which, however, proposed substantial amendments. Were the Decision adopted with the amendments proposed, then the gap between first and third pillar data protection standards would have been significantly reduced, which may have blunted criticism of the PNR judgment. As it is, however, it appears that a Council Working Group is significantly watering down the data protection standards.[64] So instead of going some way towards harmonising personal data protection standards, the Decision looks likely to set in stone sharply divergent standards.

Limitation of effects of the judgment

Before proceeding to what has happened with the US PNR regime, it is worth briefly exploring the limitation of the effects of the judgment. This is the seventh occasion, to this author's knowledge, on which the Court has annulled acts con-

[58] In most member states the legislation implementing the Data Protection Directive also covers processing in the area of law enforcement: *see* European Data Protection Supervisor Opinion *infra* n. 62, para. 4.

[59] For example, the Mutual Legal Assistance Agreement concluded with the US, *see* Council Decision 2003/516, *OJ* [2003] L 181/35.

[60] COM(2005) 475, 4.10.2005.

[61] *See* A6-0192/2006, 18.5.2006. (A draft resolution adopted in Sept. 2006).

[62] *OJ* [2006] C 47/27.

[63] Opinion adopted 24 Jan. 2006.

[64] T. Bunyan, 'EU data protection in police and judicial cooperation matters: Rights of suspects and defendants under attack by law enforcement demands', *Statewatch Analysis*, Oct. 2006, available at <http://www.statewatch.org/news/2006/oct/eu-dp.pdf>.

cerning the conclusion of an international agreement. In the first and third cases, the Court did not limit the effects,[65] whilst in the second it did but it concerned an expired international agreement.[66] In the wake of these cases, two interpretations were proffered. According to the first interpretation, the annulment eliminates the agreement *ex tunc* from Community law.[67] According to the second interpretation, '[i]t is…incorrect to take the view that the treaty can no longer have effects under internal Community law (because its conclusion has been declared void)…'.[68] No light was shed on this issue in the fourth judgment, which annulled the relevant Council decision without limiting the effects.[69] In the fifth judgment in 2003, two Council decisions concerning the conclusion of transport agreements were annulled.[70] The Court, however, limited the effects, explaining that this was 'in order to avoid any legal uncertainty as regards the applicability of the international commitments entered into by the Community within the Community's legal order.'[71] Then in early 2006, the Court annulled the Council decision concerning approval of the Rotterdam Convention without limiting the effects of its judgment.[72] However, in the companion case, the Regulation implementing the Convention was annulled, but the avoidance of legal uncertainty was invoked to justify preserving its effects.[73] In this sense, the case can be distinguished from the 2003 transport judgment. In the PNR judgment, however, the Court only expressly preserved the effect of the adequacy decision. The logic may well have been that there was no need to preserve the Council decision given that as a matter of international law the Agreement in any event remained binding.[74] But would this not create legal uncertainty 'as regards the applicability of the international commitments entered into by the Community within the Community's legal order'? In addition, if no such legal uncertainty is created here, why would it have been created in the factual matrix pertaining to its 2003 judgment?

[65] Case C-327/91 *France* v. *Commission* [1994] *ECR* I-3641 and Case C-122/95 *Germany* v. *Council* [1998] *ECR* I-973.

[66] Case C-360/93 *European Parliament* v. *Council* [1996] *ECR* I-1195.

[67] P.J.G. Kapteyn, 'Quelques réflexions sur le contrôle de la constitutionnalité des accords conclus par la Communauté avec des pays tiers', in G.C. Rodríguez Iglesias, et al. (eds.), *Mélanges en hommage à Fernand Schockweiler* (Nomos, Baden-Baden 1999) p. 275 at p. 282-283.

[68] P.J. Kuijper, 'The Court and the Tribunal of the EC and the Vienna Convention on the Law of Treaties 1969', 25 *Legal Issues of Economic Integration* (1998) p. 1 at p. 13

[69] Case C-281/01 *Commission* v. *Council* [2002] *ECR* I-2049.

[70] Case C-211/01 *Commission* v. *Council* [2003] *ECR* I-8913.

[71] Ibid, para. 57.

[72] Case C-94/03 *Commission* v. *Council*, judgment 10 Jan. 2006.

[73] Case C-178/03 *Commission* v. *Parliament and Council*, judgment 10 Jan. 2006.

[74] *See* Art. 27 of the 1969 and 1986 Vienna Conventions on the Law of Treaties. The 1986 Convention has not entered into force and the Community is not a party but it has been cited by the Court: *see* Case C-344/04 *IATA*, judgment 10 Jan. 2006, para. 40.

The effects of the adequacy decision, by contrast, need to be expressly preserved because if it is no longer 'applicable', then the CBP loses its access right and the airlines would no longer be under a data processing obligation. However, the Community, so paragraph 73 seems to read, cannot rely (as a matter of international law) on the annulment of the adequacy decision (or the Council decision) for not fulfilling the Agreement. It might be argued that it should be able to, because the Agreement itself expressly links the application of Articles 1 and 2 to the applicability of the adequacy decision and as the decision is being annulled it is no longer 'applicable'. This argument turns on how we interpret 'for so long as the Decision is applicable'. It could be assumed that the intention was to link the agreement's lifetime to expiry of the adequacy decision, which had been set at three and a half years.[75] However the parties chose clearly broader language. The explanation is likely to be the fact that the Data Protection Directive can be used to repeal and suspend the adequacy decision.[76] Were this to take place, an argument that the Community is breaching its obligations would surely fail, due to the so long as applicable proviso. The Canada PNR Agreement expressly provides that certain obligations are to 'apply for as long as the Decision is applicable, ceasing to have effect on the date that the Decision is repealed, suspended or expires without being renewed.'[77] This raises at least two points. Firstly, it is clear that if the international agreement so provides, internal law can determine the content of international obligations and where internal law changes – repeal, suspension or expiry of the adequacy decision in the express terms of the Canada Agreement – so can the international obligations. In this respect, it is necessary to be careful as to what is meant by not being able to rely on your own law as justification for not fulfilling the agreement. The second point is whether the 'so long as applicable' language indeed can be said to include annulment. For the sake of argument, we can assume that the Canada Agreement provides an exhaustive definition, but no such further explanation is provided in the US Agreement.

A related issue concerns the fact that there is an important exception to the rule that internal law cannot be invoked as justification for failure to perform. As a matter of international law, the Community could rely on its own law invalidating its consent to be bound where that consent was expressed in manifest violation of a provision of its internal law of fundamental importance regarding the competence to conclude Treaties.[78] The Court has never expressly addressed this

[75] *Supra* n. 18, Art. 7.
[76] Ibid., Art. 4(3).
[77] *Supra* n. 50, Art. 5(2).
[78] *See* Art. 46 of the 1969 and 1986 Vienna Conventions.

issue,[79] and it undoubtedly makes for a very exacting standard.[80] One wonders however whether in theory there was scope for this argument given that the Agreement as pursued, and indeed the Agreement as concluded, clearly posed problems of a constitutional nature for the Community.

The new PNR Agreement

Moving on to the steps taken in the wake of the judgment, the Parliament's victory indeed did turn out to be a Pyrrhic one. Notice of termination was duly given and negotiations commenced on a third pillar agreement with Articles 24 and 38 EU Treaty as its legal base, the European Parliament's calls for use of the *passerelle* not being heeded. The negotiations were not concluded until a week after the original agreement had been terminated, and the provisional entry into force did not take place until the process of signatures was completed on 19 October 2006.[81] Thus, for some 18 days, there was no legal basis for the transfers and airlines were back in a similar position to that which they had been in prior to the entry into force of the original agreement, either they breach their own data protection law by allowing continued electronic access or they prevent such access and face potential penalties and loss of landing rights.

The new regime is a considerable retreat from its predecessor. The first thing that becomes apparent is that it is now the Department of Homeland Security (DHS) that is given electronic access to the data,[82] whereas previously it had only been the CBP.[83] The preamble states that for the purposes of the agreement, the DHS means the CBP, 'US Immigration and Customs Enforcement and the Office of the Secretary and the entities that directly support it, but does not include other components … such as the Citizenship and Immigration Services, Transportation Security Administration, United States Secret Service, the United States Coast Guard, and the Federal Emergency Management Agency.' In short, this constitutes a massive expansion of the DHS components entitled to direct electronic access to the data.

A further major related coup for the US pertains to data sharing and disclosure. Transfer to other authorities was governed by paragraphs 28-35 of the undertakings, which imposed various limitations. Paragraph 35 however provided that the undertakings 'did not impede the use or disclosure of PNR data in any

[79] *See* however Advocate-General Lenz in Case 165/87 *Commission* v. *Council* [1988] *ECR* 5545, para 35.

[80] *See* A. Aust, *Modern Treaty Law and Practice* (Cambridge, Cambridge University Press 2000) chapter 17 in general and especially at p. 253.

[81] Decision 2006/729/CFSP/JHA, *OJ* [2006] L298/27 (Agreement attached).

[82] Para. 2, ibid.

[83] Para. 28 of the undertakings (subject to CAPPS II use).

criminal judicial proceedings or as otherwise required by law' and that the Commission would be advised of any legislation materially affecting the statements made in the undertakings. The European Union now has been informed of such legislation in a letter setting out the DHS's interpretation of various provisions of the undertakings.[84] The letter explains that a 2005 Presidential Executive Order directed the DHS and other agencies promptly to give access to terrorism information to the head of every agency with counterterrorism functions.[85] This law would be impeded by the transfer provisions and so they essentially all give way.

The letter is disturbing for numerous other reasons. Firstly, it is used to consult the European Union within the meaning of paragraph 7 of the undertakings as to the addition of data elements, in this case in the frequent-flyer data set and perhaps, though it is unclear on this point, the number of bags carried by a passenger.

Secondly, it is used to renege on the commitment to the annual review in paragraph 43 of the undertakings. Although paragraph 4 of the Agreement provides that its implementation 'shall be jointly and regularly reviewed', the letter states that 'the question of how and *whether* to conduct a joint review in 2007 will be addressed during the discussions regarding a future agreement'. [emphasis added]

Thirdly, the letter offers a reinterpretation of paragraph 34, which provided that the undertakings did not impede data use or disclosure where 'necessary for the protection of the vital interests of the data subject or of other persons, in particular as regards significant heath risks'. The letter considers that it authorizes data access 'in the context of infectious diseases and other risks to passengers'. The term 'other risks' is particularly problematic given its open-ended nature. The letter also expands upon 'vital interests', considered to encompass 'circumstances in which the lives of the data subject or of others could be at stake and includes access to information necessary to ensure that those who may carry or may have been exposed to a dangerous communicable disease can be readily identified, located, and informed without delay.' This should be considered in light of the fact that the Centre for Disease Control, a component of the US Department of Health, had already been gaining access to the data by virtue of a secret agreement concluded in October 2005.[86] The DHS is in effect providing a reading that allows it to defend its data sharing with the Centre for Disease Control.

Fourthly, the reinterpretation of when data can be pulled or pushed provides further cause for concern. Paragraph 14 provided that data would be pulled no earlier than 72 hours prior to departure, subject to the 'unusual event' of CBP obtaining advance information that person(s) of specific concern were on the

[84] *OJ* [2006] C 259/1.

[85] The legislation is referred to in the preamble of the Agreement.

[86] The agreement was released following a freedom of information request by the American Civil Liberties Union in April 2006: *see* <www.aclu.org/privacy/spying/25335prs20060425.html>.

flights, in which case the data could be pulled or a push requested prior to the 72 hour period 'when essential to combat an offense enumerated in paragraph 3'.[87] The letter states that 'while there are instances in which the U.S. government may have specific information regarding a particular threat, in most instances the available intelligence is less definitive and may require the casting of a broader net to try and uncover both the nature of the threat and the persons involved'. It then proceeds to water down the paragraph 14 requirements: It is no longer 'advance information' that is needed, merely an 'indication'; the data does not have to be 'essential' but simply 'likely to assist' and this is no longer tied strictly to the purpose limitation in paragraph 3,[88] but can relate to 'circumstances associated with [these] offenses'.

Fifthly, it places further obstacles in the way of a move to a push system and as to the type of push system. Paragraph 13 provided that the pull system was only to be used until airlines were able to implement a push system. During the negotiations of the new agreement, the European Parliament[89] and the Data Protection Working Party[90] had called for a move to the push system as the technical requirements had been in place for some time. The new agreement however provides that the DHS will have electronic access 'until there is a satisfactory system in place allowing for transmission of such data'.[91] The proviso of 'satisfactory', or 'as soon as practicable', as the letter puts it, will make it easy for the US to continue to renege on an express requirement of the undertakings. Were however a push system to be implemented, the letter tells us that this 'does not confer on airlines discretion to decide when, how or what data to push…[t]hat decision is conferred on DHS by U.S. law.' The letter also asserts that a push system had to be designed to 'permit any PNR data in the airline reservation or departure control system to be pushed to DHS in exceptional circumstances where augmented disclosure is strictly necessary to address a threat to the vital interests of the data subject or other persons.' The DHS, in other words, will not let a push system restrict its access to data elements over and above those stipulated in the Undertakings.

Finally, the most disconcerting aspect is the position taken with respect to data retention. It is pointed out that the Agreement will expire prior to the undertakings requiring destruction of any data (31 July 2007, assuming it is not extended). Having emphasized the importance of the data in identifying links among terror-

[87] The relevant offenses are reiterated in recital 15 to the adequacy decision cited in para. 55 of the judgment above.

[88] Ibid.

[89] A6-0252/2006, 19.7.2006.

[90] Opinion 5/2006, 14 June 2006.

[91] Para. 2, *supra* n. 81.

ist suspects even when over three and a half years old, the letter states that the 'questions of *whether* and when to destroy PNR data' [emphasis added] will be addressed as part of future discussions. This is shocking indeed. Put simply, the European Union can be held to ransom in future negotiations as to previously collected data. From the US standpoint, this would also apply to all the data collected during the lifetime of the original Agreement given that it expired prior to the requirements to delete or destroy having kicked in.

The Council's response, whilst paying lip service to fundamental rights, was to acknowledge that the commitments to continue to implement the undertakings allow it to deem that the DHS ensures an adequate level of data protection.[92] It is true that some of the US 'gains' were already provided for in the undertakings, and if we want to play the Council's game, we can say that the DHS thus is still committed to implementing them. But is this really meaningful considering, for example, that the whole transfer regime is trumped by US law and that it can unilaterally expand the data elements? It is merely confirmation of the patent shortcomings of the original regime. And in any case, other 'gains' are the product of reinterpretations that either expressly renege on the undertakings or are strongly inconsistent with the express wording.

Fundamental rights

All these developments become very significant when we turn to a fundamental rights analysis. This is crucial because we could see a challenge brought in a domestic court for breach of fundamental rights, and if brought in a member state, which has accepted the European Court of Justice's jurisdiction, then the Court may have to pronounce on whether the Agreement satisfies fundamental rights standards.[93] Interference is manifest so we can turn directly to justification under Article 8(2).[94] There is a strong argument to be made here that the interference is not in accordance with law. ECHR case-law requires not only that the impugned measure should have some basis in domestic law but that it 'also relates to the quality of the law, requiring it to be compatible with the rule of law'.[95] The law should be accessible to the person concerned who must be able to foresee its consequences for him.[96] The original PNR regime was composed of the adequacy

[92] *OJ* [2006] C 259/4.

[93] The European Court of Justice would need to accept that the Council Decision on the signing of the Agreement constitutes a decision within the meaning of Art. 34(2)(c) EU Treaty, which it thus has jurisdiction over under Art. 35(1) EU Treaty.

[94] For the ECHR test, *see*, e.g., ECtHR 4 May 2000, App. 28341/95, *Rotaru* v. *Romania*, para. 48 et seq.; ECtHR 16 Feb. 2000, App. 27798/95, *Amann* v. *Switzerland*, para. 46 et seq.

[95] *See* ECtHR 30 July 1998, App. 27671/95, *Valenzuela* v. *Spain*, para. 46. *See also Amann*, ibid., at paras. 50 et seq. and *Rotaru*, ibid., paras. 52 et seq.

[96] *Valenzuela*, ibid.

decision, an international agreement, undertakings, domestic US legislative measures and their implementing regulations. This web has become considerably more complex given the new US legislation and the relevant Presidential executive order. But unless you read the DHS letter, you would not be aware of which provisions of the undertakings are considered inapplicable in the context of third party transfers, and even reading the letter, leaves the reader confused. Then there are the reinterpretations, to say nothing of the disgraceful position advanced to the effect that the data retention period will be up for future discussion. If this were not enough, the web can become denser still should the US pass further legislation within the context of paragraph 35 or should the DHS decide at its discretion that it wants access to more data under paragraph 7. The new Agreement actually refers to the European Union's 'reliance upon DHS's continued implementation of the … Undertakings as interpreted in the light of subsequent events.'[97] Thus, the proposition advanced by Advocate-General Léger that the undertakings 'contain the essential information on the procedure for the use of data by CBP and on the safeguards to which that procedure is subject'[98] was unconvincing then and even more so now. Furthermore, the undertakings are not even binding law. They explicitly state, as do the 2004 and 2006 Agreements, that they do not create or confer any rights or benefits. In short, the rule of law is thoroughly absent here, and to the extent that we actually have accessible 'law', it certainly will not be possible to foresee the consequences.

Even if we assume that the legitimacy of the aims is unproblematic, the requirement that the interference is necessary in a democratic society to achieve those aims poses a host of problems. Advocate-General Léger commenced by invoking ECHR case-law allowing states a wide margin of appreciation in the national security and terrorism context.[99] But there are complications with simply transposing this to the US PNR regime. It is not just about combating terrorism, as the purpose limitation takes us well beyond terrorism; and in any case that purpose limitation is emptied of meaning by virtue of provisions such as paragraphs 34-35. Moreover the scope of the margin of appreciation depends 'not only on the nature of the legitimate aim pursued but also on the particular nature of the interference involved'.[100] The Advocate-General however decides on a standard of manifest error of assessment without considering the nature of the interference. And if the nature of the interference was not problematic enough when

[97] *Supra* n. 81, para. 1.

[98] *Supra* n. 21, para. 218.

[99] Relying in particular on ECtHR 26 March 1987, App. 9248/81, *Leander* v. *Sweden*; ECtHR 28 Oct. 1994, App. 14310/88, *Murray* v. *The United Kingdom*.

[100] *See Leander*, ibid., para. 59.

he visited the issue, it has become considerably more so since. In sum, justifying a wide margin of appreciation is no easy task.

The first major question that needs to be asked is why a pull system is necessary? If the technical requirements for a push system have been in place for some time, as the European Parliament and Data Protection Working Party claim, why are we still no nearer to its implementation? This is a particularly important issue with respect to sensitive data as well as the number of data elements. Obviously, the ideal way to guarantee that only access to stipulated data elements is provided, and that sensitive data access is curtailed, is by having the airlines push only the permitted data. Accordingly, it does not appear proportionate to the legitimate aim pursued to have a pull system, not least given that the Canada Agreement is predicated on the push system. And it is certainly not proportionate for the when, how and what data to push to be determined at US discretion as articulated in the letter.

As to the number of data elements, the inclusion of those permitting transfer of sensitive data is problematic. Deleting data based on sensitive terms does not guarantee the deletion of all sensitive data.[101] Moreover, twenty of the data elements have been considered disproportionate by the Data Protection Working Party.[102] The Advocate-General defended the 34 data elements listed, but it is clear that this list is not even fixed as the undertakings permit the CBP, and now the DHS, to expand the list. Furthermore, the Canada regime also negotiated in the counter terrorism context, and giving access to 25 data elements could be invoked as evidence against the need for the 34 data elements and beyond that is conceded to the US.

A further major problem, brushed aside by the Advocate-General in a single paragraph, concerns the data retention period.[103] Can it really be considered proportionate to retain the data of millions of individuals for a minimum of three and a half years simply because the Council asserts that investigations 'sometimes' last several years? To make matters worse, when data has been manually accessed, the period is increased by eight years. The Advocate-General underlines that we need to consider the data storage period in light of its usefulness for law-enforcement purposes. But this simply will not do. If that were the case, we could further expand the retention period and the PNR data set, throw in more sensitive data, and fall back on the usefulness for law-enforcement purposes. Such may be the US approach to these matters, but it is not going to satisfy ECHR standards. Moreover, having sought to reduce the scope of review by relying on the predomi-

[101] *See supra* n. 14.
[102] Ibid.
[103] *Supra* n. 21, para. 242.

nant aim of combating terrorism, is it not then inconsistent to try and justify a lengthy data retention period by having recourse to its usefulness for unspecified law-enforcement purposes? The original criticism of the Data Protection Working Party on the extended retention period holds, namely, that it 'is disproportionate insofar as it is not related to a concrete investigation or warrant on the data subject.'[104] Sadly, it may end up being some achievement if the European Union can even get the DHS to abide by the undertakings given that the latter does not consider itself bound by the data retention period.

The absence of a strict purpose limitation is also a major problem. If the legitimate aims are the fight against terrorism and other serious crimes, how are those aims served by the use or disclosure that can take place under paragraphs 34-35? Is the disclosure of data pertaining to vital interests of the data subject or others necessary to the fight against terrorism or serious crime? It is difficult to see how the Advocate-General could conclude that such purposes were largely linked to the legitimate aims of the PNR regime. The data sharing with the Centre for Disease Control only came to light recently, but it is testimony to the free reign the US considers itself to have. The 2006 regime only lets standards deteriorate further.

A final crucial issue concerns the importance of safeguards against abuse, which has been underlined by the Strasbourg Court.[105] Advocate-General Léger accordingly responded in the language of the Strasbourg Court. But was it credible to talk of safeguards in the context of third party transfers given paragraphs 34-35 of the undertakings? The 2006 regime makes the emptiness of those safeguards painfully clear. As for the DHS Chief Privacy Officer, this is no independent authority.[106] The holder is appointed by, and reports to, the DHS Secretary.[107] Despite its mandate requiring an annual report to Congress, it had produced only one through to October 2006, which in any event was reported to have gone through the Secretary's office before being made public.[108] Even more troubling is the

[104] *Supra* n. 14.

[105] *See*, e.g., *Leander*, *supra* n. 99 and ECtHR 6 Sept. 1978, App. 5029/71, *Klass* v. *Germany*. This requirement has also been considered in the context of whether interferences are in accordance with law: *see Rotaru*, *supra* n. 94; ECtHR 24 April 1990, App. 1105/84 *Huvig* v. *France* and App. 11801/85 *Kruslin* v. *France*.

[106] The Advocate-General referred to the Officer as having 'some degree of independence' (para. 253).

[107] *See* M. Rotenberg, 'The Sui Generis Privacy Agency: How the United States Institutionalized Privacy Oversight After 9-11', Sept. 2006, p. 36 available at SSRN: <http://ssrn.com/abstract=933690>.

[108] *See* D. Hughes, Sidelining Homeland Security's Privacy Chief, April 11 2005, CNET NEWS.COM available at <http://news.com.com/Sidelining+Homeland+Securitys+privacy+chief/2010-1071_3-5660795.html>.

allegation that it is being 'continually hampered in its investigations by non-cooperation within the DHS'.[109] A DHS lawyer has also pointed out that, although the Privacy Officer is required to investigate privacy violation complaints, the Officer does not have subpoena authority and therefore must rely on voluntary submissions of information in order to conduct investigations.[110] How in such circumstances can we expect abuse to be investigated, much less prevented? Independent supervision has become a basic tenet of European data protection law, and it is thoroughly compromised where personal data is processed by the DHS, to say nothing of what might take place where access is given to third agencies. Even the joint review has not been ensured, which makes it even more difficult to identify problems thus compromising the various circumstances that can justify suspension of data flows or even the Agreement.[111]

Conclusion

The PNR drama with the US is far from concluded. The latest regime is liable to be challenged for breaching fundamental rights standards, and as the analysis presented above suggests, it is difficult to envisage how it could realistically be considered to satisfy the ECHR criteria. Indeed, it actually is difficult to imagine that an Agreement could be any more intrusive and subject to fewer safeguards. To be sure, we need to acknowledge that the Commission and the Presidency found themselves in a difficult position, faced with an intransigent Administration that has become obsessed with its 'War on Terror'. But even if this was the best deal that the US was willing to countenance, its acceptance on the European side makes a mockery of the Union's commitment to respect fundamental rights. In the forthcoming negotiations, our representatives would do well to heed the warning of the Strasbourg Court: 'The Court, being aware of the danger … of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate.'[112]

[109] Rotenberg, *supra* n. 107, p. 34.
[110] Cited in Hughes, *supra* n. 108.
[111] *See* recital 3, Arts. 4 and 5, *supra* n. 81.
[112] *Klass*, *supra* n. 105, para. 49.

https://doi.org/10.1017/S1574019607001277 Published online by Cambridge University Press