HOUSE OF LORDS

European Union Committee

21st Report of Session 2006–07

The EU/US Passenger Name Record (PNR) Agreement

Report with Evidence

Ordered to be printed 22 May 2007 and published 5 June 2007

Published by the Authority of the House of Lords

London : The Stationery Office Limited
£price

HL Paper 108

The European Union Committee

The European Union Committee is appointed by the House of Lords "to consider European Union documents and other matters relating to the European Union". The Committee has seven Sub-Committees which are:
Economic and Financial Affairs and International Trade (Sub-Committee A)
Internal Market (Sub-Committee B)
Foreign Affairs, Defence and Development Policy (Sub-Committee C)
Environment and Agriculture (Sub-Committee D)
Law and Institutions (Sub-Committee E)
Home Affairs (Sub-Committee F)
Social and Consumer Affairs (Sub-Committee G)

Our Membership

The Members of the European Union Committee are:

Lord Blackwell
Lord Bowness
Lord Brown of Eaton-under-Heywood
Baroness Cohen of Pimlico
Lord Freeman
Lord Geddes
Lord Grenfell (Chairman)
Lord Harrison
Lord Kerr of Kinlochard
Lord Maclennan of Rogart
Lord Marlesford
Lord Powell of Bayswater
Lord Roper
Lord Sewel
Baroness Symons of Vernham Dean
Baroness Thomas of Walliswood
Lord Tomlinson
Lord Wright of Richmond

The Members of the Sub-Committee which carried out this inquiry (Sub-Committee F) (Home Affairs) are:

Baroness Bonham-Carter of Yarnbury
Earl of Caithness
Baroness D'Souza
Lord Foulkes of Cumnock
Lord Harrison
Baroness Henig
Lord Jopling
Earl of Listowel
Lord Marlesford
Lord Teverson
Lord Wright of Richmond (Chairman)

Information about the Committee

The reports and evidence of the Committee are published by and available from The Stationery Office. For information freely available on the web, our homepage is:
http://www.parliament.uk/parliamentary_committees/lords_eu_select_committee.cfm
There you will find many of our publications, along with press notices, details of membership and forthcoming meetings, and other information about the ongoing work of the Committee and its Sub-Committees, each of which has its own homepage.

General Information

General information about the House of Lords and its Committees, including guidance to witnesses, details of current inquiries and forthcoming meetings is on the internet at
http://www.parliament.uk/about_lords/about_lords.cfm

Contacts for the European Union Committee

Contact details for individual Sub-Committees are given on the website.
General correspondence should be addressed to the Clerk of the European Union Committee, Committee Office, House of Lords, London, SW1A OPW
The telephone number for general enquiries is 020 7219 5791.
The Committee's email address is euclords@parliament.uk

CONTENTS

ORAL EVIDENCE

WRITTEN EVIDENCE

NOTE:
References in the text of the Report are as follows:
(Q) refers to a question in oral evidence
(p) refers to a page of written evidence

FOREWORD—What this report is about

In recent years, and particularly since 9/11, counter-terrorism has made it essential for States to monitor and control flights into, out of and over their territory. For this they need detailed information about passengers and crew on those flights. Much of the information relied on by States is collected by the airlines—the Passenger Name Record (PNR).

The United States is exceptional in the number of air passengers who seek entry, the risks which they pose (or are seen as posing), and hence the volume of PNR data sought and the uses to which they are put. Many passengers will not be aware that very detailed information about them is transferred to the US authorities every time they fly there; if they are aware, they may think this is a small price to pay for enhanced security. But some may regard this as a potentially serious abuse of their right to privacy and to protection of their personal data. They may feel, as we do, that a better balance can be struck between public security and private rights.

The first agreement between the EU and the United States, in 2004, was an attempt to reconcile the public security demand for information with the EU laws on data protection. A second interim agreement was negotiated in 2006 after the first was annulled by the European Court of Justice. Now a third agreement is under negotiation.

We hope these negotiations will reach a successful conclusion and will result in an agreement satisfactory to both sides. We have examined the failings of the earlier agreements in detail to suggest how they could be remedied. Our recommendations stress above all the importance of the undertakings governing the collection, use, retention and transfer of data being clear, unequivocal and not susceptible of unilateral amendment.

On behalf of the EU, the negotiators are the Presidency and the Commission. But the United Kingdom Government cannot abrogate their responsibility. They have agreed the negotiating mandate, and they have influence with the United States. They have a duty to see that a satisfactory result is achieved.

The EU/US Passenger Name Record (PNR) Agreement

CHAPTER 1: INTRODUCTION

1. The terrorist attacks of 11 September 2001 in New York and Washington DC have led to major changes in the way security matters are handled throughout the Western world, and not least of course in the United States. The need to monitor and control internal flights, and international flights into, out of and over the United States has required the collection and analysis of vastly greater quantities of data relating to passengers on those aircraft. The principal beneficiary is the United States, but other beneficiaries are the passengers and crew on those aircraft, and a significant proportion of these are of course nationals and residents of the United Kingdom and of other Member States of the European Union.

2. The United States Government and other governments have long been using passenger lists to screen travellers and persons already on watch lists, or in whom they have some other interest, before they depart on a journey. Since 9/11 the focus has shifted to thwarting potential terrorists who are so far unidentified by using more of the detailed information collected by airlines and travel agencies when an individual books a flight. These Passenger Name Records (PNR) contain information, such as travel itineraries and payment details, that can be analysed in conjunction with current intelligence to identify high-risk travellers before they board their planes.

3. If this information is collected accurately, analysed correctly, and its use limited to counter-terrorism, few would challenge the need for this or its desirability. The problems arise when more information is collected than is needed for this purpose, standards of accuracy slip, and the information is shared with those not responsible for counter-terrorism and is used for other purposes.

4. The Final Report of the 9/11 Commission, published in 2004, identified a reluctance by different security authorities to share information with one another as one of the main causes of the failure to prevent the terrorist attacks, and made a number of recommendations to counter this. But the 9/11 Commission also recommended:

> "As the President determines the guidelines for information sharing among government agencies and by those agencies with the private sector, he should safeguard the privacy of individuals about whom information is shared."

5. **It is this perennial conflict between the security of the public and the privacy of the individuals who make up the public which is at the heart of our inquiry. A balance has to be struck, and the guiding consideration must be the principle of proportionality: the collection and retention of data for security purposes must be no more invasive of individual privacy than is necessary to achieve the objective for which they are collected. That objective must be narrowly and clearly defined.**

6. We sought the views of a number of persons and bodies on these issues. We took oral evidence from Ministers, we heard the views of persons speaking on behalf of interested organisations, and we visited Brussels to take evidence. We also had a useful meeting with officials of the United States Embassy. To all of these we are most grateful.

7. The timing of this inquiry is important. Negotiations are in progress for the conclusion of a new Agreement between the EU and the United States on Passenger Name Records (PNR), and we hope that this report may influence the content of the Agreement.

8. **We recommend this report to the House for debate.**

CHAPTER 2: PASSENGER NAME RECORDS

Developments in the United States after 9/11

9. The 9/11 Commission identified in detail the failures of communication between the various different US authorities responsible, but the fact that there had been such failures was apparent within days. On 20 September 2001 the President, by administrative action, created an Office of Homeland Security, one of whose major functions was to coordinate the relevant responsibilities of those authorities. This became the Department of Homeland Security (DHS) the following year.

10. The Aviation and Transportation Security Act of 2001, adopted on 19 November 2001, gave the Bureau of Customs and Border Protection (CBP), within what is now the DHS, and the Transportation Security Administration (TSA) authority to require access to Passenger Name Record data. PNR is an extensive data set held in airline computers when a travel reservation is made. CBP uses PNR for border screening, and TSA needs PNR for passenger pre-screening.

11. Information derived from PNR data is to be contrasted with information from the Advance Passenger Information System (APIS). APIS simply allows the country of destination to access at the time of departure of a flight information about the identities of passengers which it would otherwise receive on the arrival of the passengers. This basic information is held on the airlines' own departure control systems; it is mostly derived from the machine-readable sections of passports, and it includes:

- passport number;
- country which issued passport;
- passport expiry date;
- given names (as they appear on the passport);
- last name;
- gender;
- date of birth;
- nationality.

The PNR data elements

12. PNR by contrast includes data from which aspects of the passenger's history, conduct and behaviour can be deduced. In evidence to the House of Representatives about the negotiations with the EU, TSA said that PNR "can contain as many as 60 data fields or separate pieces of information." These include:

- address, email address and contact telephone;
- travel agency and agent, billing address and form of payment;
- seat number and seat information;
- frequent flyer information;
- general remarks;
- OSI (Other Service-related Information);
- SSI/SSR (Special Service Information/Special Service Requests).

13. We received evidence, some of it conflicting, on the accuracy and reliability of PNR data. Professor Elspeth Guild, giving evidence on behalf of the Centre

for European Policy Studies, made the point that "the quality of data which is collected for commercial purposes, the standards which are applied, are very different from those which are required for law enforcement …" (Q 95) It followed that the larger the number of data elements which were included, the greater the risk of inaccuracy. (Q 97) We have no difficulty accepting that, if there is a given probability of inaccuracy in a single data element, then the more data elements collected, the greater the likelihood of an inaccuracy. But it seems to us that the greater the amount of data collected, the better the chance that between them they will identify the individual accurately, even if some of the data relating to him or her are inaccurate. This was confirmed by Jonathan Faull, the head of the Commission Directorate General on Justice, Freedom and Security (JLS): "They [the Americans] would say that the more PNR you have, the lower the risk of making mistakes."(Q 143)

14. Mr Joaquín Bayo Delgado, the Assistant European Data Protection Supervisor, agreed that the more data one had, the more accurate the identification, but in his view that was not the issue. The true purpose of gathering PNR data was not simply identification, but also for security reasons such as attempting to deduce the intentions of the passenger. (Q 201) We can see that if a traveller is correctly identified but, for example, has the wrong seat number attributed to him which appears to place him in the company of a suspected criminal, this can be as dangerous as attributing the right data to the wrong person.

Data profiling and data mining

15. Most of the controversy surrounding PNR data is about the use to which they are put. We received evidence in particular about "automated profiling based on passenger data",[1] and about data mining programmes to obtain computer-generated risks assessment scores which aim to identify passengers who may pose a risk but who are not on any Government watch list.[2]

16. Data profiling can be described as the determination of characteristics or combinations of characteristics which might identify someone or something as being potentially worth investigation. Data mining is the use of advanced algorithms to trawl through huge databases to discover someone or something matching that profile. The Home Office give as an example the use by banks of software to trawl through millions of transactions to identify those matching predetermined profiles which may identify the transactions as fraudulent.[3]

17. In the context of PNR the profile is those combinations of characteristics which might identify an individual as being potentially high risk. The fact that a passenger matches that profile in no way determines that he is a criminal or even a suspect; only that there is a case for further investigation to see whether other information supports or negates the initial impression.[4] Although data mining can reveal patterns and relationships, it cannot reveal the significance of these patterns; it can identify connections between patterns in the behaviour or conduct of individuals, but it cannot identify causal relationships. These are matters left to those interpreting the information.[5] We give an example in paragraphs 24 to 27 of what can happen when they jump to the wrong conclusions.

---

1 Letter to the Chairman of 30 March 2007 from Ms Joan Ryan MP, Parliamentary Under-Secretary of State, Home Office, p 19.

2 Letter of 9 January 2007 from Privacy International to Vice-President Frattini.

3 New Powers Against Organised and Financial Crime, Cm 6875, July 2006.

4 Cf Faull Q 160.

5 Report for Congress by the Congressional Research Service: Data Mining and Homeland Security: an Overview, 18 January 2007.

18. Mr Faull told us that in his view the use of PNR data for data mining was a lawful and legitimate use of PNR data. (Q 160) We have not heard evidence to the contrary, though Dr Gus Hosein, a visiting scholar of the American Civil Liberties Union (ACLU), told us that Congress prohibits the use of funds to develop or test risk-assessment and profiling systems on passengers. (QQ 8–12) The use of these techniques in connection with data on United States citizens is something Congress has never approved and, in the view of Dr Hosein, never would approve. (Q 34)

The positive value of PNR

19. The degree to which the collection, retention and transfer of PNR data is acceptable depends of course on its value in combating terrorism and other serious cross-border crime, but there is a major obstacle to the assessment of that value. The more serious the crime, the more reluctant the authorities are to disclose details of what information was used, and in what way, to prevent its commission or to arrest and bring to trial those suspected of committing it. Even when a case comes to court, the prosecuting authorities have to disclose only such evidence as is essential for them to prove their case or as the law requires them to disclose to the defence; and this will not necessarily include all the information about the data and methods that have led to the identification of the suspects.

20. In a letter to the Chairman of 3 May 2007 Baroness Ashton of Upholland, the Parliamentary Under-Secretary of State at the Department for Constitutional Affairs (DCA),[6] has given us a number of valuable examples of the benefits of PNR profiling in identifying and disrupting human trafficking, and also an example of the exposure of a drug smuggling operation by PNR profiling. (p 25) But no examples were given to us of the use of PNR data in the fight against terrorism. We were not surprised to be told by Mr Faull that examples given to him (sometimes only in outline) of the benefits of PNR in combating terrorism were very highly confidential. (Q 140)

21. At a tripartite meeting in Berlin on 5 April 2007 between the United States (led by Mr Michael Chertoff, the Secretary of Homeland Security), the Council (led by Dr Wolfgang Schäuble, the German Minister of the Interior), and the Commission (led by Vice-President Franco Frattini), the United States delegation undertook to make public on an anonymous basis some of the security achievements which resulted from data collected by PNR.[7] On 14 May 2007 Mr Chertoff addressed the European Parliament Committee on Civil Liberties, Justice and Home Affairs—the LIBE Committee—on the PNR Agreements,[8] and made public an open letter to Members of the European Parliament giving examples of how the analysis of PNR data had prevented dangerous individuals from entering the United States. We print this letter in Appendix 3 to this report. We note that of the eight examples given, seven relate to serious crimes but not to terrorism. The first example explains how the murder of 132 individuals by a suicide bomber in Iraq provided evidence confirming that inspectors at Chicago airport had been right to refuse him entry to the United States on an earlier

6 Since 9 May 2007 the Ministry of Justice.

7 Council Document No 8282/07.

8 Dr Schäuble and Vice-President Frattini were also present.

occasion. Clearly the use of PNR data did not on this occasion prevent an act of terrorism, though it may have prevented such an act within the United States.

22. We did not receive, and did not expect to receive, details of counter-terrorism operations in which PNR data were relied on successfully. We would however have hoped to receive sufficient evidence of the use of PNR to enable us to assess for ourselves the value of such data. We would not have expected such evidence to be given in public, nor would we have referred to it in this report. But **it is an important principle of democratic accountability that Parliament should be able to reach its own conclusions, and not have to rely on statements from the executive. This would help to secure public confidence.**

23. **Nonetheless, having received no evidence to the contrary, we are prepared to accept that PNR data constitute a valuable weapon in the fight against terrorism and serious crime, and that their continued use is both necessary and justified.**

What can go wrong

24. This assessment is based on the assumption that data are accurately collected and correctly analysed. Plainly, inaccurate PNR data can produce a false identification, and so attribute to an individual conduct and behaviour which is not his. A notorious example frequently given[9] is that of Senator Edward Kennedy, who was once forbidden to land in the United States because he shared a name with an individual on a watch list.

25. Even where correspondence of information produces an accurate identification, inaccurate use of PNR data can still wrongly attribute to an individual behaviour or conduct which is not his. The case of Maher Arar is an illustration of this.

BOX 1

Maher Arar

Maher Arar, a 34-year-old wireless technology consultant, was born in Syria and came to Canada with his family at the age of 17. He became a Canadian citizen in 1991. On Sept. 26, 2002, while in transit in New York's JFK airport when flying to Montreal, Arar was detained by US officials and, on the basis of information supplied to them by the Royal Canadian Mounted Police, interrogated about alleged links to al-Qaeda. Twelve days later, he was chained, shackled and flown to Syria, where he was held in a tiny "grave-like" cell for ten months before he was moved to a better cell in a different prison. He was beaten, tortured and forced to make a false confession. He was eventually returned to Canada in October 2003. On 28 January 2004, under pressure from Canadian human rights organisations, the Government of Canada announced a Commission of Inquiry into the actions of Canadian officials. On 18 September 2006 Justice Dennis O'Connor cleared Arar of all terrorism allegations, stating he was "able to say categorically that there is no evidence to indicate that Mr. Arar has committed any offence or that his activities constitute a threat to the security of Canada".[10]

---

9 By (among others) Dr Gus Hosein (Q 34).

10 See www.maherarar.ca

26. The authorities at JFK airport correctly identified Mr Arar, and accurately identified him as knowing a person being investigated by the Royal Canadian Mounted Police. They failed to investigate the degree of this acquaintance further, they made assumptions from it which were unjustified, and they took action which would have been unjustified even if he had been guilty of the most serious crimes.[11] On 26 January 2007 the Canadian Prime Minister in a statement in Parliament apologised formally to Mr Arar, and the Canadian Government has awarded him C$10.5m (£4.4m) in compensation, the highest settlement by the Canadian Government in an individual human rights case. The US authorities refuse to accept that he is innocent; to this day he is still on their no-fly list. (Q 47)[12]

27. This of course is an extreme case, but it is an example of what can happen when the right data are wrongly used. **The principal risk of error in using PNR data seems to us to arise, not from the quality of the data, but from the erroneous interpretation of the data, even if accurate.**

[11] See the official website of the Commission of Inquiry at www.ararcommission.ca for full reports of the events relating to Maher Arar, including the Commission"s conclusions and recommendations.

[12] The Guardian, 27 January 2007.

CHAPTER 3: THE 2004 AGREEMENT: NEGOTIATION AND CONCLUSION

The EC Data Protection Directive

28. As we have said, the Aviation and Transportation Security Act of 2001 required airlines to supply PNR data to the CBP within the DHS. However Article 25 of the 1995 EC Data Protection Directive[13] provides that personal information originating from within EU Member States may be transferred to a third country only if that country "ensures an adequate level of protection." The adequacy of the level of protection is assessed in the light of all the circumstances surrounding the data transfer, in particular the purpose of the transfer and its duration.

29. The Commission decided that the United States did not ensure an adequate level of protection for PNR data transferred from Member States, which were therefore obliged to prevent the transfer of PNR data to the United States. The airlines were thus in the position that the transfer of PNR data to the United States was a breach of EC law, and of the national laws implementing the Directive;[14] but a failure to transfer the data would lead to sanctions in the United States which might extend to heavy fines and ultimately to a loss of landing rights.

30. Article 25 of the Directive provides that where the Commission has found that data protection in a third country is inadequate, it may enter into negotiations with that country; and if at the conclusion of those negotiations it receives satisfactory assurances from that country, it can make a finding that the level of protection offered is now adequate—an "adequacy decision".

EU/US negotiations

31. An interim arrangement allowed CBP to access PNR data from the beginning of March 2003. Intensive discussions with the EU resulted in commitments by the United States to address EU concerns on access, processing, use, storage, and protection of the PNR information. At the same time, led by the DHS, the United States Government engaged in an effort to obtain an adequacy decision from the Commission which would authorise permanent access to PNR data for CBP.

32. On 16 December 2003 the Commission announced details of an agreement reached with the United States on the transfer of PNR data to US authorities. The Commission negotiators obtained from the United States a number of concessions on the amount of data to be sent and how the data would be handled. The European Parliament had previously expressed strong reservations about how and what sort of data would be exchanged, and had argued that such an agreement would infringe EU citizens' privacy law rights. The Commissioner in charge of the negotiations, Frits Bolkestein, told the Parliament that the US negotiators had moved significantly from their initial position. He explained that clear limits had been fixed on the

---

[13] Directive 95/46 of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L281, 23 November 1995, p 31.

[14] In the United Kingdom, section 4 of and Schedule 1 to the Data Protection Act 1998.

amount of data to be transferred, with a closed list of 34 data elements. In addition, the United States had agreed to store the data for only 3.5 years, rather than the 50 years it had initially wanted. Three and a half years was the time of duration of the Agreement. Thirdly, the United States had finally accepted, after having refused earlier, a safeguard in the form of a joint review to be carried out with the EU authorities at least every year. Lastly, the United States was also willing to recognise the right of EU data protection authorities to represent any European passenger whose complaint to the DHS had not been satisfactorily resolved.

33. When the US authorities began negotiations with the EU in February 2003 they sought to include 38 data elements. The Article 29 Working Party[15] considered these in their Opinion 4/2003 adopted on 13 June 2003 and concluded that twenty of them were acceptable. These included No Show history (where the passenger buys a ticket but does not travel), and Go show (the purchase of a ticket at the airport at the last minute). In the course of negotiations the United States dropped the number of data elements they required to 34. Strangely, the four which they dropped were among those which the Working Party had thought acceptable: identifiers for free tickets, number of bags, number of bags on each segment, and voluntary/involuntary upgrades.

34. The 34 data elements on the final list accordingly include 18 which the Working Party thought went "well beyond what could be considered adequate, relevant and not excessive". Those which particularly concerned the Working Party were the General remarks, OSI (Other Service-Related Information) and SSI/SSR (Special Service Information/Special Service Requests.[16] It is here that sensitive data can appear—defined as "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and data concerning the health or sex life of the individual".[17] An example given to us would be a request by a passenger for halal food.[18]

35. There is thus nothing magical about the number 34, when it comes to deciding on data elements. The Agreement concluded by the EU with Canada in 2005, to which we refer in detail in paragraphs 91 to 94, contains 25 data elements; in preliminary negotiations with the Australians, they are asking for only 19 data elements.[19] Although all 34 data elements are potentially available in the case of each passenger, "CBP believes that it will be rare that an individual PNR will include a full set of the identified data".[20] We have been told that PNR data consisting of ten data elements are more usual.

36. On 29 January 2004 the Article 29 Working Party gave a formal opinion on the draft Agreement.[21] It noted that there had been some improvement in the

---

15 The Data Protection Working Party established under Article 29 of the Data Protection Directive 95/46/EC.

16 These are commonly referred to as general remarks and open fields: see Undertaking 5.

17 Defined in Undertaking 9: see paragraph 40 and Appendix 3.

18 Mr Bayo Delgado, Q 196.

19 Dr Gus Hosein, Q 36.

20 Undertaking 4.

21 Opinion 2/2004 on the Adequate Protection of Personal Data contained in the PNR of Air Passengers to be transferred to the United States, Bureau of Customs and Border Protection (US CBP).

Undertakings now offered on how the data would be handled, but took the view that they would still not justify an adequacy decision. The Working Party concluded that the purposes of the data transfer should be limited to fighting terrorism and specific terrorism-related crimes to be defined; the lists of data elements and the data retention periods should be proportionate; data subjects should have access to their data and to an independent redress mechanism; and the commitments should be legally binding on the United States.

37. Professor Stefano Rodota, the then Chairman of the Article 29 Working Party, addressed the LIBE Committee of the European Parliament the following month to explain the Working Party's "inadequacy" finding. He explained that in the view of the Working Party the proposed adequacy decision was likely to be in breach both of Article 8 (privacy) and Article 6 (right to a fair trial) of the European Convention on Human Rights. There was no possibility of appeal to an independent authority in the United States or elsewhere that would have authority to review data transfer. The lack of explicit guarantees was exacerbated by the very considerable level of discretion granted to the United States administration by the current text. It violated at least three cardinal principles of EU law: necessity, purpose and proportionality. It did not impose a limit on the types of authorities to which passenger data could legally be transferred, nor did it afford the EU any safeguards against the United States changing the nature of their undertakings by reference to alleged changes in circumstances. As we show in Chapter 5, this proved to be a prescient remark. Professor Rodota concluded by drawing attention to the Report which this Committee had recently published which fully supported the "inadequacy" finding of the Article 29 Working Party.[22]

Conclusion of the 2004 Agreement

38. There was little change in the Undertakings between January and May 2004. Nevertheless the Commission adopted an Adequacy Decision on 14 May 2004, amounting to a formal finding that, for the purposes of Article 26(5) of the Directive, the Undertakings offered by the CBP on 11 May 2004 and annexed to the Commission Decision provided adequate protection for the data of passengers flying to or from the United States. Three days after the adoption of the Commission Adequacy Decision, the Council on 17 May 2004 adopted a Decision authorising the signature on behalf of the EC of an Agreement with the United States—the 2004 PNR Agreement. The Agreement was signed in Washington D.C. on 28 May 2004 by a representative of the Presidency on behalf of the EU and by the then Secretary of the DHS on behalf of the United States. It entered into force on that day.[23]

39. The Commission Adequacy Decision is set out in Appendix 4. The Undertakings are annexed to it. The list of 34 PNR data elements required by CBP forms an attachment to the Undertakings. The text of the Agreement itself is set out in Appendix 5.

---

22 *Fighting illegal immigration: should carriers carry the burden?* Fifth Report, Session 2003–04, HL Paper 29, paragraphs 30 to 34.

23 As stated in the judgment of the European Court of Justice, paragraph 32.

40. There is sometimes confusion about the purpose of this Agreement. It was not intended to authorise the transfer of PNR data by the airlines to the US authorities, nor does it purport to do so. Its purpose was to legalise the "pulling" by CBP of PNR data from air carriers' registration systems if and only if this took place in accordance with the Commission Adequacy Decision, and hence in accordance with the Undertakings offered by the United States and annexed to that Decision.

The Undertakings

41. The Undertakings given by the US authorities which enabled the Commission to issue its Adequacy Decision are set out in full in Appendix 4. The following are some of the most significant:

- PNR data are to be used by CBP strictly for the purposes of preventing and combating (1) terrorism and related crimes; (2) other serious crime, including organised crime, that are transnational in nature; and (3) flights from warrants or custody for the crimes described above (Undertaking 3);
- CBP will consult with the Commission regarding revision of the required PNR data elements prior to effecting any such revision (7);
- CBP will not use sensitive data—personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and data concerning the health or sex life of the individual (9);
- CBP will "pull" passenger information from air carriers reservations systems until such time as air carriers are able to implement a system to "push" data to the CBP (13);
- CBP in its discretion will only provide PNR data to other government authorities (including other components of DHS), including foreign government authorities, with counter-terrorism or law enforcement functions, on a case by case basis, for purposes of preventing or combating offences identified in paragraph 3 (28–29);
- Requests by the data subject to receive a copy of PNR data contained in the CBP databases are processed under the Freedom of Information Act (37);
- CBP undertakes to rectify data in its database where it determines that a correction is justified (by attaching a note reflecting the inaccuracy rather than correcting the PNR record itself); the complaints can be made by individuals or by EU data protection authorities on their behalf (39–42);
- CBP and DHS undertake to conduct at least once a year a joint review with the Commission and representatives of the Member States on the implementation of the Undertakings (43);
- The Undertakings apply for 3.5 years; after 2.5 years DHS will initiate discussions with the Commission with the aim of extending them on mutually acceptable terms (46).

42. These Undertakings, while in no way diminishing the value of PNR as a tool in combating terrorism, would, if strictly adhered to and interpreted in the

spirit of the Agreement, have constituted a valuable restriction on the use of PNR data which might well have justified the Commission's Adequacy Decision. However there are other Undertakings which considerably diminish the value of these. Undertaking 47 provides that "These Undertakings do not create or confer any right or benefit on any person or party, private or public." In other words, they are a statement of intent, but cannot be relied on in a court of law. Breach of an undertaking could not be used to support a claim by a person that his PNR data had been misused and that he had thereby suffered loss.

43. Undertakings 34 and 35 can be and, as will appear in Chapter 5, have been used to make very significant changes to the PNR data elements, to the Undertakings themselves, and hence to the uses to which the data elements can be put. The first of these Undertakings reads:

> "No statement herein shall impede the use or disclosure of PNR data to relevant government authorities, where such disclosure is necessary for the protection of the vital interests of the data subject or of other persons, in particular as regards significant health risks. Disclosures for these purposes will be subject to the same conditions for transfers set forth in paragraphs 31 and 32 of these Undertakings."

There is nothing to say who is to determine, and on what basis, what is a "vital interest" of the data subject, when disclosure is "necessary", or which are the "relevant" government authorities to which disclosure is made.

44. Undertaking 35 reads:

> "No statement in these Undertakings shall impede the use or disclosure of PNR data in any criminal judicial proceedings or as otherwise required by law. CBP will advise the European Commission regarding the passage of any US legislation which materially affects the statements made in these Undertakings."

This means that changes in United States law which require PNR data to be used for other purposes will override the Undertakings.

Cost

45. Airlines are commercial organisations. They are of course concerned with the safety of their passengers, their crews and their aircraft, but ultimately their aim is to make a profit. When, three years ago, we considered a draft EU Directive[24] on the obligation by carriers to communicate passenger information to Government authorities, we received evidence from the Board of Airline Representatives in the UK (BARUK), the British Air Transport Association (BATA), Britannia Airways and British Airways, all complaining about the burden (not just the cost) that the proposed Directive would place on them.[25] That report was published in February 2004, when negotiations

---

[24] Subsequently adopted as Directive 2004/82/EC on the obligation of carriers to communicate passenger data, OJ 2004 L 261/24.

[25] The evidence is published on pages 15–19 of the report *Fighting illegal immigration: should carriers carry the burden?* Fifth Report, Session 2003–04, HL Paper 29.

on the 2004 Agreement were drawing to a close, and our report referred to these, and commented on the burden such an Agreement would place on air carriers.[26]

46. In the context of this inquiry BATA have sent us evidence of their own, incorporating the views of British Airways and Virgin Atlantic. (p 54) The airlines believe that the cost of providing the data should lie with the requesting authority. We believe their hopes of achieving this are minimal, given that the negotiating mandate of the Council and Commission does not include any reference to the cost.[27] There are however other burdens which could and should be lightened, and which we consider in paragraphs 124 to 130 below.

Informing the travelling public

47. Passengers intending to fly to the United States have a right to be told in advance that significant personal data will be transferred to the US authorities. The onus must not be on the passenger to seek this information; it is the airline's duty to provide it.

48. In a formal Opinion[28] the Article 29 Working Party has put forward a short model form and a longer response to Frequently Asked Questions which would enable airlines to carry out this duty in a consistent and satisfactory way. The Working Party suggests that the following methods should be used:

- if the booking is made through a travel agent, the passenger should be given the short form and, if he or she requests it, the longer form;
- if the booking is made by telephone, the short form should be read to the passenger, who should be told how to access the longer form (e.g. by visiting a website);
- if the booking is made on the internet, the short form should appear on the screen without the passenger having to take any positive step, and the short form should enable the passenger to click on the longer form.

49. **It is important that intending passengers should be aware of who will receive their personal data, and subject to what conditions. We agree with the Working Party that the airlines should be responsible for informing passengers, and we endorse the Working Party's proposals.**

50. Some airlines already provide information of this type. By way of illustration we show what people booking a British Airways flight online, regardless of the destination, are able to access if they wish to check to which government authorities British Airways may pass the personal data they have provided.

---

[26] *Ibid.*, paragraphs 30–34.

[27] Evidence of the Department for Transport Aviation Directorate, which would have preferred the mandate to include a reference to the cost (p 55).

[28] Opinion 2/2007 of 15 February 2007.

TABLE 1

British Airways: Frequently Asked Questions

Question
Where can I find details of the access to British Airways booking records for US and other governments?
Answer
Under U.S. Law, U.S. Customs and Border Protection (CBP) will receive certain travel and reservation information, known as Passenger Name Record or PNR data, about passengers flying between the European Union and the U.S. CBP has undertaken that it uses this PNR data for the purposes of preventing and combating terrorism and other transnational serious crimes. The PNR may include information provided during the booking process or held by airlines or travel agents. The information will be retained for at least three years and six months and may be shared with other authorities. Airlines are also required by UK laws to provide passenger data to UK Customs and Immigration. It is expected that passenger data will have to be disclosed to other governments such as Australia and Canada in the near future. Accordingly any information we hold about you and your travel arrangements may be disclosed to the customs and immigration authorities of any country in your itinerary. **Q1. What data do you hold about me which may be accessed?** We hold data about you which we require for the purpose of conducting business with you. This may include details you have told us about any medical, disability, or health conditions you may have; payment details; contact information; and any special requirements you have specified. **Q2. Who will you pass the data to, and who will they share it with?** The data will be given to the Border Control authorities, for example, Customs, of countries which have a legal right to acquire the data. They may share it with other enforcement authorities for the purposes of preventing and combating terrorism and other serious criminal offences **Q3. What if I refuse you permission to release my data to the authorities?** If you are flying to or through a country which requires the information, we will have to cancel your reservation and will be unable to carry you to or through that country. **Q4. Which countries have legislation to permit access to my data?** At present, there is legislation in Australia, Canada, UK, and USA requiring carriers to grant access to passenger information. Other countries may follow in the future. **Q5. What will the authorities be using the data for?** Data is used for enforcement purposes, including use in threat analysis to identify and interdict potential terrorists, and other threats to national and public security; and to focus government resources on high risk concerns, thereby facilitating and safeguarding bona-fide travellers. **Q6. Are my credit card details included?** If payment has been made by credit card and this data is included in your passenger information record, the authorities may view details. **Q7. How long will data be held for?** Each country should hold the data for no longer than is required for the purpose for which it was stored. **Q8. Will the data be transmitted in a secure fashion?** Yes, British Airways will pass the data to the authorities by secure means.

CHAPTER 4: THE 2004 AGREEMENT: DECLINE AND FALL

The challenge from the European Parliament

51. We have described in paragraph 37 the address given by the then Chairman of the Article 29 Working Party to the LIBE Committee of the European Parliament in February 2004. He was supported by Peter Hustinx, the European Data Protection Supervisor (EDPS). At the end of the debate the rapporteur, Johanna Boogerd-Quaak MEP, said that it was unacceptable that an agreement should be concluded which, in all probability, did not conform with EC law. She proposed that the Committee should write to the Parliament's Legal Services to ascertain whether an Opinion could be obtained from the European Court of Justice (ECJ) on the legality of the proposed Adequacy Decision.

52. The Parliament's quarrel was in fact not so much with the legality of the proposed Decision as with the substance of the data protection undertakings, which the Parliament regarded as inadequate. The proposal to link a challenge to the legality of the Decision with its main complaint on the substance proved fatal to its case.

The Court proceedings

53. In the Court proceedings the Parliament sought the annulment both of the Commission Adequacy Decision and of the Council Decision authorising the signature of the Agreement.[29] The grounds advanced for annulment of the Adequacy Decision were that it was *ultra vires,* in breach of the fundamental principles of the Directive, in breach of fundamental rights and in breach of the principle of proportionality. The EDPS intervened on behalf of the Parliament, and the United Kingdom on behalf of the Commission and the Council.

54. In his Opinion of 22 November 2005 Advocate-General Léger advised that the Adequacy Decision was unlawful, since the Directive on which it was based was an EC (first pillar) instrument, and therefore inappropriate for dealing with third pillar matters.[30] Making PNR data available to CBP constituted "personal-data processing operations which concern public security and relate to State activities in areas of criminal law. Those processing operations are, therefore, excluded from the material scope of Directive 95/46."[31] The Advocate-General also took the view that the legal base for the Council Decision (Article 95 TEC) was defective, the object of the Agreement being the prevention of terrorism and other serious crime, and the relationship with the single market being only "incidental". If the Court agreed with him, this was enough to conclude the case. Since however it was open to the Court to disagree with him on this issue, he went on to consider the substantive complaint about the data protection issues, and

---

29 Joined Cases C–317/04 and C–318/04.

30 The Treaty establishing the European Community (TEC) deals primarily with the internal market: what are now known as first pillar matters. Title VI of the Treaty on European Union (TEU) gave the European Union (as opposed to the European Community) the power to deal with Police and Judicial Cooperation in Criminal Matters. These are so-called third pillar matters, which are therefore outside the scope of the TEC.

31 Paragraph 97 of the Opinion.

found that the Undertakings were adequate, as was the procedure leading to the conclusion of the Agreement.

55. In its judgment of 30 May 2006[32] the Court agreed with the Advocate-General on the issue of legality, holding that activities under Title VI of the Treaty on European Union, such as activities in the fields of public security, State security and the activities of the State in areas of criminal law, fell outside the scope of the Directive. The Court also agreed that Article 95 did not provide an adequate legal base for the Council Decision. It accordingly annulled both Decisions, and concluded that it was unnecessary to consider the Parliament's other arguments. Given the consequences of its judgment, the Court preserved the effect of the Adequacy Decision until 30 September 2006 to allow time for the first pillar Agreement to be denounced and a third pillar Agreement to be negotiated.

56. The result of the Parliament's challenge on legality was therefore that:

- it rendered consideration of the substantive issues unnecessary, so that the Parliament obtained no ruling on the one matter on which it wanted a ruling;
- it struck down the 2004 Agreement which, though in its view inadequate, was better than nothing;
- by moving the matter from the first pillar to the third pillar, it ensured that the Parliament would have no formal say in the negotiation of any subsequent agreement.

[32] 2006 ECR I–4721

CHAPTER 5: THE 2006 INTERIM AGREEMENT AND THE BAKER LETTER

57. The Commission Adequacy Decision and the Council Decision authorising signature of the 2004 Agreement both having been annulled, the Agreement based on them had to be denounced. Article 7 of the Agreement allowed either party to terminate it, the termination to take effect 90 days after it had been notified to the other party. Accordingly the Council and Commission notified the United States Government on 3 July 2006 of the termination of the Agreement 90 days later, i.e. on 30 September 2006, the date on which the Court's judgment took effect.[33]

58. The EU therefore had less than three months to negotiate a new agreement. This agreement would be based on the third pillar rather than the first pillar, so that the parties would be the United States and the European Union, rather than the European Community. The negotiations on the Agreement were completed on 6 October 2006, and on that day the Council adopted a Decision authorising the Presidency to sign the new Agreement. It was signed on behalf of the EU on 16 October, and on behalf of the United States by the Secretary of DHS on 19 October, from which date it applied "provisionally".[34] We set out the text of this Agreement in Appendix 6. We refer to it as "the 2006 Agreement" or "the Interim Agreement".

59. Between the conclusion of negotiations on the 2006 Agreement and its signature Stewart Baker, the Assistant Secretary for Policy at the DHS, wrote to the Presidency and the Commission a letter "intended to set forth our understandings with regard to the interpretation of a number of provisions of the Passenger Name Record (PNR) Undertakings issued on May 11, 2004 by the Department of Homeland Security (DHS)". This letter was received by email on 11 October 2006, and acknowledged by the Presidency, and by Jonathan Faull on behalf of the Commission.[35] The texts of the two letters are set out in Appendix 7.

60. By the Interim Agreement the EU undertook to ensure that air carriers operating flights to, from or over the United States should process the PNR data in their reservation systems as required by DHS; but this was expressly "in reliance upon DHS's continued implementation of the Undertakings *as interpreted in the light of subsequent events*". The words we have italicised are the justification for the letter from Stewart Baker ("the Baker letter") for, as Jonathan Faull explained to us, although the negotiations began with the EU saying "The Undertakings are untouchable", they had to accept that "Things have changed in Washington in the last couple of years." (QQ 158–159). These changes, and the consequent "interpretation" of provisions of the Undertakings, have meant that the commitments of the United States under the Interim Agreement are markedly different from those under the 2004 Agreement.

---

33 OJ C219/1 of 12 September 2006.

34 OJ L298/29 of 27 October 2006.

35 OJ C259/4 of 27 October 2006.

Sharing of PNR with other agencies

61. One of the main changes since May 2004 is the provision in the Intelligence Reform and Terrorism Prevention Act of 2004 requiring the President to establish a new Information Sharing Environment (ISE). He did this by an Executive Order of 25 October 2005 requiring DHS and other agencies "promptly to give access … to terrorism information to the head of each other agency that has counterterrorism functions".

62. This means that, although the Undertakings, and especially Undertakings 28–32, forbid the routine sharing of PNR data with other government agencies, United States law now requires this. The justification for this is given as Undertaking 35, which we cited in full in paragraph 44: "No statement in these Undertakings shall impede the use or disclosure of PNR data in any criminal judicial proceedings or as otherwise required by law".

The "frequent flyer" data element

63. The Baker letter dealt with more than just the interpretation of the Undertakings. Data element 11 is "Frequent flyer information [limited to miles flown and addresses]". The letter explains that "the frequent flyer field may offer addresses, telephone numbers, and email addresses, all of which may provide crucial links to terrorism". Undertaking 7 allows CBP to consult with the Commission regarding revision of the PNR data elements. Mr Baker tells us that "With this letter the US has consulted … with the EU" about the need to obtain the frequent flyer number, and indeed "any data element listed in Attachment A to the Undertakings" wherever that element may be found.

Vital interests of the data subject

64. In October 2006 avian flu was very much headline news, though it has since receded from the limelight. This perhaps explains why in the Baker letter DHS "reconfirms" that access to PNR data "in the context of infectious disease and other risks to passengers" is authorised by Undertaking 34. We set out that Undertaking in paragraph 43, and we pointed out how the width of its wording was open to abuse. Now we are told that "vital interests of the data subjects or others" includes information about exposure to dangerous communicable diseases. We are not told how disclosure in the case of health risks is consistent with Undertaking 3: PNR to be used "strictly" for combating terrorism and crime.

65. When the Baker letter first came to our attention we put this to Baroness Ashton of Upholland, the Parliamentary Under-Secretary of State at the Department for Constitutional Affairs (DCA) responsible for data protection. In her reply of 16 February 2007 she told us that the Government "would be content with the use of PNR data for this purpose."

Time of retention of current data

66. Undertaking 15 provides that after 3.5 years PNR data that have not been manually accessed during that time will be destroyed. Ms Cecilia Verkleij from Commission DG JLS explained to us (Q 164) that in the negotiations for the 2004 Agreement the United States started arguing in favour of retention for 50 years and went down to 7 years; the Commission wanted one year. Three and a half years was a compromise, chosen in essence

because it was as long as the 2004 Agreement was destined to last. Undertaking 46 explains that the Undertakings will apply for 3.5 years, but that "[I]f no mutually acceptable arrangement can be concluded prior to the expiration of these Undertakings, the Undertakings will cease to be in effect."

67. The Baker letter suggests that, as a result, this 3.5 year retention limit has no effect:

> "The Agreement will have expired before Paragraph 15 of the Undertakings requires the destruction of any data, and questions of whether and when to destroy PNR data collected in accordance with the Undertakings will be addressed by the United States and the European Union as part of future discussions."

This would be in blatant disregard of the final sentence of Undertaking 15, which reads:

> "With respect to PNR which CBP accesses [or receives] directly from air carrier reservations systems during the effective dates of these Undertakings, CBP will abide by the retention policies set forth in the present paragraph, *notwithstanding the possible expiration of the Undertakings pursuant to paragraph 46 herein*." [our italics]

68. This final sentence is an accurate statement of the law as we understand it. Data transferred on 1 July 2004 were governed by an Undertaking that they would be deleted on or before 1 January 2008. The fact that, by that date, the Agreement will no longer be in force does not make the obligations under that Undertaking any the less binding on the US authorities.

69. There is also an ethical dimension. The suggestion behind Ms Verkleij's reply is that, so long as the Agreement expired before the end of the agreed data retention period, the length of this period was irrelevant because the United States never had any intention of being bound by this provision. We are reluctant to believe this of partners who, we are told, have always negotiated in good faith.

70. This too is a matter we put specifically to Baroness Ashton. In her letter of 16 February 2007 she stated categorically that "any data that are or have been transferred under the original and current Agreements will continue to attract a data retention period of 3.5 years". In oral evidence we put to her the apparent conflict between this statement and the Baker letter, and she repeated four times that the correct period was 3.5 years, but then appeared to qualify this by saying: "If the Americans, as part of the negotiations, wish to argue that data should be retained for a longer time then they will have to make that case, and that case will then become part of the balancing between the importance of keeping data for the right length of time based on experience and knowledge that they will acquire … versus what seems an inappropriate length of time. That will be part of the negotiation." (QQ 77–80) It is not entirely clear to us whether this last reply referred to retention of data under the 2004 and 2006 Agreements, or under the new Agreement to be negotiated.

71. For the purposes of the new Agreement being negotiated we have concluded[36] that fixing a precise time limit is not the most important aspect of data retention. We would not therefore be opposed to an Agreement

---

[36] Paragraphs 110 to 114.

which provided that data transferred under the 2004 and 2006 Agreements should be retained for longer than 3.5 years. What we strongly oppose is the assumption that this can take place simply by a unilateral abrogation of the Undertaking, without the consent of the EU expressed in a provision of the new Agreement.

72. **The negotiators should as a matter of principle insist that data transferred under the 2004 and 2006 Agreements must be destroyed no later than 3.5 years after the transfer, unless a formal Agreement is negotiated allowing these data to be retained longer.**

Consultation

73. We mentioned in paragraph 63 Mr Baker's statement: "With this letter the US has consulted … with the EU". In his written evidence the Information Commissioner wrote:

> "The Commissioner and his EU counterparts have noted with concern that mechanisms provided for at paragraph 7 of the Undertakings for consultation by the US with the EU on the expansion of the data items appear to have been used in practice as a basis for unilateral declaration by the US side of their intention to expand the items. This is not what the Commissioner and his counterparts envisaged by a consultative arrangement."

74. We wondered whether there had in fact been any consultation at all prior to the sending of the Baker letter. Mr Faull assured us that the letter followed extensive discussions and consultations on the specific issue. (Q 154) We would have been concerned if there had not been prior consultations, but we wonder whether consultations which plainly did not include "the [Information] Commissioner and his EU counterparts" were of any great value.

Adequacy: our assessment

75. Mr Faull's letter acknowledging the Baker letter concludes:

> "The commitments of DHS to continue to implement the Undertakings allow the EU to deem that, for the purposes of the implementation of the Agreement, it ensures an adequate level of data protection."

In the case of an agreement between the United States and the EU (rather than the EC), there was no need for a formal Adequacy Decision, nor indeed any possibility of one. But our view is that, once the Undertakings were given the interpretation in the Baker letter, even those who had previously regarded them as providing an adequate level of data protection might well have changed their minds.

76. **Whatever the justification for extending data elements, for wider sharing of data, or for using data to identify possible carriers of dangerous communicable diseases, there is no justification at all for doing so through a unilateral declaration by one of the parties to an agreement**.

77. **An undertaking which includes a provision allowing the party giving it to amend it virtually at will is of very limited value, and scarcely deserves the name. No such provision should be included in any future agreement.**

CHAPTER 6: NEGOTIATIONS FOR A NEW AGREEMENT

78. The interim Agreement expires "in any event no later than 31 July 2007, unless extended by mutual agreement".[37] Negotiations for a new Agreement began early in 2007.

79. Undertaking 48 provides that "The provisions of these Undertakings shall not constitute a precedent for any future discussions with the European Commission, the European Union, any related entity or any third State regarding the transfer of any form of data". The Interim Agreement contains a recital to the same effect. The purpose of these statements is plainly to make clear to the parties (in practice the EU) that there can be no expectation that any Undertakings previously given will be repeated.

Who negotiates for the EU?

80. Article 24(1) of the Treaty on European Union is clear: "When it is necessary to conclude an agreement with one or more States or international organisations in implementation of this title[38] the Council may authorise the Presidency, assisted by the Commission as appropriate, to open negotiations to that effect." The Member States thus decide on a mandate for the negotiations, and authorise the Presidency and the Commission to negotiate on behalf of the EU. The theory is that both the Presidency and the Commission take part in the negotiations. In oral evidence on 22 March 2007 Mr Faull told us that negotiations for the new Agreement were taking place under the German Presidency who were "absolutely" in charge of the negotiations. (Q 158) At a seminar on the PNR Agreement organised by the LIBE Committee of the European Parliament on 26 March 2007 he stated that the Commission was willing to give the Council all the assistance it could in the negotiations.

81. We have mentioned in paragraph 21 the meeting on 5 April 2007 with Mr Michael Chertoff, the United States Secretary of Homeland Security. Both the German Minister of the Interior, Dr Wolfgang Schäuble, and the Minister of Justice, Ms Brigitte Zypries, were present, and PNR was prominent among the topics discussed. But the meeting was described as a Troika, and the third party was the Commission, represented by Vice-President Frattini and Mr Faull. We believe that in practice the Commission plays a pivotal role in the negotiations, nor could it be otherwise, given the transient nature of the Presidency under the present Treaties. The first Agreement was concluded in the first half of 2004 under the Irish Presidency. Austria held the Presidency when the Court gave its judgment on 30 May 2006, and therefore had to begin the process of negotiating a new Agreement, but this was continued and concluded under the Finnish Presidency. Now Germany is formally in the lead, and the negotiations will be continued under the Portuguese Presidency if necessary, though it is not high on their agenda: "They would like to see it out of the way under the German Presidency". (Q 183)

---

[37] Interim Agreement, paragraph 7.

[38] "this title" is Title V (Provisions on a Common Foreign and Security Policy); by paragraph (4) of Article 24, paragraph (1) of that Article also applies to Title VI (Provisions on Police and Judicial Cooperation in Criminal Matters).

82. When the negotiations for the 2004 Agreement began in 2003, the Joint Statement issued after the talks on 17 and 18 February 2003 made clear that only "senior officials of the European Commission … led by [the then] Director General for External Relations Guy Legras" negotiated on behalf of the EU. The true position is still that the Commission, and now Jonathan Faull in person, is the one fixed point acting on behalf of the EU in these negotiations: "We provide the continuity". (Q 182)

83. The United Kingdom, by reason of its relationship with the United States, might be thought to be in a unique position to influence the negotiations; but while we understand that there is some contact between the authorities of the two countries on this question, it does not appear to influence the negotiations very much. Baroness Ashton told us: "There is no doubt that the UK has a role to play in relation to the US but the negotiations are specifically EU and I think that is right and proper." (Q 71)

Timetable

84. As we have made clear, the Interim Agreement expires on 31 July this year. At the Berlin meeting on 5 April the parties agreed that they must keep to this deadline, and that there was a need by then to negotiate an agreement covering at least the nature of the data transmitted, the purpose for which they were used and the time of retention, rights of access to the data and supervision of the agreement. But they stated that they were aware that the current Interim Agreement could be prolonged beyond 31 July, and the US delegation said that they were satisfied with the Interim Agreement.[39] From this one can deduce that the US delegation have no incentive to negotiate a stricter agreement, or indeed any agreement, by 31 July. **It may be that the only result of the negotiations will be an agreement, no doubt reluctant on the part of the EU, to extend the Interim Agreement. This would in our view be the worst of all possible results.**

The views of the European Parliament and the data protection authorities

85. As explained above, the European Parliament does not have a legislative (as opposed to a consultative) role to play in the formulation of third pillar law, and hence in the negotiation of the Agreement. The same is true of the EDPS, the national data protection authorities, and the Article 29 Working Party which is composed of them. This does not prevent them having and expressing strong views about the degree to which the privacy rights of individuals are safeguarded, both in the current interim Agreement, and in the Agreement being negotiated.

86. On 11 October 2006 Ms Paula Lehtomäki on behalf of the Finnish Presidency and Vice-President Frattini on behalf of the Commission made a statement to the European Parliament on the outcome of the negotiations with the United States. They regarded the negotiations and the resultant Interim Agreement as a success, but only one of the members who spoke in the debate (Michael Cashman MEP) agreed with them. The rest deplored the terms of the Agreement with varying degrees of emphasis. Sophie in't Veld MEP, the rapporteur of the LIBE Committee on PNR,

[39] Council Document 8282/07.

drew particular attention to the Baker letter: the extension of the purposes to fighting infectious diseases, the sharing of data with other agencies, some unspecified, and the suggestion that the data retention period should be ignored. Many of these points were reiterated in subsequent debates on 31 January and 14 February 2007.

87. On 26 March 2007 two seminars were held at the European Parliament building to discuss the Interim Agreement and the negotiations for the new Agreement.[40] The morning seminar was organised by the Article 29 Working Party, the afternoon seminar by the LIBE Committee. Many of the speakers were the same.[41] Given the constitution and functions of these two Committees, it is not surprising that speakers tended to concentrate on the data protection aspects, and to voice concerns about the privacy of individuals; but there were also speakers from the Association of European Airlines, Amadeus (the body which undertakes the technical side of PNR transfers on behalf of many of the largest airlines), and the Home Office (on the UK e-Borders Programme).

88. Although the breadth of the data elements and the non-binding nature of the Undertakings were prominent in the discussions, the principal cause for concern was again the Baker letter, and the way it had been used to defeat much of the value of the Undertakings.

89. **The fact that the European Parliament no longer has a formal role to play is not a reason why the views of its members should be disregarded. On the contrary, in a Union of democracies special attention must be paid to the views of representatives, since they are well placed to balance the public good against private rights**.

90. **The European Data Protection Supervisor, and national data protection authorities individually and collectively in the Article 29 Working Party, have great experience of the practical working of data protection laws and of non-binding declarations on the handling of personal data. Those negotiating a new agreement should be guided by their opinions.**

The EC/Canada PNR Agreement

91. We have already referred to the Agreement of 3 October 2005 with Canada[42] which is the only other PNR Agreement currently in force.[43] The EDPS (p 49) and others of our witnesses suggested that this should be used as a model in the negotiations for the new Agreement with the United States.

92. As in the case of the 2004 Agreement with the United States, the other party to the Canada Agreement is the EC rather than the EU, and that Agreement too is based on a Commission Adequacy Decision. Its legal basis is therefore equally suspect, and if it came to be considered by the ECJ it too would

---

40 We refer to them as "the March seminars".

41 The co-chairmen of the morning seminar were Mr Peter Schaar, the current Chairman of the Article 29 Working Party, and Mr Stavros Lambrinidis, the Vice-Chairman of the LIBE Committee. One of the chairmen of the afternoon seminar was Mr Jean-Marie Cavada, the Chairman of the LIBE Committee, and Mr Schaar was one of the main speakers, as was Mr Peter Hustinx, the EDPS. Mr Jonathan Faull also spoke at both seminars.

42 OJ L82/15 of 21 March 2006.

43 An agreement with Australia is under negotiation.

almost certainly be annulled. But since it was regarded by the EDPS,[44] the Article 29 Working Party[45] and the European Parliament as satisfactory it was not the subject of Court proceedings and so has not been annulled. It is therefore still in force. Mr Faull, while emphasising that the two countries did not have the same laws or concerns, thought **the Canada Agreement could be "a reference point, a starting point" for negotiations with the United States; we agree.**

93. Some of the features which distinguish the Canada Agreement from the US Agreements are the following:

- it is concerned not just with PNR but also with Advance Passenger Information (API);
- although in fact intended for the transfer of PNR data to Canada, it is drafted in terms which would allow it to be used for the reciprocal transfer of PNR data from Canada to the EU;
- there are only 25 data elements, and none of them is equivalent to the general remarks and open fields in the US Agreement;[46]
- the Canadian Border Service Agency (CBSA) does not require carriers to collect PNR information that they do not themselves require;
- information is from the outset "pushed" by the airlines rather than "pulled" by the CBSA;
- the Undertakings are called "Commitments", and do not state that they confer no legal rights or benefits—but nor do they state that they are legally binding;
- there is no Commitment equivalent to United States Undertaking 35 which allows a change in the law to be used to amend or nullify other Commitments.

94. These are all features to which we will refer as we come to consider the negotiation of the new agreement with the United States.

Data Elements

95. We considered in Chapter 2 the PNR data elements, and views on their reliability. In Chapter 3 we considered the Undertakings in the 2004 Agreement, and in Chapter 5 the effect on these of the Baker letter. In the light of those conclusions we now look to see what those negotiating the new Agreement on behalf of the EU should be seeking to achieve.

96. As we have explained in paragraph 32, the 34 elements in the current Agreement are a compromise. Mr Faull told us that "[the Americans] may well ask for more information. Our view at the moment is that the 34 PNR items are probably sufficient and may even be excessive in number, and we will certainly at least wish to negotiate very seriously with our American partners about each individual item of information." (Q 145)

97. What seems clear to us is that, if a country like Canada which takes its national security no less seriously than the United States is satisfied with only

---

44 Opinion of 15 June 2005.

45 Opinion 1–2005 of 19 January 2005.

46 See paragraph 34 above.

25 data items, the United States must be required to produce for each and every additional item that it requires detailed and particular justification for the inclusion of that item. That justification must be made available to those negotiating on behalf of the EU, and **we expect them to take a robust attitude in the negotiations before being satisfied that any additional data item is essential and therefore permissible.**

98. A number of our witnesses[47] particularly objected to the inclusion in the data elements of open-ended data elements like "general remarks" or "open fields", which merely serve as a means of introducing other data not specifically listed, in particular sensitive data. We share this view. If a data element is essential, it must be possible to define it with sufficient particularity. If that is not possible, it must be excluded.

99. **It would be wrong to include among the agreed data elements open-ended data elements like "general remarks" or "open fields", which merely serve as a means of introducing other data elements not specifically listed**.

Undertakings

100. An undertaking is more than just a statement of intent: it is, as the Canada Agreement says, a commitment. If the party giving it does not intend to be bound by it, there is no point in negotiating it. **We hope therefore that the talks will have started on the basis that the Undertakings being negotiated, unlike the current ones, are legally binding on the United States authorities.**

101. In the same way that, in the case of data elements, no "general remarks" must be used to add to the list, in the case of undertakings there is no place for one like the current No 34 which effectively allows data to be passed to persons and bodies for whom they were not intended and used for purposes other than those specified in the Agreement; or like No 35 which allows changes in the law to override them without any further negotiation. What the Undertakings say, and what they mean, must be clear from the four corners of the document. There is no scope for statements which are so unclear that they leave room for unilateral interpretation.

102. **All the terms of the Undertakings being negotiated must be specific, unequivocal, contained in the document itself, and not susceptible of amendment without the agreement of all the parties.**

103. **If any clarification is needed, this is a matter for subsequent open negotiation between the parties. There can be no scope for amendment by unilateral "interpretation" of the Undertakings**.

Purpose limitation

104. As we have explained, the wider use of PNR data started after 9/11 as a counter-terrorism exercise. The recitals to the 2004 Agreement state that its purpose is "to prevent and combat terrorism and transnational crime". Undertaking 3 states that it is to prevent and combat "(1) terrorism and related crimes; (2) other serious crimes, including organised crime, that are transnational in nature; (3) flights from warrants or custody for the crimes

[47] EDPS Q195. Information Commissioner p 58. Mr Tony Bunyan, Director of Statewatch, Q 96.

described above". The prevention of "serious crime" immediately raises the question, how serious must a crime be to fall within this description and so be covered by the PNR Agreement? Few crimes are more serious than the smuggling of children (an example given to us by Baroness Ashton of a crime solved by reference to PNR);[48] most people would agree that the smuggling of tobacco (an example given to us by Ms Ryan)[49] is not in the same league, let alone road traffic offences (Q 57) (which in any event are seldom transnational in nature).

105. We would not attempt to define what is a "serious" crime. Since however the expression is used in the same sentence as "terrorism and related crimes", that is an indication of the severity of the crimes which are contemplated by the Agreement. If it is intended by both parties that PNR data are to be used for dealing with less serious crimes, the new Agreement should say so clearly.

106. Moreover it is now plainly the intention of the United States (as indeed it is of Canada) that PNR data should be used to identify major health risks from serious communicable diseases, and to protect the public against them. This too should be stated unequivocally at the outset. There is no reason why the diseases covered should not be listed, and likewise the persons or bodies to whom information may be passed. We note however that more than half a million persons enter the United States illegally every year across the many thousands of miles of land borders.[50] Since PNR data are derived only from air travel, it seems to us that these data are likely to be of only limited use in preventing the spread of communicable diseases.

107. **Under the 2004 Agreement the use of PNR data was to be limited to:**

- **the prevention and combating of terrorism and related crimes;**
- **other serious crimes, including organised crime, that are transnational in nature; and**
- **flights from warrants or custody for these crimes.**

The negotiators should seek to retain these limitations in the new Agreement.

108. **We believe that the use of PNR data for general law enforcement purposes, as opposed to countering terrorism and serious crime, is undesirable and unacceptable.**

109. **If, contrary to our view, it is agreed that data should be used for other purposes, those purposes must be specifically listed at the outset. Words such as "vital interests of the data subject" are too vague.**

Retention of future data

110. Any PNR data which appear to be significant for anti-terrorism or law enforcement purposes, and which have been "manually accessed" for those purposes, can be retained for as long as they are useful. There is in such a case no limit on the retention time, nor should there be. The issue is the length of time for which data which are retained routinely but which do not appear to have any significance should be kept on the basis that they might one day be useful.

---

48 Letter to the Chairman of 3 May 2007; supplementary evidence, p 25.

49 Letter to the Chairman of 30 March 2007; supplementary evidence, p 19.

50 Final Report of the 9/11 Commission, paragraph 12.4.

111. That period is currently 3.5 years not just in the US Agreement but also in the Canada Agreement.[51] The Baker letter states that "even data that is more than 3.5 years old can be crucial in identifying links between terrorist suspects". Mr Faull explained the value of this in the case of "clean skins"—persons with no police record, not known to the authorities in any way, who suddenly feature in a terrorist attack. At that stage it may prove important to reconstruct a pattern of that person's life: "PNR tells you with whom the named person has been reserving flights, next to whom he or she has been sitting on planes regularly, where they have been flying to and from et cetera." (QQ 165–167, 172)

112. Mr Bayo Delgado told us that in the view of the EDPS 3.5 years was "already excessive", and that there was "an enormous disproportion between the effectiveness of that long period of retention and the results of that retention". (Q 206) But Mr Tony Bunyan, the Director of Statewatch and no friend of the current Agreement, though he would start negotiations on the basis that information should be held for only 24 hours, was not prepared to disagree with the proposition that 3.5 years was too short a period; he did not regard it as being set in stone. (Q 123)

113. It seems to us that the correct period is the shortest reasonable period which will allow law enforcement and counter-terrorism investigators to do their work properly. Fixing a precise time limit seems to us to be less important than ensuring that the data, for so long as they are kept, are kept and handled securely and used only for the permitted purposes, and that an adequate redress mechanism is in place.

114. **We are prepared to accept that routine retention of data for longer than 3.5 years may be necessary, and may be acceptable so long as the data are kept and handled securely. What is not acceptable is for these data to be used in that time for purposes other than those strictly permitted under the Agreement.**

Data sharing

115. We have explained in paragraphs 61 and 62 how, while Undertakings 28 to 33 allow the sharing of PNR data with other Government authorities (including other components of DHS) only on a case by case basis and subject to stringent limitations, United States law now requires DHS to facilitate the disclosure of such data to any authorities exercising counter-terrorism functions which need such data. The Baker letter states that DHS will not provide "unconditional direct electronic access", but does not state what conditions will apply. We are told that "DHS will ensure that such authorities will respect comparable standards of data protection to that applicable to DHS, in particular in relation to purpose limitation, data retention, further disclosure, [and other matters]."

116. This is an aspect of the Baker letter which causes us great disquiet. Personal and private information which was intended only for CBP within DHS is now being disclosed to the rest of DHS, and by DHS to other authorities, on a bulk basis. We were told by Mr Bunyan that some 1,500 agencies at federal, State and local level might be involved in this work.[52] Once further

---

51 Commitment 8.

52 Q130, and supplementary evidence p 39.

disclosure is made on the same basis by one authority exercising counter-terrorism functions to another such authority, and perhaps at one or more further removes, it is hard to see what control will be retained by CBP, still less by the EU. This has particular implications for the identification and correction of errors in the data, a matter we consider below.

117. It is vital that the new Agreement should address this issue. There is a world of difference between Undertakings "not impeding" the use or disclosure of PNR data as required by United States law, and Undertakings for practical purposes scarcely applying at all to further data sharing. We are prepared to accept that there will be circumstances where the sharing of such data by CBP with other parts of DHS and with other authorities will be not only desirable but necessary. We have in any case to accept that this is now what United States law requires. What we cannot accept is that CBP, and the EU, should lose all control over such data sharing.

118. **If United States government authorities with whom data are shared by CBP believe that other authorities need access to such data, the decision must be for CBP. Access should be subject to the same undertakings as CBP has given. Records of this data sharing should be kept for independent inspection.**

119. **It may not always be possible for data to be scrutinised on a case by case basis before they are shared with other authorities, but indiscriminate bulk sharing should not be permitted. It must be for CBP to "push" the information to other authorities, not for those authorities to "pull" it from the CBP database.**

Rights of redress

120. In Undertaking 36 CBP states that it will inform the travelling public about the uses to which their PNR data are put, the applicable conditions, and the procedures for redress. Such information may be in the small print on a travel agent's conditions, or passengers may have to access CBP's website.

121. Those passengers—the data subjects—who do discover that information about them is held by CBP may if they wish write to CBP in Washington DC asking to see a copy. Under the United States Freedom of Information Act this will be disclosed—unless "in exceptional circumstances" CBP denies or postpones disclosure.

122. Requests for rectification of data, or complaints about the uses to which data are put, may be made to the US authorities; if unresolved, the complaint can be referred to the DHS Chief Privacy Officer. If an EU data subject is supported by the data protection authority of his Member State, there is an expedited procedure. Baroness Ashton told us that there is now an on-line Travel Redress Inquiry Program (TRIP) allowing passengers to ask for their information to be reviewed. (Q 66) But ultimately, the final decision rests with the authorities rather than the courts, because the Privacy Act of 1974 applies only to United States citizens and residents.

123. One of the most frequent complaints is about being on a no-fly list. A would-be passenger will very likely not be aware that he is on a no-fly list unless and until he attempts to fly to the United States. At that stage he will discover that he is on the list, but very likely he will not be aware of the reason. He

will be in an unenviable position—a position shared by at least 30,000 other passengers.[53] It is as easy for someone to be placed on a no-fly list as it is difficult to be removed from that list even if the entry can be shown to be unjustified. **The negotiators must stress how serious it is for an individual to be wrongly placed on a no-fly list, and must ensure that provision is made for rapid access to an enforceable means of redress.**

Pull v Push

124. The 2004 Agreement provides:

> "CBP may electronically access the PNR data from air carriers' reservation/departure control systems (reservation systems) located within the territory of the Member States of the European Community … only until there is a satisfactory system in place allowing for the transmission of such data by the air carriers."

In the words of Undertaking 13 "CBP will 'pull' passenger information from air carrier reservation systems until such time as air carriers are able to implement a system to 'push' the data to CBP."

125. It has always been clear that the United States prefers to "pull" data because this gives it control over when and how often it does so. Despite the fact that the airlines are able and willing to "push" the data, the 2006 Agreement in substance repeats the words of the 2004 Agreement, and the Baker letter qualifies this further by stating:

> "The push system does not confer on airlines any discretion to decide when, how or what data to push, however. That decision is conferred on DHS by US law."

We note that while United States legislators can confer what duties they please on DHS, it does not follow that they can by law require air carriers outside their jurisdiction to cease to exercise their discretion in deciding what data to "push". But they do have other sanctions at their disposal to enforce their views.

126. In his statement to the European Parliament on 11 October 2006 to which we referred in paragraph 86, Vice-President Frattini said: "It has been agreed that the new ['push'] mechanism … will come into operation no later than December 2006, that is within a month and a half at the latest"—i.e. by the beginning of December. The Information Commissioner told us, in evidence dated 5 March 2007, that the delays in moving to a "push" system were a major concern to the Article 29 Working Party. Baroness Ashton assured us that "[t]he ambition will be, by the time we have finished the negotiations, it will be a Push system." (Q 69)

127. On 22 March 2007 Mr Faull told us that the situation was mixed: some airlines had switched to "push" but there was still some "pulling"; it was a purely technical issue. It seems to us however that there are no longer any technical issues; the issues are whether there are any advantages to airlines in going over to a "push" system if they are going to have to "push" data whenever requested by the US authorities. Under the Canada Agreement the airlines have always operated a "push" system; Canada requires a single "push" of data at departure. This, in the view of Virgin Atlantic, "places far

---

[53] Faull Q187; Paper prepared by the Article 29 Working Party for the seminar on 26 March 2007.

less burden on the airlines than the four pushes required by the US plus a mechanism for obtaining additional ad hoc pushes on request." This was the view of BA:

> "BA is concerned about how the ad hoc Push should operate. One option, not preferred by BA, is to provide manpower to manually send PNR data when an ad hoc Pull of PNR data is requested by the authority. BA would prefer to automate the system so that the reservations system automatically generates PNR data on request. BA acknowledges that there is little difference between this and a Pull system."

128. The British Air Transport Association (BATA), the trade association for UK-registered airlines, summarised the position as follows:

> "The US wish to retain their current mechanism for obtaining data (a data 'pull'). However, the EU feel that this does not afford adequate protection as data is freely available, is not filtered and is not restricted to relevant flights. This means that we are trying to implement a solution that the US does not really want, and hence it is difficult to progress with clarity on how this should work. Any new Agreement needs to clearly resolve these issues and provide adequate time for compliance." (p 54)[54]

129. The US authorities seem to us to be regretting their Undertaking, given three years ago, to change from a "pull" to a "push" system as soon as the airlines were technically ready, and are doing all they can to ensure that they retain the ability to access the databases of airlines whenever and as often as they like. In doing so they are placing an unacceptable burden on the airlines, which bear the full cost of the exercise. We see no reason why they should not, like the Canadians, be satisfied with a single "push" of data at the time of departure.

130. **The negotiators should ensure that the United States honours the commitment given three years ago to move to a system allowing the airlines to "push" the data to them, and should insist on a single "push" of data at the time of departure.**

Review of the working of the Agreement

131. The 2004 Agreement provides that CBP and the Commission will "jointly and regularly" review the implementation of the Agreement. Undertaking 43 is more detailed:

> "CBP, in conjunction with DHS, undertakes to conduct once a year, or more often if agreed by the parties, a joint review with the European Commission assisted as appropriate by representatives of European law-enforcement authorities and/or authorities of Member States of the European Union on the implementation of these Undertakings …"

132. There has been one such review, in September 2005. The planned 2006 review was cancelled because of the negotiations on the Interim Agreement. The Baker letter simply states, without apology, that "the question of how and whether to conduct a joint review in 2007 will be addressed during the discussions regarding a future agreement."

---

54 The individual views of Virgin Atlantic and BA were made available to us by BATA.

133. The report of the 2005 Review which was published is singularly uninformative because the US authorities insisted that it should be very heavily "redacted". Much that might have been of interest was blanked out, down to the names of those taking part. Access by the high-level EU officials to a number of records was limited, and they were required to sign confidentiality agreements exposing them to criminal sanctions for any breach. We agree with Mr Bunyan that this is not the way in which two equal partners should work. (Q 127)

134. Mr Faull told us that "the Americans found the Joint Review useful, important, but also extremely cumbersome. It occupied a lot of their time, and I would not be surprised if they sought in the negotiations a somewhat lighter form of review in a new Agreement". (Q 141) Reading between the lines, this no doubt is what they had already requested: that, or no review at all. If this is the case, it will be contrary to the views of all our witnesses.

135. Baroness Ashton said: "Yes, it [the review] is an important mechanism; yes, I think it has worked well; yes, I think it should be part of the next stage." (Q 65) The Assistant EDPS told us that "The fact that a mechanism of revision has to take place is fundamental … the mechanism has to be there, it is crucial." (Q 212) The Information Commissioner believes that "the continuation of the annual joint review mechanism is an essential safeguard that will help ensure compliance with restrictions such as those on wider use." (p 57) The importance of a regular independent audit was also stressed by Mr Schaar at the Brussels seminars on 26 March 2007.

136. The view of Professor Elspeth Guild was:

> "There must be a full review of the application of the agreement; any issues in respect of differences in interpretation on the meaning of the agreement and the application of the agreement need to be specified … the report … needs to be published, it needs to be timely and it needs to provide an opportunity for additional opinions by those who have been responsible for carrying out the review." (Q 129)

We agree. We would in particular like to see reports setting out in detail the degree to which data are shared by CBP with other US authorities, and the conditions applying to such data sharing.

137. **The new Agreement must provide for thorough annual reviews of the working of the PNR Agreement, and the parties must ensure that they take place as intended. The EDPS and national data protection authorities must take part. The EU team must be allowed the fullest access to data to enable it to assess the value of PNR data in the fight against terrorism.**

138. **This is an Agreement between equal parties. The EU team should not have to sign general non-disclosure agreements, even though there will of course be matters which they will agree not to disclose**.

139. **Reports of reviews should set out in detail the degree to which data are shared by CBP with other US authorities, and the conditions applying to such data sharing.**

140. **Reports of reviews must be published. Any editing of a report prior to publication should be confined to what is strictly necessary for security reasons.**

CHAPTER 7: OTHER DEVELOPMENTS

141. Some of the evidence we have received on the current PNR Agreements, and on the negotiations for a new Agreement, has included views on the Visa Waiver Program and on other peripheral but related PNR matters which are of interest: the possibility of a global approach, the desirability of other EU initiatives, and current United Kingdom developments. It may be useful if we refer to these matters briefly, even though they are not strictly part of our inquiry.

Visa Waiver Program

142. United States citizens do not need a visa to enter any of the Member States of the EU, but the converse is not true. Nationals of Greece[55] and of the twelve States which have acceded to the EU since 1 May 2004, other than Slovenia, still need visas to enter the United States. This is based on the fact that over 3% of their nationals who apply for a visa are refused one. However this threshold is now being raised to 10%,[56] which will allow many of these States to join the Visa Waiver Program (VWP).[57]

143. A visa application allows the United States to ask what questions it wishes, and to refuse entry, at an earlier stage, but the information from a visa application tells the authorities much less about the conduct of the applicant than PNR. Information obtained from PNR is not an alternative to information obtained from visas, but complements it. There is no formal link between the two, but there is a political link: the current negotiations allow the EU to press the case for the VWP to be extended to the Member States which do not yet participate in it.

144. We were told by Dr Hosein that Congress would like to shut down the VWP if it could, since they do not like the idea of anyone coming to the US without a visa. Officials are more realistic: they know that the VWP is good for trade. (Q 24) They would not want US citizens to have to apply for visas to Western Europe, and the processing of visa applications is so resource intensive that it would be unrealistic to have to go back to this.

A global approach to PNR?

145. In general, States have the right to control flights into, out of and over their territories, and they do so. The United States is exceptional only in the number of air passengers who seek entry, the risks which they pose (or are seen as posing), and hence the volume of PNR data sought and the uses to which they are put.

146. The different approaches taken by individual States are already apparent. The Information Commissioner told us:

> "The Information Commissioner and the Article 29 Working Party believe that as air transport operates on a global basis, a global solution to the PNR issue is desirable. An instrument established under the

---

55 Greece is the only State of the EU–15 whose nationals still need visas for the US.

56 Meeting with Secretary Chertoff on 5 April 2007; Council Document 8282/07.

57 The twelve non-EU States which participate in the VWP are Andorra, Australia, Brunei, Iceland, Japan, Liechtenstein, New Zealand, Norway, San Marino, Singapore and Switzerland.

> auspices of the International Civil Aviation Organisation (ICAO) could set out a common set of data items and procedures that all states could follow. This would be preferable to each state specifying its own requirements and then concluding an ever increasing number of bilateral agreements. Achieving a common international instrument with appropriate data protection safeguards would ensure a consistent approach and reduce confusion for airlines and passengers." (p 57)

147. This may be a long-term goal, but we believe this is a suggestion well worth pursuing.

A common EU approach to the use of PNR

148. The current Agreements between the EU and the United States, and between the EC and Canada, are designed to enable the United States and Canada respectively to receive PNR data from Europe. However we have already explained[58] that, unlike the US Agreement, the Canada Agreement is drafted in a way which would enable it to be used to govern the transfer of PNR data from Canada to Europe.

149. Undertaking 45 of the US Agreement states that, if a system is implemented in the EU requiring carriers to provide EU authorities with PNR data for passengers travelling to or from the EU, CBP will "encourage US-based airlines to cooperate"—a rather grudging offer. In the case of the Canada Agreement, by contrast, Commitment 40 explains that section 4.83 of the Canadian Aeronautics Act allows Canadian air carriers operating flights from any destination, or any carriers operating flights departing from Canada, to provide a foreign State with PNR information about passengers flying to that State, where the law of that State requires this; and Commitment 41 states that this would apply to the EU if it or any of its Member States passes laws requiring access to API and PNR data for persons travelling to the EU.

150. Mr Faull told us: "The Commission's view is that it would make sense to have a PNR system for ourselves in the European Union on the basis of which we would then have very good grounds for saying to our American partners, 'This must be completely reciprocal. We have our PNR system, you have yours'". But he added that he did not see any enthusiastic demand among Member States for this. Those that needed such information had set up national systems. (QQ 179–180)

151. The EU Action Plan for Combating Terrorism, updated in September 2006, calls for the development and implementation of the exchange and analysis of PNR. To help assess the different policy options the Commission sent questionnaires to Member States, data protection authorities and airline associations. The questionnaire sent to airline associations on 19 December 2006 specifically sought their views on the likely cost to them of the different options. BATA sent us a copy of the response of the Association of European Airlines (AEA). This was not a very positive response; it explained that AEA airlines had no wish to be involved in law enforcement functions unconnected with security and safety, and emphasised the considerable burdens which such an exercise would place on the airlines.

152. We sympathise with the AEA in the desire of its members not to become involved in general law enforcement functions. However we believe that a

---

[58] Paragraph 93.

common EU approach to the use of PNR for the purposes for which it was originally intended under the US Agreement must come sooner rather than later, and we welcome the Commission's work. We understand that a draft Framework Decision may be brought forward later this year.[59]

United Kingdom initiatives

153. In oral evidence Ms Ryan told us a little about United Kingdom initiatives (QQ 52–57), and she amplified this in a letter to the Chairman of 30 March 2007 (p 19). There was also a presentation by a Home Office official to the March seminars.[60]

154. e-Borders is an initiative to improve United Kingdom border control by enhancing joint working between border agencies. It involves Customs, the Intelligence Agencies, the Police and United Kingdom visas, and is coordinated by the Home Office. The Department for Work and Pensions and the Passport Service are among other beneficiaries. Operating capability is planned for July 2008, with full capability by 2014.

155. Project Semaphore is the pilot project for e-Borders which was launched in November 2004. It collects both API and PNR from 40 carriers on 72 routes; currently this amounts to 20.9 million annualised passenger movements, and by April 2008 the figure may be 30 million. It has so far resulted in some 900 arrests for crimes including murder, rape, drug and tobacco smuggling and passport offences. Checks have also led to the identification of holders of fraudulently obtained passports who have consequently been refused leave to enter the United Kingdom. Ms Ryan told us that in January 2007 23 successes were recorded by Project Semaphore as a result of automated profiling based on passenger data. (p 19)

156. Any increased detection of crimes or immigration offences is welcome, but we have yet to hear that the collection of these data has led to successes in combating terrorism or serious cross-border crime. However we appreciate that Project Semaphore is only a pilot project, and we hope that it, and e-Borders, will in time show their full potential.

---

59 Supplementary evidence from Ms Ryan, p 20.

60 See paragraph 87.

CHAPTER 8: SUMMARY OF CONCLUSIONS AND RECOMMENDATIONS

157. It is the perennial conflict between the security of the public and the privacy of the individuals who make up the public which is at the heart of our inquiry. A balance has to be struck, and the guiding consideration must be the principle of proportionality: the collection and retention of data for security purposes must be no more invasive of individual privacy than is necessary to achieve the objective for which they are collected. That objective must be narrowly and clearly defined. (paragraph 5)

Passenger Name Records

158. It is an important principle of democratic accountability that Parliament should be able to reach its own conclusions on the value of PNR in combating terrorism, and not have to rely on statements from the executive. This would help to secure public confidence. (paragraph 22)

159. Nonetheless, having received no evidence to the contrary, we are prepared to accept that PNR data constitute a valuable weapon in the fight against terrorism and serious crime, and that their continued use is both necessary and justified. (paragraph 23)

160. The principal risk of error in using PNR data seems to us to arise, not from the quality of the data, but from the erroneous interpretation of the data, even if accurate. (paragraph 27)

161. It is important that intending passengers should be aware of who will receive their personal data, and subject to what conditions. We agree with the Working Party of national data protection authorities that the airlines should be responsible for informing passengers, and we endorse the Working Party's proposals. (paragraph 49)

The Interim Agreement

162. The negotiators should as a matter of principle insist that data transferred under the 2004 and 2006 Agreements must be destroyed no later than 3.5 years after the transfer, unless a formal Agreement is negotiated allowing these data to be retained longer. (paragraph 72)

163. Whatever the justification for extending data elements, for wider sharing of data, or for using data to identify possible carriers of dangerous communicable diseases, there is no justification at all for doing so through a unilateral declaration by one of the parties to an agreement. (paragraph 76)

164. An undertaking which includes a provision allowing the party giving it to amend it virtually at will is of very limited value, and scarcely deserves the name. No such provision should be included in any future agreement. (paragraph 77)

Negotiations for a new Agreement

165. In our view the worst possible result of the negotiations would be an agreement to extend the current Interim Agreement. (paragraph 84)

The views of the European Parliament and the data protection authorities

166. The fact that the European Parliament no longer has a formal role to play is not a reason why the views of its members should be disregarded. On the contrary, in a Union of democracies special attention must be paid to the views of representatives, since they are well placed to balance the public good against private rights. (paragraph 89)

167. The European Data Protection Supervisor, and national data protection authorities individually and collectively in the Article 29 Working Party, have great experience of the practical working of data protection laws and of non-binding declarations on the handling of personal data. Those negotiating a new agreement should be guided by their opinions. (paragraph 90)

The EC/Canada PNR Agreement

168. We believe that the PNR Agreement with Canada could be a useful starting point for the negotiations with the United States. (paragraph 92)

Data elements

169. We expect those negotiating the new Agreement to take a robust attitude in the negotiations before being satisfied that any additional data item is essential and therefore permissible. (paragraph 97)

170. It would be wrong to include among the agreed data elements open-ended data elements like "general remarks" or "open fields", which merely serve as a means of introducing other data elements not specifically listed. (paragraph 99)

Undertakings

171. We hope that the talks will have started on the basis that the Undertakings being negotiated, unlike the current ones, are legally binding on the United States authorities. (paragraph 100)

172. All the terms of the Undertakings being negotiated must be specific, unequivocal, contained in the document itself, and not susceptible of amendment without the agreement of all the parties. (paragraph 102)

173. If any clarification is needed, this is a matter for subsequent open negotiation between the parties. There can be no scope for amendment by unilateral "interpretation" of the Undertakings. (paragraph 103)

Purpose limitation

174. Under the 2004 Agreement the use of PNR data was to be limited to:

- the prevention and combating of terrorism and related crimes;
- other serious crimes, including organised crime, that are transnational in nature; and
- flights from warrants or custody for these crimes.

The negotiators should seek to retain these limitations in the new Agreement. (paragraph 107)

175. We believe that the use of PNR data for general law enforcement purposes, as opposed to countering terrorism and serious crime, is undesirable and unacceptable. (paragraph 108)

176. If, contrary to our view, it is agreed that data should be used for other purposes, those purposes must be specifically listed at the outset. Words such as "vital interests of the data subject" are too vague. (paragraph 109)

Retention of future data

177. We are prepared to accept that routine retention of data for longer than 3.5 years may be necessary, and may be acceptable so long as the data are kept and handled securely. What is not acceptable is for these data to be used in that time for purposes other than those strictly permitted under the Agreement. (paragraph 114)

Data sharing

178. If United States government authorities with whom data are shared by the Bureau for Customs and Border Protection (CBP) believe that other authorities need access to such data, the decision must be for CBP. Access should be subject to the same undertakings as CBP has given. Records of this data sharing should be kept for independent inspection. (paragraph 118)

179. It may not always be possible for data to be scrutinised on a case by case basis before they are shared with other authorities, but indiscriminate bulk sharing should not be permitted. It must be for CBP to "push" the information to other authorities, not for those authorities to "pull" it from the CBP database. (paragraph 119)

180. The negotiators must stress how serious it is for an individual to be wrongly placed on a no-fly list, and must ensure that provision is made for rapid access to an enforceable means of redress. (paragraph 123)

"Pull" v "Push"

181. The negotiators should ensure that the United States honours the commitment given three years ago to move to a system allowing the airlines to "push" the data to them, and should insist on a single "push" of data at the time of departure. (paragraph 130)

Review of the working of the Agreement

182. The new Agreement must provide for thorough annual reviews of the working of the PNR Agreement, and the parties must ensure that they take place as intended. The EDPS and national data protection authorities must take part. The EU team must be allowed the fullest access to data to enable it to assess the value of PNR data in the fight against terrorism. (paragraph 137)

183. This is an Agreement between equal parties. The EU team should not have to sign general non-disclosure agreements, even though there will of course be matters which they will agree not to disclose. (paragraph 138)

184. Reports of reviews should set out in detail the degree to which data are shared by CBP with other US authorities, and the conditions applying to such data sharing. (paragraph 139)

185. Reports of reviews must be published. Any editing of a report prior to publication should be confined to what is strictly necessary for security reasons. (paragraph 140)

Report

186. We recommend this Report to the House for debate. (paragraph 8)

APPENDIX 1: SUB-COMMITTEE F (HOME AFFAIRS)

The members of the Sub-Committee which conducted this inquiry were:

Baroness Bonham-Carter of Yarnbury
Earl of Caithness
Baroness D'Souza
Lord Foulkes of Cumnock
Lord Harrison
Baroness Henig
Lord Jopling
Earl of Listowel
Lord Marlesford
Lord Teverson
Lord Wright of Richmond (Chairman)

Declarations of Interests:

A full list of Members' interests can be found in the Register of Lords Interests:

http://www.publications.parliament.uk/pa/ld/ldreg.htm

Interests declared by Members relevant to this inquiry

Lord Foulkes of Cumnock
Member, Intelligence and Security Committee

Baroness Henig
Chair of the Security Industry Authority
President of the Association of Police Authorities

Lord Wright of Richmond
Former Chairman, Joint Intelligence Committee

APPENDIX 2: LIST OF WITNESSES

The following witnesses gave evidence. Those marked * gave oral evidence.

British Air Transport Association (BATA)

* Centre for European Policy Studies (CEPS)

* Department for Constitutional Affairs (DCA) (since 9 May 2007 the Ministry of Justice)

Department for Transport Aviation Directorate

* European Commission, Directorate-General Justice, Freedom & Security (D-G JLS)

* European Data Protection Supervisor (EDPS)

Professor Paul de Hert , Tilburg Institute for Law, Technology and Society, The Netherlands, and Vrije Universiteit, Brussels; Ms Gloria González Fuster, Researcher, Institute for European Studies, Vrije Universiteit, Brussels

* Home Office

* Dr Gus Hosein, Visiting Scholar, American Civil Liberties Union

Office of the Information Commissioner

* Statewatch

APPENDIX 3: LETTER FROM THE SECRETARY OF HOMELAND SECURITY TO MEMBERS OF THE EUROPEAN PARLIAMENT

May 14, 2007

Dear Member of the European Parliament,

Thank you for the opportunity to appear today before the Committee on Civil Liberties, Justice and Home Affairs to further our important dialogue on matters critical to the security of the European Union and the United States.

We face a shared challenge in preventing acts of terrorism against our countries and our citizens. At the same time, we share a fundamental and unwavering commitment to protect the civil liberties and privacy that are the hallmarks of all free and democratic nations.

Recent terrorist attacks in Algeria and Morocco, as well as earlier attacks in Madrid and London, the foiled plot this past August against transatlantic aircraft bound for the United States, and the recent convictions of five British terrorists, underscore the serious, nature of the threat we face and the importance of developing common tools and approaches to counter this global menace.

One of these tools is Passenger Name Record (PNR) data, which is a limited set of information provided by air passengers travelling between Europe and the United States. PNR data, used in combination with passenger manifest data, allows U.S. officers to check passenger names and other basic information against lists of known or suspected terrorists and criminals so that we can enhance screening of dangerous people and prevent them from boarding commercial aircraft.

Combined with other intelligence, we use PNR data to check for links that might reveal unknown terrorist connections, such as a traveler who has provided contact information overlapping with a known terrorist. It is our ability to identify these hidden links that has made PNR so valuable to our counterterrorism efforts and the reason it is imperative we reach a new understanding regarding how this information will continue to be shared and protected.

Below are several examples of how analyzing PNR data has prevented dangerous individuals from entering the United States.

In June 2003, using PNR data and other analytics, one of our inspectors at Chicago's O'Hare airport pulled aside an individual for secondary inspection and questioning. When the secondary officers weren't satisfied with his answers they took his fingerprints and denied him entry to the United States. The next time we saw those fingerprints—or at least parts of them—they were on the steering wheel of a suicide vehicle that blew up and killed 132 people in Iraq.

In January 2003, Customs and Border Protection (CBP) officers in Miami used PNR to disrupt an internal conspiracy within an airline that was smuggling cocaine between Venezuela and Miami. A corrupt ticket counter agent would identify low risk travelers (typically families) and add an additional bag to their reservation after they departed the ticket counter. This bag would be filled with cocaine. Corrupt airline employees in Miami plotted to remove the added bags from circulation prior to inspection by CBP in Miami.

On March 11, 2005, CPB arrested two individuals for smuggling drugs from London to Chicago. Their PNR information revealed the use of common credit cards. This credit card's reservation history denied a third traveler who had used the same card and listed a second credit card. Analysis of this new credit card

number identified three additional travelers. Three of the four travelers were arrested during subsequent travel for drug smuggling.

In January 2006, CBP officers used PNR data to identify a passenger posing a high risk for document fraud. The passenger, posing as a citizen of Singapore, was scheduled to depart Korea for the United States. The subject's travel itinerary was targeted by a query using data from recent cases of document fraud in Sri Lanka. CBP officers contacted airline representatives in Korea and requested assistance in verifying the traveler's documents. With airline assistance, CBP determined the subject's travel document was a counterfeit Singapore passport. The subject was in possession of his Sri Lankan passport. The subject was also a positive match to the Transportation Security Administration's No Fly List and suspected of being an armed and dangerous terrorist. The subject was denied boarding for the flight. He was subsequently stopped on another date using the same method of PNR targeting. In the second incident, he attempted to travel to the U.S. using a counterfeit UK passport.

In February 2006, CBP officers used PNR data to identify a passenger with a high-risk for narcotics possession arriving from the Dominican Republic. The subject, a returning U.S. legal permanent resident, purchased his ticket using cash and made certain changes to his reservation. Upon arrival, the subject was selected for an enforcement exam. During an examination of the subject's personal effects, CBP officers discovered two packages containing heroin. The subject was placed under arrest and turned over to Immigration and Customs Enforcement for prosecution.

At Boston Logan Airport in April 2006, CBP officers used PNR data to identify two passengers whose travel patterns exhibited high-risk indicators. During the secondary interview process, one subject stated that he was traveling to the United States on business for a group that is suspected of having financial ties to Al Qaeda. The examination of the subject's baggage revealed images of armed men, one of which was labelled "Mujahadin." Both passengers were refused admission.

In May 2006, PNR analysis identified a high-risk traveler arriving at Atlanta Hartsfield airport from Europe. CBP officers determined that the individual's visa was issued one week prior to September 11, 2001, yet he had never travelled to the United States. The subject's passport listed him as a "flight instructor" and his reasons for traveling to the United States included the plan to "see a man in New York for two days." The individual was ultimately linked to numerous individuals who U.S. law enforcement regards as security risks and immigration violators. The passenger was denied admission.

In May 2006, CBP officers used PNR data to target a high-risk passenger arriving from Amsterdam. Officers linked the subject to a split PNR; the second traveler was a Palestinian who previously claimed political asylum. The high-risk passenger was also identified through a known telephone number used by terrorist suspects contained within his PNR. Upon arrival the subject applied for admission as a Jordanian citizen and was referred to secondary inspection for further examination. The subject revealed that his purpose of travel was to visit a relative for thirty days. During the secondary inspection, the subject revealed that he had been arrested and convicted on terrorist related charges in a third country. The subject also admitted to being a former member of an organization that espoused political views and supported violent acts that include suicide bombings. The Joint Terrorism Task Force and Immigration and Customs. Enforcement were contacted and responded to interview the subject. Upon completion of the

interview the subject claimed credible fear of returning to Jordan. He later recanted and was expeditiously removed from the United States. .

If such a system had been fully developed before 9/11, we might have been spared that tragedy. Consider this: two hijackers, Nawaq Alhamzi, appeared on a watch list and would have been "flagged" when they purchased their tickets. Through analysis of their PNR data, we could have learned that three other hijackers—including Mohammed Atta—used the same address as Alhamzi and Al-Midhar; five other hijackers used the same telephone number as Atta; and still one other used the same frequent flyer number. The analysis of PNR and other basic data that we use today would have flagged all nineteen hijackers as connected to Alhamzi and Al-Midhar. If we surrender this tool, we will abandon the real-time defenses that can save our citizens' lives.

These concrete examples illustrate the necessity of analyzing and sharing PNR data. But it is also important to note the strong privacy protections in place to safeguard this information. PNR data is protected under the U.S. Privacy Act and the Freedom of Information Act, among other laws, as well as the robust oversight provided through the U.S. Congress, American courts, and internal controls such as the Department of Homeland Security's Privacy Office, Inspector General, and Government Accountability Office. In addition, our policies ensure that records pertaining to foreign nationals are properly protected. PNR data is also used in strict accordance with U.S law. Our officers make determinations based on relevant criteria developed from investigative and intelligence work. PNR data does not alone tell us who is and who isn't a terrorist. It simply helps our officers make a more complete and informed assessment at the border to decide who warrants further scrutiny prior to entry. And PNR data is not used to create a "risk score" that remains with an individual or automatically adds a person to a terrorist watch list.

One of the central lessons of the 9/11 attacks, and subsequent attacks in Europe and elsewhere, is that we must break down barriers to information sharing. That same lesson must extend to our use of PNR data. We must not take this valuable counter-terrorism tool away from border law enforcement professionals by limiting or restricting the kind of information sharing and analysis that has already proven effective.

I appreciate the time you have given me today to address the Committee, and I look forward to working with you as we seek new ways to strengthen international cooperation in our fight against terrorism while protecting the fundamental rights and liberties we all cherish.

Sincerely,

Michael Chertoff

APPENDIX 4: COMMISSION ADEQUACY DECISION, UNDERTAKINGS AND PNR DATA ELEMENTS

Commission Decision of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection [61]

THE COMMISSION OF THE EUROPEAN COMMUNITIES,

Having regard to the Treaty establishing the European Community,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data 62, and in particular Article 25(6) thereof,

Whereas:

(1) Pursuant to Directive 95/46/EC, Member States are required to provide that the transfer of personal data to a third country may take place only if the third country in question ensures an adequate level of protection and if the Member States' laws implementing other provisions of the Directive are complied with prior to the transfer.

(2) The Commission may find that a third country ensures an adequate level of protection. In that case, personal data may be transferred from the Member States without additional guarantees being necessary.

(3) Pursuant to Directive 95/46/EC the level of data protection should be assessed in the light of all the circumstances surrounding a data transfer operation or a set of data transfer operations, particular consideration being given to a number of elements relevant for the transfer and listed in Article 25(2) thereof.

(4) In the framework of air transport, the "Passenger Name Record" (PNR) is a record of each passenger's travel requirements which contains all information necessary to enable reservations to be processed and controlled by the booking and participating airlines. For the purposes of this Decision, the terms "passenger" and "passengers" include crew members. "Booking airline" means an airline with which the passenger made his original reservations or with which additional reservations were made after commencement of the journey. "Participating airlines" means any airline on which the booking airline has requested space, on one or more of its flights, to be held for a passenger.

(5) The United States Bureau of Customs and Border Protection (CBP) of the Department of Homeland Security (DHS) requires each carrier, operating passenger flights in foreign air transportation to or from the United States, to provide it with electronic access to PNR to the extent that PNR is collected and contained in the air carrier's automated reservation system.

---

61 OJ L235, 6.7.2004, p 11.

62 OJ L 281, 23.11.1995, p 31. Directive as amended by Regulation (EC) No 1882/2003 (OJ L 284, 31.10.2003, p. 1).

(6) The requirements for personal data contained in the PNR of air passengers to be transferred to CBP, are based on a statute enacted by the United States in November 2001 [63] and upon implementing regulations adopted by CBP under that statute[64].

(7) The United States legislation in question concerns the enhancement of security and the conditions under which persons may enter and leave the country, matters on which the United States has the sovereign power to decide within its jurisdiction. The requirements laid down are not, moreover, inconsistent with any international commitments which the United States has undertaken. The United States is a democratic country, governed by the rule of law and with a strong civil liberties tradition. The legitimacy of its law-making process and strength and independence of its judiciary are not in question. Press freedom is a further strong guarantee against the abuse of civil liberties.

(8) The Community is fully committed to supporting the United States in the fight against terrorism within the limits imposed by Community law. Community law provides for striking the necessary balances between security concerns and privacy concerns. For example, Article 13 of Directive 95/46/EC provides that Member States may legislate to restrict the scope of certain requirements of that Directive, where it is necessary to do so for reasons of national security, defence, public security and the prevention, investigation, detection and prosecution of criminal offences.

(9) The data transfers concerned involve specific controllers, namely airlines operating flights between the Community and the United States, and only one recipient in the United States, namely CBP.

(10) Any arrangement to provide a legal framework for PNR transfers to the United States, in particular through this Decision should be time-limited. A period of three and a half years has been agreed. During this period, the context may change significantly and the Community and the United States agree that a review of the arrangements will be necessary.

(11) The processing by CBP of personal data contained in the PNR of air passengers transferred to it is governed by conditions set out in the Undertakings of the Department of Homeland Security Bureau of Customs and Border Protection (CBP) of 11 May 2004 (hereinafter referred to as the Undertakings) and in United States domestic legislation to the extent indicated in the Undertakings.

(12) As regards domestic law in the United States, the Freedom of Information Act (FOIA) is relevant in the present context in so far as it controls the conditions under which CBP may resist requests for disclosure and thus keep PNR confidential. The Act governs the disclosure of PNR to the person whom it concerns, closely linked to the data subject's right of access. It applies without distinction to United States and non-United States citizens.

(13) As regards the Undertakings, and as provided in paragraph 44 thereof, the statements in the Undertakings will be, or have already been, incorporated in statutes, regulations, directives or other policy instruments in the United States and will thus have varying degrees of

---

[63] Title 49, United States Code, section 44909(c)(3).

[64] Title 19, Code of Federal Regulations, section 122.49b.

legal effect. The Undertakings will be published in full in the Federal Register under the authority of the DHS. As such, they represent a serious and well considered political commitment on the part of the DHS and their compliance will be subject to joint review by the United States and the Community. Non-compliance could be challenged as appropriate through legal, administrative and political channels and, if persistent, would lead to the suspension of the effects of this Decision.

(14) The standards by which CBP will process passengers' PNR data on the basis of United States legislation and the Undertakings cover the basic principles necessary for an adequate level of protection for natural persons.

(15) As regards the purpose limitation principle, air passengers' personal data contained in the PNR transferred to CBP will be processed for a specific purpose and subsequently used or further communicated only in so far as this is not incompatible with the purpose of the transfer. In particular, PNR data will be used strictly for purposes of preventing and combating: terrorism and related crimes; other serious crimes, including organised crimes, that are transnational in nature; and flight from warrants or custody for those crimes.

(16) As regards the data quality and proportionality principle, which need to be considered in relation to the important public interest grounds for which PNR data are transferred, PNR data provided to CBP will not subsequently be changed by it. A maximum of 34 PNR data categories will be transferred and the United States authorities will consult the Commission before adding any new requirements. Additional personal information sought as a direct result of PNR data will be obtained from sources outside the government only through lawful channels. As a general rule, PNR will be deleted after a maximum of three years and six months, with exceptions for data that have been accessed for specific investigations, or otherwise manually accessed.

(17) As regards the transparency principle, CBP will provide information to travellers as to the purpose of the transfer and processing, and the identity of the data controller in the third country, as well as other information.

(18) As regards the security principle, technical and organisational security measures are taken by CBP which are appropriate to the risks presented by the processing.

(19) The rights of access and rectification are recognised, in that the data subject may request a copy of PNR data and rectification of inaccurate data. The exceptions provided for are broadly comparable with the restrictions which may be imposed by Member States under Article 13 of Directive 95/46/EC.

(20) Onward transfers will be made to other government authorities, including foreign government authorities, with counter-terrorism or law-enforcement functions, on a case-by-case basis, for purposes that correspond to those set out in the statement of purpose limitation. Transfers may also be made for the protection of the vital interests of the data subject or of other persons, in particular as regards significant health risks or in any criminal judicial proceedings or as otherwise required by law. Receiving agencies are bound by the express terms of disclosure to

use the data only for those purposes and may not transfer the data onwards without the agreement of CBP. No other foreign, federal, State or local agency has direct electronic access to PNR data through CBP databases. CBP will refuse public disclosure of PNR, by virtue of exemptions from the relevant provisions of FOIA.

(21) CBP does not use sensitive data as referred to in Article 8 of Directive 95/46/EC, and, until a system of filters to exclude such data from PNR transferred to the United States is in place, undertakes to introduce the means to delete them and in the meantime not to use them.

(22) As regards the enforcement mechanisms to ensure compliance by CBP with these principles, the training and information of CBP staff is provided for, as well as sanctions with regard to individual staff members. CBP's respect for privacy in general will be under the scrutiny of the DHS's Chief Privacy Officer, who is an official of the DHS but has a large measure of organisational autonomy and must report annually to Congress. Persons whose PNR data has been transferred may address complaints to CBP, or if unresolved, to the DHS Chief Privacy Officer, directly or through data protection authorities in Member States. The DHS Privacy Office will address, on an expedited basis, complaints referred to it by data protection authorities in Member States on behalf of residents of the Community, if the resident believes his or her complaint has not been satisfactorily dealt with by CBP or the DHS Privacy Office. Compliance with the Undertakings will be the subject of annual joint review to be conducted by CBP, in conjunction with DHS, and a Commission-led team.

(23) In the interest of transparency and in order to safeguard the ability of the competent authorities in the Member States to ensure the protection of individuals as regards the processing of their personal data, it is necessary to specify the exceptional circumstances in which the suspension of specific data flows may be justified, notwithstanding the finding of adequate protection.

(24) The Working Party on Protection of Individuals with regard to the Processing of Personal Data established under Article 29 of Directive 95/46/EC has delivered opinions on the level of protection provided by the United States authorities for passengers' data, which have guided the Commission throughout its negotiations with the DHS. The Commission has taken note of these opinions in the preparation of this Decision[65]

(25) The measures provided for in this Decision are in accordance with the opinion of the Committee established under Article 31(1) of Directive 95/46/EC,

---

[65] Opinion 6/2002 on transmission of passenger manifest information and other data from airlines to the United States, adopted by the Working Party on 24 October 2002 , available at: http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp66_en.pdf
Opinion 4/2003 on the level of protection ensured in the United States for the transfer of passengers' data, adopted by the Working Party on 13 June 2003 , available at: http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp78_en.pdf
Opinion 2/2004 on the adequate protection of personal data contained in the PNR of air passengers to be transferred to the United States Bureau of Customs and Border Protection (US CBP), adopted by the Working Party on 29 January 2004 , available at: http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp87_en.pdf

HAS ADOPTED THIS DECISION:

Article 1

For the purposes of Article 25(2) of Directive 95/46/EC, the United States' Bureau of Customs and Border Protection (hereinafter referred to as CBP) is considered to ensure an adequate level of protection for PNR data transferred from the Community concerning flights to or from the United States, in accordance with the Undertakings set out in the Annex.

Article 2

This Decision concerns the adequacy of protection provided by CBP with a view to meeting the requirements of Article 25(1) of Directive 95/46/EC and shall not affect other conditions or restrictions implementing other provisions of that Directive that pertain to the processing of personal data within the Member States.

Article 3

1. Without prejudice to their powers to take action to ensure compliance with national provisions adopted pursuant to provisions other than Article 25 of Directive 95/46/EC, the competent authorities in Member States may exercise their existing powers to suspend data flows to CBP in order to protect individuals with regard to the processing of their personal data in the following cases:

   (a) where a competent United States authority has determined that CBP is in breach of the applicable standards of protection; or

   (b) where there is a substantial likelihood that the standards of protection set out in the Annex are being infringed, there are reasonable grounds for believing that CBP is not taking or will not take adequate and timely steps to settle the case at issue, the continuing transfer would create an imminent risk of grave harm to data subjects, and the competent authorities in the Member State have made reasonable efforts in the circumstances to provide CBP with notice and an opportunity to respond.

2. Suspension shall cease as soon as the standards of protection are assured and the competent authorities of the Member States concerned are notified thereof.

Article 4

1. Member States shall inform the Commission without delay when measures are adopted pursuant to Article 3.

2. The Member States and the Commission shall inform each other of any changes in the standards of protection and of cases where the action of bodies responsible for ensuring compliance with the standards of protection by CBP as set out in the Annex fails to secure such compliance.

3. If the information collected pursuant to Article 3 and pursuant to paragraphs 1 and 2 of this Article provides evidence that the basic principles necessary for an adequate level of protection for natural persons are no longer being complied with, or that any body responsible for ensuring compliance with the standards of protection by CBP as set out in the Annex

is not effectively fulfilling its role, CBP shall be informed and, if necessary, the procedure referred to in Article 31(2) of Directive 95/46/EC shall apply with a view to repealing or suspending this Decision.

Article 5

The functioning of this Decision shall be monitored and any pertinent findings reported to the Committee established under Article 31 of Directive 95/46/EC, including any evidence that could affect the finding in Article 1 of this Decision that protection of personal data contained in the PNR of air passengers transferred to CBP is adequate within the meaning of Article 25 of Directive 95/46/EC.

Article 6

Member States shall take all the measures necessary to comply with the Decision within four months of the date of its notification.

Article 7

This Decision shall expire three years and six months after the date of its notification, unless extended in accordance with the procedure set out in Article 31(2) of Directive 95/46/EC.

Article 8

This Decision is addressed to the Member States.

Done at Brussels, 14 May 2004

For the Commission
Frederik Bolkestein
Member of the Commission

ANNEX

UNDERTAKINGS OF THE DEPARTMENT OF HOMELAND SECURITY BUREAU OF CUSTOMS AND BORDER PROTECTION (CBP)

In support of the plan of the European Commission (Commission) to exercise the powers conferred on it by Article 25(6) of Directive 95/46/EC (the Directive) and to adopt a decision recognising the Department of Homeland Security Bureau of Customs and Border Protection (CBP) as providing adequate protection for the purposes of air carrier transfers of Passenger [66] Name Record (PNR) data which may fall within the scope of the Directive, CBP undertakes as follows:

Legal authority to obtain PNR

1. By legal statute (title 49, United States Code, section 44909(c)(3)) and its implementing (interim) regulations (title 19, Code of Federal Regulations, section 122.49b), each air carrier operating passenger flights in foreign air transportation to or from the United States, must provide CBP (formerly, the US Customs Service) with electronic access to PNR data to the extent it is collected and contained in the air carrier's automated reservation/departure control systems (reservation systems).

Use of PNR data by CBP

2. Most data elements contained in PNR data can be obtained by CBP upon examining a data subject's airline ticket and other travel documents pursuant to its normal border control authority, but the ability to receive this data electronically will significantly enhance CBP's ability to facilitate bona fide travel and conduct efficient and effective advance risk assessment of passengers.

3. PNR data are used by CBP strictly for purposes of preventing and combating:
1. terrorism and related crimes; 2. other serious crimes, including organised crime, that are transnational in nature; and 3. flight from warrants or custody for the crimes described above. Use of PNR data for these purposes permits CBP to focus its resources on high-risk concerns, thereby facilitating and safeguarding bona fide travel.

Data requirements

4. Data elements which CBP require are listed herein at Attachment A. (Such identified elements are hereinafter referred to as "PNR" for purposes of these Undertakings.) Although CBP requires access to each of those 34 (thirty-four) data elements listed in Attachment A, CBP believes that it will be rare that an individual PNR will include a full set of the identified data. In those instances where the PNR does not include a full set of the identified data, CBP will not seek direct access from the air carrier's reservation system to other PNR data which are not listed on Attachment A.

---

[66] For the purposes of these Undertakings, the terms "passenger" and "passengers" shall include the crew members.

5. With respect to the data elements identified as "OSI" and "SSI/SSR" (commonly referred to as general remarks and open fields), CBP's automated system will search those fields for any of the other data elements identified in Attachment A. CBP personnel will not be authorised to manually review the full OSI and SSI/SSR fields unless the individual that is the subject of a PNR has been identified by CBP as high-risk in relation to any of the purposes identified in paragraph 3 hereof.

6. Additional personal information sought as a direct result of PNR data will be obtained from sources outside the government only through lawful channels, including through the use of mutual legal assistance channels where appropriate, and only for the purposes set forth in paragraph 3 hereof. For example, if a credit card number is listed in a PNR, transaction information linked to that account may be sought, pursuant to lawful process, such as a subpoena issued by a grand jury or a court order, or as otherwise authorised by law. In addition, access to records related to e-mail accounts derived from a PNR will follow US statutory requirements for subpoenas, court orders, warrants, and other processes as authorised by law, depending on the type of information being sought.

7. CBP will consult with the European Commission regarding revision of the required PNR data elements (Attachment A), prior to effecting any such revision, if CBP becomes aware of additional PNR fields that airlines may add to their systems which would significantly enhance CBP's ability to conduct passenger risk assessments or if circumstances indicate that a previously non-required PNR field will be needed to fulfil the limited purposes referred to in paragraph 3 of these Undertakings.

8. CBP may transfer PNRs on a bulk basis to the Transportation Security Administration (TSA) for purposes of TSA's testing of its Computer Assisted Passenger Pre-screening System II (CAPPS II). Such transfers will not be made until PNR data from US domestic flights have first been authorised for testing. PNR data transferred under this provision will not be retained by TSA or any other parties directly involved in the tests beyond the period necessary for testing purposes, or be transferred to any other third party.[67] The purpose of the processing is strictly limited to testing the CAPPS II system and interfaces and, except in emergency situations involving the positive identification of a known terrorist or individual with established connections to terrorism, is not to have any operational consequences. Under the provision requiring an automated filtering method described in paragraph 10, CBP will have filtered and deleted "sensitive"data before transferring any PNRs to TSA on a bulk basis under this paragraph.

Treatment of "sensitive" data

9. CBP will not use "sensitive" data (i.e. personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and data concerning the health or sex life of the individual) from the PNR, as described below.

---

[67] For purposes of this provision, CBP is not considered a party directly involved in the CAPPS II testing or a "third party".

10. CBP will implement, with the least possible delay, an automated system which filters and deletes certain "sensitive" PNR codes and terms which CBP has identified in consultation with the European Commission.

11. Until such automated filters can be implemented CBP represents that it does not and will not use "sensitive" PNR data and will undertake to delete "sensitive" data from any discretionary disclosure of PNR under paragraphs 28 to 34 [68]

Method of accessing PNR data

12. With regard to the PNR data which CBP access (or receive) directly from the air carrier's reservation systems for purposes of identifying potential subjects for border examination, CBP personnel will only access (or receive) and use PNR data concerning persons whose travel includes a flight into or out of [69] the United States.

13. CBP will "pull" passenger information from air carrier reservation systems until such time as air carriers are able to implement a system to "push" the data to CBP.

14. CBP will pull PNR data associated with a particular flight no earlier than 72 hours prior to the departure of that flight, and will re-check the systems no more than three (3) times between the initial pull, the departure of the flight from a foreign point and the flight's arrival in the United States, or between the initial pull and the departure of the flight from the United States, as applicable, to identify any changes in the information. In the event that the air carriers obtain the ability to "push" PNR data, CBP will need to receive the data 72 hours prior to departure of the flight, provided that all changes to the PNR data which are made between that point and the time of the flight's arrival in or departure from the United States, are also pushed to CBP [70]. In the unusual event that CBP obtains advance information that person(s) of specific concern may be travelling on a flight to, from or through the United States, CBP may pull (or request a particular push) of PNR data prior to 72 hours before departure of the flight to ensure that proper enforcement action may be taken when essential to prevent or combat an offence enumerated in paragraph 3 hereof. To the extent practicable, in such instances where PNR data must be accessed by CBP prior to 72 hours before the departure of the flight, CBP will utilise customary law enforcement channels.

Storage of PNR data

15. Subject to the approval of the National Archives and Records Administration (44 U.S.C. 2101, *et seq.*), CBP will limit online access to

---

[68] Prior to CBP's implementation of automated filters (as referenced in paragraph 10 hereof), if "sensitive" data exists in a PNR which is the subject of a non-discretionary disclosure by CBP as described in paragraph 35 hereof, CBP will make every effort to limit the release of "sensitive" PNR data, consistent with US law.

[69] This would include persons transiting through the United States.

[70] In the event that the air carriers agree to push the PNR data to CBP, the agency will engage in discussions with the air carriers regarding the possibility of pushing PNR data at periodic intervals between 72 hours before departure of the flight from a foreign point and the flight's arrival in the United States, or within 72 hours before the departure of the flight from the United States, as applicable. CBP seeks to utilise a method of pushing the necessary PNR data that meets the agency's needs for effective risk assessment, while minimising the economic impact upon air carriers.

PNR data to authorised CBP users [71] for a period of seven (7) days, after which the number of officers authorised to access the PNR data will be even further limited for a period of three years and six months (3,5 years) from the date the data are accessed (or received) from the air carrier's reservation system. After 3,5 years, PNR data that have not been manually accessed during that period of time, will be destroyed. PNR data that have been manually accessed during the initial 3, 5-year period will be transferred by CBP to a deleted record file [72], where they will remain for a period of eight (8) years before they are destroyed. This schedule, however, would not apply to PNR data that are linked to a specific enforcement record (such data would remain accessible until the enforcement record is archived). With respect to PNR which CBP accesses (or receives) directly from air carrier reservation systems during the effective dates of these Undertakings, CBP will abide by the retention policies set forth in the present paragraph, notwithstanding the possible expiration of the Undertakings pursuant to paragraph 46 herein.

CBP computer system security

16. Authorised CBP personnel obtain access to PNR through the closed CBP intranet system which is encrypted end to-end and the connection is controlled by the Customs Data Center. PNR data stored in the CBP database are limited to "read only" access by authorised personnel, meaning that the substance of the data may be programmatically reformatted, but will not be substantively altered in any manner by CBP once accessed from an air carrier's reservation system.

17. No other foreign, federal, State or local agency has direct electronic access to PNR data through CBP databases (including through the Interagency Border Inspection System (IBIS)).

18. Details regarding access to information in CBP databases (such as who, where, when (date and time) and any revisions to the data) are automatically recorded and routinely audited by the Office of Internal Affairs to prevent unauthorised use of the system.

19. Only certain CBP officers, employees or information technology contractors[73] (under CBP supervision) who have successfully completed a background investigation, have an active, password-protected account in

---

[71] These authorised CBP users would include employees assigned to analytical units in the field offices, as well as employees assigned to the National Targeting Center. As indicated previously, persons charged with maintaining, developing or auditing the CBP database will also have access to such data for those limited purposes.

[72] Although the PNR record is not technically deleted when it is transferred to the Deleted Record File, it is stored as raw data (not a readily searchable form and, therefore, of no use for "traditional" law enforcement investigations) and is only available to authorised personnel in the Office of Internal Affairs for CBP (and in some cases the Office of the Inspector General in connection with audits) and personnel responsible for maintaining the database in CBP's Office of Information Technology, on a "need to know" basis. Although the PNR record is not technically deleted when it is transferred to the Deleted Record File, it is stored as raw data (not a readily searchable form and, therefore, of no use for "traditional" law enforcement investigations) and is only available to authorised personnel in the Office of Internal Affairs for CBP (and in some cases the Office of the Inspector General in connection with audits) and personnel responsible for maintaining the database in CBP's Office of Information Technology, on a "need to know" basis.

[73] Access by "contractors" to any PNR data contained in the CBP computer systems would be confined to persons under contract with CBP to assist in the maintenance or development of CBP's computer system

the CBP computer system, and have a recognised official purpose for reviewing PNR data, may access PNR data.

20. CBP officers, employees and contractors are required to complete security and data privacy training, including passage of a test, on a biennial basis. CBP system auditing is used to monitor and ensure compliance with all privacy and data security requirements.

21. Unauthorised access by CBP personnel to air carrier reservation systems or the CBP computerised system which stores PNR is subject to strict disciplinary action (which may include termination of employment) and may result in criminal sanctions being imposed (fines, imprisonment of up to one year, or both) (see title 18, United States Code, section 1030).

22. CBP policy and regulations also provide for stringent disciplinary action (which may include termination of employment) to be taken against any CBP employee who discloses information from CBP's computerised systems without official authorisation (title 19, Code of Federal Regulations, section 103.34).

23. Criminal penalties (including fines, imprisonment of up to one year, or both) may be assessed against any officer or employee of the United States for disclosing PNR data obtained in the course of his employment, where such disclosure is not authorised by law (see title 18, United States Code, sections 641, 1030, 1905).

CBP treatment and protection of PNR data

24. CBP treats PNR information regarding persons of any nationality or country of residence as law-enforcement sensitive, confidential personal information of the data subject, and confidential commercial information of the air carrier, and, therefore, would not make disclosures of such data to the public, except as in accordance with these Undertakings or as otherwise required by law.

25. Public disclosure of PNR data is generally governed by the Freedom of Information Act (FOIA) (title 5, United States Code, section 552) which permits any person (regardless of nationality or country of residence) access to a US federal agency's records, except to the extent such records (or a portion thereof) are protected from public disclosure by an applicable exemption under the FOIA. Among its exemptions, the FOIA permits an agency to withhold a record (or a portion thereof) from disclosure where the information is confidential commercial information, where disclosure of the information would constitute a clearly unwarranted invasion of personal privacy, or where the information is compiled for law enforcement purposes, to the extent that disclosure may reasonably be expected to constitute an unwarranted invasion of personal privacy (title 5, United States Code, sections 552(b)(4), (6), (7)(C)).

26. CBP regulations (title 19, Code of Federal Regulations, section 103.12), which govern the processing of requests for information (such as PNR data) pursuant to the FOIA, specifically provide that (subject to certain limited exceptions in the case of requests by the data subject) the disclosure requirements of the FOIA are not applicable to CBP records relating to: 1. confidential commercial information; 2. material involving personal privacy where the disclosure would constitute a clearly unwarranted invasion of personal privacy; and 3. information compiled for law enforcement

purposes, where disclosure could reasonably be expected to constitute an unwarranted invasion of personal privacy[74].

27. CBP will take the position in connection with any administrative or judicial proceeding arising out of a FOIA request for PNR information accessed from air carriers, that such records are exempt from disclosure under the FOIA.

Transfer of PNR data to other government authorities

28. With the exception of transfers between CBP and TSA pursuant to paragraph 8 herein, Department of Homeland Security (DHS) components will be treated as "third agencies", subject to the same rules and conditions for sharing of PNR data as other government authorities outside DHS.

29. CBP, in its discretion, will only provide PNR data to other government authorities, including foreign government authorities, with counter-terrorism or law-enforcement functions, on a case-by-case basis, for purposes of preventing and combating offences identified in paragraph 3 herein. (Authorities with whom CBP may share such data shall hereinafter be referred to as the Designated Authorities).

30. CBP will judiciously exercise its discretion to transfer PNR data for the stated purposes. CBP will first determine if the reason for disclosing the PNR data to another Designated Authority fits within the stated purpose (see paragraph 29 herein). If so, CBP will determine whether that Designated Authority is responsible for preventing, investigating or prosecuting the violations of, or enforcing or implementing, a statute or regulation related to that purpose, where CBP is aware of an indication of a violation or potential violation of law. The merits of disclosure will need to be reviewed in light of all the circumstances presented.

31. For purposes of regulating the dissemination of PNR data which may be shared with other Designated Authorities, CBP is considered the "owner" of the data and such Designated Authorities are obligated by the express terms of disclosure to: 1. use the PNR data only for the purposes set forth in paragraph 29 or 34 herein, as applicable; 2. ensure the orderly disposal of PNR information that has been received, consistent with the Designated Authority's record retention procedures; and 3. obtain CBP's express authorisation for any further dissemination. Failure to respect the conditions for transfer may be investigated and reported by the DHS Chief Privacy Officer and may make the Designated Authority ineligible to receive subsequent transfers of PNR data from CBP.

32. Each disclosure of PNR data by CBP will be conditioned upon the receiving agency's treatment of this data as confidential commercial information and law enforcement sensitive, confidential personal information of the data subject, as identified in paragraphs 25 and 26 hereof, which should be treated as exempt from disclosure under the Freedom of Information Act (5 U.S.C. 552). Further, the recipient agency will be advised that further disclosure of such information is not permitted without the express prior approval of CBP. CBP will not authorise any

---

74 CBP would invoke these exemptions uniformly, without regard to the nationality or country of residence of the subject of the data.

further transfer of PNR data for purposes other than those identified in paragraphs 29, 34 or 35 herein.

33. Persons employed by such Designated Authorities who without appropriate authorisation disclose PNR data, may be liable for criminal sanctions (title 18, United States Code, sections 641, 1030 and 1905).

34. No statement herein shall impede the use or disclosure of PNR data to relevant government authorities, where such disclosure is necessary for the protection of the vital interests of the data subject or of other persons, in particular as regards significant health risks. Disclosures for these purposes will be subject to the same conditions for transfers set forth in paragraphs 31 and 32 of these Undertakings.

35. No statement in these Undertakings shall impede the use or disclosure of PNR data in any criminal judicial proceedings or as otherwise required by law. CBP will advise the European Commission regarding the passage of any US legislation which materially affects the statements made in these Undertakings.

Notice, access and opportunities for redress for PNR data subjects

36. CBP will provide information to the travelling public regarding the PNR requirement and the issues associated with its use (i.e. general information regarding the authority under which the data are collected, the purpose for the collection, protection of the data, data-sharing, the identity of the responsible official, procedures available for redress and contact information for persons with questions or concerns, etc., for posting on CBP's website, in travel pamphlets, etc.).

37. Requests by the data subject (also known as first party requesters) to receive a copy of PNR data contained in CBP databases regarding the data subject are processed under the Freedom of Information Act (FOIA). Such requests may be addressed to: Freedom of Information Act (FOIA) Request, US Customs and Border Protection, 1300 Pennsylvania Avenue, NW, Washington, DC 20229, if by mail; or such request may be delivered to the Disclosure Law Officer, US Customs and Border Protection, Headquarters, Washington, DC. Further information regarding the procedures for making FOIA requests is contained in section 103.5 of title 19 of the US Code of Federal Regulations. In the case of a first-party request, the fact that CBP otherwise considers PNR data to be confidential personal information of the data subject and confidential commercial information of the air carrier will not be used by CBP as a basis under FOIA for withholding PNR data from the data subject.

38. In certain exceptional circumstances, CBP may exercise its authority under FOIA to deny or postpone disclosure of all (or, more likely, part) of the PNR record to a first party requester, pursuant to title 5, United States Code, section 552(b) (e.g. if disclosure under FOIA "could reasonably be expected to interfere with enforcement proceedings" or "would disclose techniques and procedures for law enforcement investigations (...) (which) could reasonably be expected to risk circumvention of the law"). Under FOIA, any requester has the authority to administratively and judicially challenge CBP's decision to withhold information (see 5 U.S.C. 552(a)(4)(B); 19 CFR 103.7 to 103.9).

39. CBP will undertake to rectify[75] data at the request of passengers and crew members, air carriers or data protection authorities (DPAs) in the EU Member States (to the extent specifically authorised by the data subject), where CBP determines that such data is contained in its database and a correction is justified and properly supported. CBP will inform any Designated Authority which has received such PNR data of any material rectification of that PNR data.

40. Requests for rectification of PNR data contained in CBP's database and complaints by individuals about CBP's handling of their PNR data may be made, either directly or via the relevant DPA (to the extent specifically authorised by the data subject) to the Assistant Commissioner, Office of Field Operations, US Bureau of Customs and Border Protection, 1300 Pennsylvania Avenue, NW, Washington, DC 20229.

41. In the event that a complaint cannot be resolved by CBP, the complaint may be directed, in writing, to the Chief Privacy Officer, Department of Homeland Security, Washington, DC 20528, who will review the situation and endeavour to resolve the complaint[76]

42. Additionally, the DHS Privacy Office will address on an expedited basis, complaints referred to it by DPAs in the European Union (EU) Member States on behalf of an EU resident to the extent such resident has authorised the DPA to act on his or her behalf and believes that his or her data-protection complaint regarding PNR has not been satisfactorily dealt with by CBP (as set out in paragraphs 37 to 41 of these Undertakings) or the DHS Privacy Office. The Privacy Office will report its conclusions and advise the DPA or DPAs concerned regarding actions taken, if any. The DHS Chief Privacy Officer will include in her report to Congress issues regarding the number, the substance and the resolution of complaints regarding the handling of personal data, such as PNR[77].

Compliance issues

43. CBP, in conjunction with DHS, undertakes to conduct once a year, or more often if agreed by the parties, a joint review with the European Commission assisted as appropriate by representatives of European law-enforcement authorities and/or authorities of the Member States of the

---

[75] By "rectify", CBP wishes to make clear that it will not be authorised to revise the data within the PNR record that it accesses from the air carriers. Rather, a separate record linked to the PNR record will be created to note that the data were determined to be inaccurate and the proper correction. Specifically, CBP will annotate the passenger's secondary examination record to reflect that certain data in the PNR may be or are inaccurate.

[76] The DHS Chief Privacy Officer is independent of any directorate within the Department of Homeland Security. She is statutorily obligated to ensure that personal information is used in a manner that complies with relevant laws. The determinations of the Chief Privacy Officer shall be binding on the Department and may not be overturned on political grounds.

[77] Pursuant to section 222 of the Homeland Security Act of 2002 (the Act) (Public Law 107–296, dated 25 November 2002), the Privacy Officer for DHS is charged with conducting a "privacy impact assessment" of proposed rules of the Department on "the privacy of personal information, including the type of personal information collected and the number of people affected" and must report to Congress on an annual basis regarding the "activities of the Department that affect privacy ...". Section 222(5) of the Act also expressly directs the DHS Privacy Officer to hear and report to Congress regarding all "complaints of privacy violations"

European Union[78], on the implementation of these Undertakings, with a view to mutually contributing to the effective operation of the processes described in these Undertakings.

44. CBP will issue regulations, directives or other policy documents incorporating the statements herein, to ensure compliance with these Undertakings by CBP officers, employees and contractors. As indicated herein, failure of CBP officers, employees and contractors to abide by CBP's policies incorporated therein may result in strict disciplinary measures being taken, and criminal sanctions, as applicable.

Reciprocity

45. In the event that an airline passenger identification system is implemented in the European Union which requires air carriers to provide authorities with access to PNR data for persons whose current travel itinerary includes a flight to or from the European Union, CBP shall, strictly on the basis of reciprocity, encourage US-based airlines to cooperate.

Review and termination of Undertakings

46. These Undertakings shall apply for a term of three years and six months (3,5 years), beginning on the date upon which an agreement enters into force between the United States and the European Community, authorising the processing of PNR data by air carriers for purposes of transferring such data to CBP, in accordance with the Directive. After these Undertakings have been in effect for two years and six months (2, 5 years), CBP, in conjunction with DHS, will initiate discussions with the Commission with the goal of extending the Undertakings and any supporting arrangements, upon mutually acceptable terms. If no mutually acceptable arrangement can be concluded prior to the expiration date of these Undertakings, the Undertakings will cease to be in effect.

No private right or precedent created

47. These Undertakings do not create or confer any right or benefit on any person or party, private or public.

48. The provisions of these Undertakings shall not constitute a precedent for any future discussions with the European Commission, the European Union, any related entity, or any third State regarding the transfer of any form of data.

11 May 2004

---

[78] The composition of the teams on both sides will be notified to each other in advance and may include appropriate authorities concerned with privacy/data protection, customs control and other forms of law enforcement, border security and/or aviation security. Participating authorities will be required to obtain any necessary security clearances and will adhere to the confidentiality of the discussions and documentation to which they may be given access. Confidentiality will not however be an obstacle to each side making an appropriate report on the results of the joint review to their respective competent authorities, including the US Congress and the European Parliament. However, under no circumstances may participating authorities disclose any personal data of a data subject; nor may participating authorities disclose any non-public information derived from documents to which they are given access, or any operational or internal agency information they obtain during the joint review. The two sides will mutually determine the detailed modalities of the joint review.

ATTACHMENT A

PNR data elements required by CBP from air carriers

1. PNR record locator code
2. Date of reservation
3. Date(s) of intended travel
4. Name
5. Other names on PNR
6. Address
7. All forms of payment information
8. Billing address
9. Contact telephone numbers
10. All travel itinerary for specific PNR
11. Frequent flyer information (limited to miles flown and address(es))
12. Travel agency
13. Travel agent
14. Code share PNR information
15. Travel status of passenger
16. Split/divided PNR information
17. E-mail address
18. Ticketing field information
19. General remarks
20 Ticket number
21. Seat number
22. Date of ticket issuance
23. No show history
24. Bag tag numbers
25. Go show information
26. OSI information
27. SSI/SSR information
28. Received from information
29. All historical changes to the PNR
30. Number of travellers on PNR
31. Seat information
32. One-way tickets
33. Any collected APIS (Advanced Passenger Information System) information
34. ATFQ (Automatic Ticketing Fare Quote) fields

APPENDIX 5: 2004 AGREEMENT

Agreement between the European Community and the United States of America on the processing and transfer of PNR data by air carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection [79]

THE EUROPEAN COMMUNITY AND THE UNITED STATES OF AMERICA,

RECOGNISING the importance of respecting fundamental rights and freedoms, notably privacy, and the importance of respecting these values, while preventing and combating terrorism and related crimes and other serious crimes that are transnational in nature, including organised crime,

HAVING REGARD to US statutes and regulations requiring each air carrier operating passenger flights in foreign air transportation to or from the United States to provide the Department of Homeland Security (hereinafter "DHS"), Bureau of Customs and Border Protection (hereinafter "CBP") with electronic access to Passenger Name Record (hereinafter "PNR") data to the extent it is collected and contained in the air carrier's automated reservation/departure control systems,

HAVING REGARD to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and in particular Article 7(c) thereof,

HAVING REGARD to the Undertakings of CBP issued on 11 May 2004, which will be published in the Federal Register (hereinafter "the Undertakings"),

HAVING REGARD to Commission Decision C (2004) 1799 adopted on 17 May 2004, pursuant to Article 25(6) of Directive 95/46/EC, whereby CBP is considered as providing an adequate level of protection for PNR data transferred from the European Community (hereinafter "Community") concerning flights to or from the US in accordance with the Undertakings, which are annexed thereto (hereinafter "the Decision"),

NOTING that air carriers with reservation/departure control systems located within the territory of the Member States of the European Community should arrange for transmission of PNR data to CBP as soon as this is technically feasible but that, until then, the US authorities should be allowed to access the data directly, in accordance with the provisions of this Agreement,

AFFIRMING that this Agreement does not constitute a precedent for any future discussions and negotiations between the United States and the European Community, or between either of the Parties and any State regarding the transfer of any other form of data,

HAVING REGARD to the commitment of both sides to work together to reach an appropriate and mutually satisfactory solution, without delay, on the processing of Advance Passenger Information (API) data from the Community to the US,

HAVE AGREED AS FOLLOWS:

---

[79] OJ L183, 20.5.2004, p 84.

(1) CBP may electronically access the PNR data from air carriers' reservation/departure control systems ("reservation systems") located within the territory of the Member States of the European Community strictly in accordance with the Decision and for so long as the Decision is applicable and only until there is a satisfactory system in place allowing for transmission of such data by the air carriers (2) Air carriers operating passenger flights in foreign air transportation to or from the United States shall process PNR data contained in their automated reservation systems as required by CBP pursuant to US law and strictly in accordance with the Decision and for so long as the Decision is applicable.

(2) Air carriers operating passenger flights in foreign air transportation to or from the United States shall process PNR data contained in their automated reservation systems as required by CBP pursuant to US law and strictly in accordance with the Decision and for so long as the Decision is applicable.

(3) CBP takes note of the Decision and states that it is implementing the Undertakings annexed thereto.

(4) CBP shall process PNR data received and treat data subjects concerned by such processing in accordance with applicable US laws and constitutional requirements, without unlawful discrimination, in particular on the basis of nationality and country of residence.

(5) CBP and the European Commission shall jointly and regularly review the implementation of this Agreement.

(6) In the event that an airline passenger identification system is implemented in the European Union which requires air carriers to provide authorities with access to PNR data for persons whose current travel itinerary includes a flight to or from the European Union, DHS shall, in so far as practicable and strictly on the basis of reciprocity, actively promote the cooperation of airlines within its jurisdiction.

(7) This Agreement shall enter into force upon signature. Either Party may terminate this Agreement at any time by notification through diplomatic channels. The termination shall take effect ninety (90) days from the date of notification of termination to the other Party. This Agreement may be amended at any time by mutual written agreement.

(8) This Agreement is not intended to derogate from or amend legislation of the Parties; nor does this Agreement create or confer any right or benefit on any other person or entity, private or public.

This Agreement is drawn up in duplicate in the Czech, Danish, Dutch, English, Estonian, Finnish, French, German, Greek, Hungarian, Italian, Latvian, Lithuanian, Maltese, Polish, Portuguese, Slovak, Slovenian, Spanish and Swedish languages, each text being equally authentic. In case of divergence, the English version shall prevail.

Signed at …. , on … [80]

for the European Community

for the United States of America

Tom RIDGE

Secretary of the United States Department of Homeland Security

---

[80] The Agreement was signed at Washington D.C. on 28 May 2004.

APPENDIX 6: 2006 INTERIM AGREEMENT

Agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security [81]

THE EUROPEAN UNION and THE UNITED STATES OF AMERICA,

DESIRING to prevent and combat terrorism and transnational crime effectively as a means of protecting their respective democratic societies and common values,

RECOGNISING that, in order to safeguard public security and for law enforcement purposes, rules should be laid down on the transfer of Passenger Name Record (PNR) data by air carriers to the Department of Homeland Security (hereinafter DHS). For the purposes of this Agreement, DHS means the Bureau of Customs and Border Protection, US Immigration and Customs Enforcement and the Office of the Secretary and the entities that directly support it, but does not include other components of DHS 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,

RECOGNISING the importance of preventing and combating terrorism and related crimes, and other serious crimes that are transnational in nature, including organised crime, while respecting fundamental rights and freedoms, notably privacy,

HAVING REGARD to US statutes and regulations requiring each air carrier operating passenger flights in foreign air transportation to or from the United States to provide DHS with electronic access to PNR data to the extent that they are collected and contained in the air carrier's automated reservation/departure control systems (hereinafter "reservation systems"),

HAVING REGARD to Article 6(2) of the Treaty on European Union on respect for fundamental rights, and in particular to the related right to the protection of personal data,

HAVING REGARD to relevant provisions of the Aviation Transportation Security Act of 2001, the Homeland Security Act of 2002, the Intelligence Reform and Terrorism Prevention Act of 2004 and Executive Order 13388 regarding cooperation between agencies of the United States Government in combating terrorism,

HAVING REGARD to the Undertakings as published in the US Federal Register[82] and implemented by DHS,

NOTING that the European Union should ensure that air carriers with reservation systems located within the European Union arrange for transmission of PNR data to DHS as soon as this is technically feasible but that, until then, the US authorities should be allowed to access the data directly, in accordance with the provisions of this Agreement,

AFFIRMING that this Agreement does not constitute a precedent for any future discussions or negotiations between the United States and the European Union, or

---

[81] OJ L298, 27.10.2006, p 30.

[82] Vol. 69, No 131, p. 41543.

between either of the Parties and any State regarding the processing and transfer of PNR or any other form of data,

HAVING REGARD to the commitment of both sides to work together to reach an appropriate and mutually satisfactory solution, without delay, on the processing of Advance Passenger Information (API) data from the European Union to the United States,

NOTING that in reliance on this Agreement, the EU confirms that it will not hinder the transfer of PNR data between Canada and the United States and that the same principle will be applied in any similar agreement on the processing and transfer of PNR data,

HAVE AGREED AS FOLLOWS:

(1) In reliance upon DHS's continued implementation of the aforementioned Undertakings as interpreted in the light of subsequent events, the European Union shall ensure that air carriers operating passenger flights in foreign air transportation to or from the United States of America process PNR data contained in their reservation systems as required by DHS.

(2) Accordingly, DHS will electronically access the PNR data from air carriers' reservation systems located within the territory of the Member States of the European Union until there is a satisfactory system in place allowing for transmission of such data by the air carriers.

(3) DHS shall process PNR data received and treat data subjects concerned by such processing in accordance with applicable US laws and constitutional requirements, without unlawful discrimination, in particular on the basis of nationality and country of residence.

(4) The implementation of this Agreement shall be jointly and regularly reviewed.

(5) In the event that an airline passenger information system is implemented in the European Union or in one or more of its Member States that requires air carriers to provide authorities with access to PNR data for persons whose travel itinerary includes a flight to or from the European Union, DHS shall, in so far as practicable and strictly on the basis of reciprocity, actively promote the cooperation of airlines within its jurisdiction.

(6) For the purpose of applying this Agreement, DHS is deemed to ensure an adequate level of protection for PNR data transferred from the European Union concerning passenger flights in foreign air transportation to or from the United States.

(7) This Agreement shall enter into force on the first day of the month after the date on which the Parties have exchanged notifications indicating that they have completed their internal procedures for this purpose. This Agreement shall apply provisionally as of the date of signature. Either Party may terminate or suspend this Agreement at any time by notification through diplomatic channels. Termination shall take effect thirty (30) days from the date of notification thereof to the other Party This Agreement shall expire upon the date of application of any superseding agreement and in any event no later than 31 July 2007, unless extended by mutual written agreement.

This Agreement is not intended to derogate from or amend legislation of the United States of America or the European Union or its Member States. This Agreement does not create or confer any right or benefit on any other person or entity, private or public.

This Agreement shall be drawn up in duplicate in the English language. It shall also be drawn up in the Czech, Danish, Dutch, Estonian, Finnish, French, German, Greek, Hungarian, Italian, Latvian, Lithuanian, Maltese, Polish, Portuguese, Slovak, Slovenian, Spanish and Swedish languages, and the Parties shall approve these language versions. Once approved, the versions in these languages shall be equally authentic.

Done at Luxembourg on 16 October 2006

and at Washington D.C. on 19 October 2006.

For the European Union

E. TUOMIOJA

Minister for Foreign Affairs

President of the Council of the European Union

For the United States of America

Secretary Michael CHERTOFF

Department of Homeland Security

APPENDIX 7: BAKER EXCHANGE OF LETTERS

Letter to the Council Presidency and the Commission from the Department of Homeland Security (DHS) of the United States of America, concerning the interpretation of certain provisions of the undertakings issued by DHS on 11 May 2004 in connection with the transfer by air carriers of passenger name record (PNR)[83]

This letter is intended to set forth our understandings with regard to the interpretation of a number of provisions of the Passenger Name Record (PNR) Undertakings issued on May 11, 2004 by the Department of Homeland Security (DHS). For the purposes of this letter, DHS means the Bureau of Customs and Border Protection, U.S. Immigration and Customs Enforcement and the Office of the Secretary and the entities that directly support it, but does not include other components of DHS 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. We look forward to further reviewing these and other issues in the context of future discussions toward a comprehensive, reciprocal agreement based on common principles.

Sharing and Disclosure of PNR

The Intelligence Reform and Terrorism Prevention Act of 2004 required the President to establish an Information Sharing Environment "that facilitates the sharing of terrorism information." Following this enactment, on October 25, 2005 the President issued Executive Order 13388, directing that DHS and other agencies "promptly give access to…terrorism information to the head of each other agency that has counterterrorism functions" and establishing a mechanism for implementing the Information Sharing Environment.

Pursuant to Paragraph 35 of the Undertakings (which states that "No statement in these Undertakings shall impede the use or disclosure of PNR data in any criminal judicial proceedings or as otherwise required by law" and allows DHS to "advise the European Commission regarding the passage of any U.S. legislation which materially affects the statements made in these Undertakings"), the U.S. has now advised the EU that the implementation of the Information Sharing Environment required by the Act and the Executive Order described above may be impeded by certain provisions of the Undertakings that restrict information sharing among U.S. agencies, particularly all or portions of paragraphs 17, 28, 29, 30, 31, and 32.

In light of these developments and in accordance with what follows, the Undertakings should be interpreted and applied so as to not impede the sharing of PNR data by DHS with other authorities of the U.S. government responsible for preventing or combating of terrorism and related crimes asset forth in Paragraph 3 of the Undertakings

DHS will therefore facilitate the disclosure (without providing unconditional direct electronic access) of PNR data to U.S. government authorities exercising a counter-terrorism function that need PNR for the purpose of preventing or combating terrorism and related crimes in cases (including threats, flights, individuals, and routes of concern) that they are examining or investigating. DHS

[83] OJ C259, 27.10.2006, p 1.

will ensure that such authorities respect comparable standards of data protection to that applicable to DHS, in particular in relation to purpose limitation, data retention, further disclosure, awareness and training, security standards and sanctions for abuse, and procedures for information, complaints and rectification. Prior to commencing facilitated disclosure, each receiving authority will confirm in writing to DHS that it respects those standards. DHS will inform the EU in writing of the implementation of such facilitated disclosure and respect for the applicable standards before the expiration of the Agreement.

Early Access Period for PNR

While Paragraph 14 limits the number of times PNR can be pulled, the provision puts no such restriction on the "pushing" of data to DHS. The push system is considered by the EU to be less intrusive from a data privacy perspective. The push system does not confer on airlines any discretion to decide when, how or what data to push, however. That decision is conferred on DHS by U.S. law. Therefore, it is understood that DHS will utilize a method of pushing the necessary PNR data that meets the agency's needs for effective risk assessment, taking into account the economic impact upon air carriers.

In determining when the initial push of data is to occur, DHS has discretion to obtain PNR more than 72 hours prior to the departure of a flight so long as action is essential to combat an offence enumerated in Paragraph 3. Additionally, 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. Paragraph 14 is therefore understood to permit access to PNR outside of the 72 hour mark when there is an indication that early access is likely to assist in responding to a specific threat to a flight, set of flights, route, or other circumstances associated with offenses described in Paragraph 3 of the Undertakings. In exercising this discretion, DHS will act judiciously and with proportionality.

DHS will move as soon as practicable to a push system for the transfer of PNR data in accordance with the Undertakings and will carry out no later than the end of 2006 the necessary tests for at least one system currently in development if DHS's technical requirements are satisfied by the design to be tested. Without derogating from the Undertakings and in order to avoid prejudging the possible future needs of the system any filters employed in a push system, and the design of the system itself must permit any PNR data in the airline reservation or departure control systems 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.

Data Retention

Several important uses for PNR data help to identify potential terrorists; even data that is more than 3.5 years old can be crucial in identifying links among terrorism suspects. The Agreement will have expired before Paragraph 15 of the Undertakings requires the destruction of any data, and questions of whether and when to destroy PNR data collected in accordance with the Undertakings will be addressed by the United States and the European Union as part of future discussions.

The Joint Review

Given the extensive joint analysis of the Undertakings conducted in September 2005 and the expiration of the agreement prior to the next Joint Review, the question of how and whether to conduct a joint review in 2007 will be addressed during the discussions regarding a future agreement.

Data Elements

The frequent flyer field may offer addresses, telephone numbers, email addresses; all of these, as well as the frequent flyer number itself, may provide crucial evidence of links to terrorism. Similarly, information about the number of bags carried by a passenger may have value in a counterterrorism context. The Undertakings authorize DHS to add data elements to the 34 previously set forth in Attachment "A" of the Undertakings, if such data is necessary to fulfill the purposes set forth in paragraph 3.

With this letter the U.S. has consulted under Paragraph 7 with the EU in connection with item 11 of Attachment A regarding DHS's need to obtain the frequent flier number and any data element listed in Attachment A to the Undertakings wherever that element may be found.

Vital Interests of the Data Subject or Others

Recognizing the potential importance of PNR data in the context of infectious disease and other risks to passengers, DHS reconfirms that access to such information is authorized by paragraph 34, which provides that the Undertakings must not impede the use of PNR for the protection of the vital interests of the data subject or of other persons or inhibit the direct availability of PNR to relevant authorities for the purposes set forth in Paragraph 3 of the Undertakings. "Vital interests" encompasses 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. Such data will be protected in a manner commensurate with its nature and used strictly for the purposes for which it was accessed.

Stewart Baker

Assistant Secretary for Policy

Reply by the Council Presidency and the Commission to the letter from the USA's Department of Homeland Security

On 11 October 2006 we received, by electronic transmission, your letter to the Council Presidency and the Commission, concerning the interpretation of certain provisions of the Undertakings issued by DHS on 11 May 2004 in connection with the transfer by air carriers of passenger name records (PNR) data.

While taking note of the content of your letter, we wish to reaffirm the importance that the EU and its Member States attach to respect for fundamental rights, in particular to the protection of personal data.

The commitments of DHS to continue to implement the Undertakings allow for the EU to deem that, for purposes of the implementation of the Agreement, it ensures an adequate level of data protection

Irma ERTMAN Jonathan FAULL

APPENDIX 8: LIST OF ABBREVIATIONS

ACLU	American Civil Liberties Union
AEA	Association of European Airlines
APIS	Advance Passenger Information System
Article 29 Working Party	Data Protection Working Party established under Article 29 of the Data Protection Directive 95/46/EC
ATS	Automated Targeting System
BA	British Airways
BARUK	Board of Airline Representatives in the UK
BATA	British Air Transport Association
CBSA	Canadian Border Service Agency
CEPS	Centre for European Policy Studies
CBP	Bureau of Customs and Border Protection within DHS
DCA	Department for Constitutional Affairs
DHS	United States Department of Homeland Security
DG JLS	Directorate-General Justice Freedom and Security of the Commission
EC	European Community
ECJ	European Court of Justice
EDPS	European Data Protection Supervisor
EU	European Union
ICAO	International Civil Aviation Organisation
ICO	Information Commissioner's Office
JHA	Justice and Home Affairs
LIBE Committee	Committee on Civil Liberties, Justice and Home Affairs of the European Parliament
OSI	Other service-related information
PNR	Passenger Name Record
SSI/SSR	Special Service Information/Special Service Requests
TEC	Treaty establishing the European Community
TEU	Treaty on European Union
TRIP	Travel Redress Inquiry Program
TSA	Transportation Security Administration
VWP	Visa Waiver Program

APPENDIX 9: OTHER RELEVANT REPORTS FROM THE SELECT COMMITTEE

Recent Reports from the Select Committee

Annual Report 2006 (46th Report, Session 2005–06, HL Paper 261)

Relevant Reports prepared by Sub-Committee F

Session 2004–05

After Madrid: the EU's response to terrorism (5th Report, HL Paper 53)

The Hague Programme: a five year agenda for EU justice and home affairs (10th Report, HL Paper 84)

Session 2005–06

Behind Closed Doors: the meeting of the G6 Interior Ministers at Heiligendamm (40th Report, HL Paper 221)

Session 2006–07

After Heiligendamm: doors ajar at Stratford-upon-Avon (5th Report, HL Paper 32)

Schengen Information System II (SIS II) (9th Report, HL Paper 49)

Prüm: an effective weapon against terrorism and crime? (18th Report, HL Paper 90)

Minutes of Evidence

TAKEN BEFORE THE SELECT COMMITTEE ON THE EUROPEAN UNION (SUB-COMMITTEE F)

WEDNESDAY 28 FEBRUARY 2007

Present	Bonham-Carter of Yarnbury, B	Henig, B
	Caithness, E of	Jopling, L
	D'Souza, B	Listowel, E of
	Foulkes of Cumnock, L	Marlesford, L
	Harrison, L	Wright of Richmond, L (Chairman)

Examination of Witness

Witness: Dr Gus Hosein, Visiting Scholar, American Civil Liberties Union, examined.

Q1 ***Chairman:*** Doctor, you are very welcome.
Dr Hosein: Thank you for having me.

Q2 ***Chairman:*** I am sorry your colleague has been waylaid. Thank you very much for coming to give evidence to us. For the record, this meeting is on the record and it is part of this Committee's inquiry into the EU/US Passenger Name Record Agreement, to be known as PNR from now on. Dr Hosein, I wonder whether, on your own behalf and on behalf of your colleague, you would like to give us an opening statement.
Dr Hosein: Absolutely.

Q3 ***Chairman:*** Would you be prepared to describe not only your own connection but, also, insofar as you are able to, speak on behalf of Privacy International. I know that Simon Davies is not here actually speaking on behalf of Privacy International but I think it would be helpful for the Committee to have your picture of what both organisations are and your interest in the subject of this inquiry.
Dr Hosein: As background, today I am speaking as a Visiting Scholar of the American Civil Liberties Union, which is the largest civil liberties organisation in the United States, and which has taken the government to task on most of the anti-terrorism measures in the past few years. I am also a Senior Fellow of Privacy International, which is the organisation that Simon Davies is a Director of. Together, Simon and I have been working on EU/US surveillance measures since the 1990s, but particularly since 2001 with the advent of passenger data transfers and the more recent transfer of financial information, and so on and so forth. Together, Simon and I are also Visiting Fellows of the London School of Economics where we have done research on this issue and other issues, such as ID cards and communications surveillance. We have spoken before at various Committees in the House of Lords on those issues in the past. Specifically on Passenger Name Records and the transfer of data to the United States, we denote that US law does have a number of protections and safeguards; they have the Privacy Act 1974, for instance, which is a relatively strong safeguard against the abuse of information. The problem with that regime, however, is that it only protects the interests of US persons. That is, if you are not a US citizen or US resident that law does not apply to you. So that is why the whole transfer of data between the EU and the US is such a massive legal problem because American citizens have rights within the United States but EU citizens do not. Meanwhile, within the EU regime EU citizens and foreigners have privacy rights, and that is the battle between the two blocs. I am not sure if you were briefed on the latest news that has emerged from the United States but the *Washington Post* today has run an article about a new data mining programme that has emerged from the Department of Homeland Security that seems to be the son of Total Information Awareness, which was the programme that was shut down a few years ago; somehow it has re-emerged and the Department of Homeland Security has promised the American public they have nothing to worry about because they have only been using foreigners' data and across America there is not that concern about the data of foreigners. That is the general problem that we deal with on a daily basis when it comes to this issue; the legal black hole, and then there is the inattention to data outside of the US by Americans.

Q4 ***Chairman:*** Thank you very much. You used the expression "data mining". Can you explain what you mean by that?
Dr Hosein: Data mining is the collection of vast amounts of information from various sources and then running algorithms against that data to draw patterns and conclusions. So if you are able to

develop a profile of what you imagine a terrorist would be like—what kind of mobile phone company that terrorist would use; what kind of travel patterns, what kind of telephone patterns, and so on and so forth—and then collect vast amounts of information about vast amounts of people the theory is that using advanced algorithms you can identify other people with similar profiles to that terrorist.

Q5 ***Lord Foulkes of Cumnock:*** Can I ask one question about the organisation? Ironically, I know a bit more about the American Civil Liberties Union than about Privacy International. Although Simon Davies is not here you obviously work very closely with him. Is it a membership organisation, Privacy International, and how many members does it have, if it is?
Dr Hosein: It is not a membership organisation it is a watch-over organisation with an advisory board of 50 people from 30 countries established in 1992. So we have been a London-based organisation since that time.

Q6 ***Lord Foulkes of Cumnock:*** Is it a registered charity?
Dr Hosein: It is a limited liability company.
Lord Foulkes of Cumnock: It is a limited liability company. Does it have a sort of charter or—what do they call these things?
Baroness D'Souza: A mission statement.

Q7 ***Lord Foulkes of Cumnock:*** A mission statement! Thank you very much.
Dr Hosein: Yes, I have not memorised the mission statement but, generally, we act as a watch-dog organisation looking at surveillance policies and freedom of expression policies emerging around the world. We have conducted campaigns in Australia, the Philippines, New Zealand and, of course, in the United States and across Europe. In the past few years we have been very busy with the European Parliament and lobbying against some of the proposals emerging from the European Commission.

Q8 ***Lord Harrison:*** Can I just ask a supplementary on data mining? Has it existed long enough for conclusions to be drawn as to how effective it is? If these algorithms are used against vast amounts of data have they indeed thrown up profiles of people who are then examined and who are found to fit the frame and, indeed, may have had such tendencies that we should want to be aware of? I gather from your tone that you have some doubt about the effectiveness, but I do not know whether perhaps you could illumine that.
Dr Hosein: For the sake of being fair and slightly academic, I will give you one example where it does not work and one example where you could say it has worked. The jury is still out as to whether data mining works; there have not been enough open studies to verify what kind of algorithm was used, whether it was a fair algorithm, what kind of data was used, whether the data was actually reliable, which is one of the key problems because sometimes the data is inaccurate but they then make judgments against you. This is exactly the problem with PNR, but I will come back to that in a second. The first case I will give you is MATRIX. The acronym stands for multi-state access to law enforcement information, but I cannot remember the exact words. It was a private company that offered this service to the US Government after September 11 2001. They approached the Department of Justice in the United States and said: "We are willing to run a data mining office; set up data that we have gotten from member companies and from the Government and we are going to help you identify terrorists". The company also told the US Government that because of the law in the United States the US Government is unable to do this but because this company is a private company they are able to process this information without any due regard for civil liberties. So the company then ran, against this mass dataset, the profiles of the 19 hijackers and said: "Who else in the United States resembles these 19 hijackers?" If I recall correctly the exact number was 250,000 Americans who were just like those 19 hijackers. So there was a lot of fury but, also, excitement over the idea of data mining. Apart from selling this product to the Department of Justice, this company then went to all of the States to try to sell it to each and every one of the States, so that their police would be able to have access to these data stores, and so on and so forth, but because of the public uproar and because of the number of errors that emerged every State ended up abandoning that programme and falling out of it to the point where there was only one State left standing, and that was the State of Florida. Then, finally, the project came to a close. So that is one of the cases where it does not particularly work well. In the *Washington Post* article this morning I read about this new data mining scheme that has not been tested openly, but the proponents of the scheme have said it has proven to be useful in the situation of Guantanamo Bay, where they have data-mined the detainees. Originally, before the data mining, they identified the detainees they knew were caught up with bad people and they developed a profile based on those bad people and applied it to the rest of the detainees, and were then able to identify the detainees who were innocent. So in that sense data mining is applied to prove that you are an innocent, not to identify the guilty. So that is a case where, arguably, you could say data mining has worked in that small situation based on I-do-not-know-what kind of data they have on these detainees. However, when you apply data mining to a large

population, such as a country, you have the inherent problems of how good is the algorithm, how reliable is the data and how legal is this entire process? In the United States, for instance, data mining is tantamount to being illegal. After the uproar over Total Information Awareness, which was the first programme to be developed by the Department of Defense, eventually Congress (and, remember, this is actually a Republican Congress) pulled the funding and said: "You are no longer allowed to do research in this area". Then there was another data mining programme through passenger surveillance of Computer-Aided Passenger Pre-Screening programme, just to make sure that violent offenders do not board aeroplanes, and eventually the funding was pulled on that and the Department of Homeland Security admitted that the system could not be built, so they had to move on. On top of that, a piece of legislation was passed saying that no funding can go towards a data mining programme of any sort in the United States, ones that apply to the general population. Somehow these programmes keep on emerging but there is no funding for them.

Q9 ***Lord Jopling:*** Who are the people who are doing the research to try to demonstrate that data mining works and what access do they have to what some of us would think was the most sensitive intelligence information, like, for instance, material gathered by Menwith Hill in Yorkshire? How deeply are the people who are trying to establish this system permitted to go into sensitive intelligence information?
Dr Hosein: To begin with your last question first, the individuals who are involved have the highest levels of clearance in the United States Government. They are former directors of agencies. Two of them have been admirals in the Navy—so they have the highest possible clearance. On the exact departments that have been doing this work, one department was the Department of Homeland Security. They have been responsible for the passenger surveillance programme, in particular, and that applies particularly to the sub-agency within the Department of Homeland Security, which is the Transport Security Administration. Another department in the Department of Homeland Security that has been doing data mining has been the Customs and Border Police. That is the department that, it emerged, was doing profiling of all passengers to the United States. This news just emerged in November about an Automated Targeting System. The most significant research programme on data mining emerged from the Department of Defense, from the Department of Defense that was responsible for the creation of the Arpanet, which eventually evolved through to become the Internet. This is where the brightest of the bright do their research within the Department of Defense, and they were responsible for Total Information Awareness (or the Terrorist Information Awareness programme, as it was renamed). So it is always those with the highest clearances making use of various forms of data. You rightly pointed out the data issue.

Q10 ***Lord Jopling:*** Before you go on to that, you did refer to "private company" earlier on. Does some of this research take place outside the various defence departments of state, whoever they are?
Dr Hosein: There are a number of private contractors who are interested in selling these types of services. So the company behind the MATRIX system was eventually bought up by Reed Elsevier, the publishing company. There are a number of consultants who advise on these projects from the private sector, particularly from Booz Allen Hamilton, which is a company that is the largest contractor for IT to the US Government, particularly because three of their five directors are former heads of the intelligence agencies, such as the National Security Agency and the Central Intelligence Agency. One of their vice-presidents was appointed the Head of National Intelligence in the United States. So it is these types of firms that are aiding the research in this field. There are also academic institutions, and I am afraid I cannot list them off the top of my head, who get funding to conduct research on the algorithms of data mining, but they do not get access to the wide variety of data. To come back to the data issue, the source of the data is always a source of controversy. At first the US Government approached a number of airlines in the United States, such as Northwest and JetBlue, and there are quiet agreements to transfer all data to the Department of Homeland Security to test out these algorithms historically, to see if they would be able to sustain a real environment. Once the news of these transfers emerged, passengers filed a number of legal complaints against these companies, saying: "We did not consent to our data to be used". When that strategy failed the Department of Homeland Security then said: "Okay, we will use the data of foreigners", particularly the EU passengers under the PNR Agreement. So the PNR Agreement that emerged in 2004 between the EU and the US permitted for the use of the data on EU passengers for the testing of what was then known as the Computer-Aided Passenger Pre-Screening system, or CAPPS-II. The most recent news about data mining from the United States is that it uses foreigner data and anonymised data of American citizens, so, again, that is going to be a source of controversy because American citizens are going to ask: "How anonymised is this data before you mined it?".

Q11 ***Baroness D'Souza:*** I gather from what you say that the ban on funding for the Government itself to undertake this kind of data mining activity does not extend to the American Government paying private companies or academic research institutions for research that they are doing?
Dr Hosein: I believe that is entirely correct.

Q12 ***Baroness D'Souza:*** So, in fact, the American Government is funding it.
Dr Hosein: Absolutely. After the Total Information Awareness programme met its demise a lot of the researchers and the research funds that had been allocated to this were actually put into what are called "black budgets", so within the budgets that other people could not see. Then there is the other strategy, which was when we found out about the Automated Targeting System, which is the data mining programme that is conducted at the US border, which we just discovered in November of this past year. The way that the US Government got around the funding problem is that this targeting system was originally applied to cargo. So it was developed and funded to apply to cargo—the ship moving the cargo, who sent the cargo, and so on and so forth. What the Customs and Border Police failed to notify Congress was that they then started adding passenger data to this same machine. So, in a sense, additional funding was not required. In a sense, it was a "bait-and-switch"; it is: "Here, fund this cargo-profiling system", and, "Oh, lo and behold we are applying this to passenger data". It is leading to Congressional hearings because there is this concern that regardless somehow this scheme is illegal under US law.

Q13 ***Lord Marlesford:*** Is all of what you have been saying purely related to terrorism or does it also cover other forms of serious crime?
Dr Hosein: It is important to note, first, that the PNR transfer agreement applies to terrorism and serious crime and organised crime of a trans-national nature. So it is a little broader than terrorism already. The MATRIX system was being applied beyond terrorism as well, and the Automated Targeting System (again, this is something that we learned about in November), according to its mandate and according to the statements made to the public from the Department of Homeland Security, is for combating terrorism, serious crime and border offences. So it has broadened out in its purpose, and I would almost say that its primary purpose never was terrorism per se; its primary purpose was to help manage the flow of information heading towards the US Government regarding foreign travellers.

Q14 ***Chairman:*** I think Lord Marlesford has very helpfully set the scene for our first question! You have defined for us very concisely the purpose of the PNR agreement, which is to enhance the security of the United States, both against terrorism and against organised crime. To what extent do you think this has actually been effective? It is a difficult answer, but can I also, at the risk of pre-empting a later question, ask you to draw a comparison between the effectiveness of the PNR Agreement and the effectiveness of a visa system?
Dr Hosein: It is inevitable that the mass surveillance of a given population has some advantages; it is inevitable that you will be able to pick out somebody amongst the masses. For instance, with the US VISIT system, which is the fingerprinting system at the borders, the government is very fond of saying they have had 80 million people travel through the United States and get fingerprinted and they have caught 2,000 people. They did not say they were 2,000 terrorists but they said they had caught 2,000 people. If you do the calculations, that is a 0.000025 per cent success rate. So I am not entirely sure what you are looking for when it comes to effectiveness. It is easy to say how effective this is, it is harder to prove it, in the sense that when passenger data was first considered as useful data for the US Government, it was originally considered for the Computer-Aided Passenger Pre-Screening System, or CAPPS-II (which I will refer to as CAPPS-II from now on). Since that time the CAPPS-II system has failed. The former Secretary of Homeland Security, Tom Ridge, when he gave his press conference about how they were shutting down CAPPS-II, he literally took a knife to his heart and said: "We're cutting it; we're killing it; it's dead", not only because of the privacy concern but the technological concerns. This is where we get into the whole area of the actual effectiveness of this data. I have spoken at length with a number of industry officials in the airline industry and they always reiterate very carefully that PNR is not some beautiful dataset that every government is dying to get their hands on; PNR is a highly unreliable set of data. There are misspellings of names and there is inaccurate information taken down generally about eating, seating, and so on and so forth. It is not this perfect set of data. As a result, how useful is this imperfect set of data? When you promise to use it for data mining it is highly dangerous because you are going to start identifying the wrong people for the wrong crimes, as we have seen emerge in the United States with their own watch-list—the "no-fly" list is what it is called—where they verify names of people before they get on aeroplanes within the United States. There have been 30,000 complaints against that watch-list of people who have been unable to get on 'planes. We have not heard similar

situations about foreigners being unable to get in the United States because there is no duty to report on these issues.

Q15 ***Chairman:*** Can I interrupt you there? You referred to unreliability. To what extent, from your understanding of where the PNR Agreement stands, does the Agreement take into account that degree of unreliability?
Dr Hosein: Absolutely not at all. In all the political rhetoric (and this debate is mostly about political rhetoric) it has only been about how this data is inherently useful for the war on terror; there has been no critical questions regarding the integrity of the data. I have to admit, when I discovered that this—it was only about a year ago—data was not reliable, I was shocked because I bought into the whole argument that this was essential.

Q16 ***Chairman:*** I am sorry, I interrupted you.
Dr Hosein: One final point, which is that it is important to remember that when the US Government passed the law regarding access to Passenger Name Records it was actually just one line within a large piece of legislation. The one line said that the US Government may demand from foreign carriers to hand over Passenger Name Records. That is all it said. It is a massive piece of legislation, and one line. Somehow that one line emerged and developed into this massive surveillance system. I do not believe the US Congress is fully aware of how far it has gone.

Q17 ***Lord Jopling:*** The Agreement lists the 34 "data elements". I wonder if you could tell us to what extent those 34 items are used. Are there some which have not been used at all? I wonder if you could tell me which of them are, in practice, used and exploited.
Dr Hosein: I have to provide a very large caveat before I answer that, which is that very few people understand how this data is being used, and the reason very few people understand is because there has not been open review. The only review of the US Government's use of Passenger Name Records occurred in 2005 and was conducted by a number of EU officials and two officials from the Data Protection Commission Offices; one being the Assistant Information Commissioner in the United Kingdom and one being a Deputy Commissioner in Germany. They conducted the only review that has taken place and when they conducted the review they were forced to sign non-disclosure agreements by the US Government, so they could not, other than what was within the legal mandate, discuss the general operations of the data mining and how it is actually conducted. That report was only published last year (the report that eventually emerged, which was heavily redacted) and still to this date we are unable to fully understand how this information is being used. So, having said that, the controversial points when it comes to 34 fields of data focus particularly on what are numbers 26 and number 27, the OSI information and the SSI/SSR information. These are the fields that could contain sensitive personal information of a medical nature or a religious nature. So this could be where a request for halal food is made or if it says you have heart disease. It also discloses information about your travelling companions, so it could say you are travelling with somebody who is not your official, legal partner, and so on and so forth. The situation after the first agreement between the EU and the US was that this data would be 'pulled' to the United States by the US Government, which would then log into the reservation systems and grab this data themselves. Or, if it was possible, the carriers would send this data to the US Government, at which point the US Government would filter the sensitive fields. So they would go through all the data and delete the data that said anything about the food requests or your travelling companions. The review that took place in 2005 gave the US Government a favourable note on this; it said that the US Government had effectively implemented this filtering process. The question always emerges why do the carriers not filter this information before they send it on to the US Government, and many of the carriers I have spoken to are very happy to do so, but there are a select few carriers, including British Airways, who are reluctant to filter the information; they prefer to send the wholesale information to the US Government and let the US Government take care of the filtering.

Q18 ***Baroness D'Souza:*** Why?
Dr Hosein: I believe it is slightly beyond my competency to say why, but I would guess it is because of the cost issues.

Q19 ***Lord Jopling:*** How on earth do airlines or anybody else know if you are travelling to New York or somewhere with your mistress or somebody else? You have got two separate names and two separate bookings, maybe. How on earth does anybody know who your travelling companion is?
Dr Hosein: The seating arrangements and whether at the time of booking you requested to sit with somebody else would probably be stored within the PNR.

Q20 ***Lord Jopling:*** You have talked about the items 26 and 27. I wonder if you would enlarge on that and, also, bring in 25, the No-show one, and just enlarge on the way those work, if you would be kind enough.

Dr Hosein: If I could just clarify, on 25 (this is a note that I incorrectly raised with the clerk earlier), it is actually "Go-show" information. Upon research, I found that Go-show information is about the passengers who have purchased a ticket at the airport; they are the last-minute fliers.

Q21 ***Chairman:*** We thought we had made a misprint in the questions.
Dr Hosein: I had also noticed that, but field 23 is No-show information as well. So Go-show is specifically a walk-up passenger; someone who presents themselves without a ticket or reservation and buys a ticket to travel immediately. Not all airlines treat this individual as a Go-show. That is an important note as well. Every airline and every reservation system treats PNR in a very different way. So some carriers will say: "This person does not qualify for the Go-show field"; instead they will just say a one-way passenger. So there is disparity amongst airlines about how this information is dealt with.

Q22 ***Lord Jopling:*** Would you like to expand a bit more and tell us a little more about the OSI and the SSI and SSR?
Dr Hosein: As much as I can, which is based on conversations with airline officials. The answers are always very different because it is almost as if these are free fields; there is no conformed way of establishing the data in this field; it is where they put other related information. They may have different formats for putting what your food preferences are within the OSI, and special service requests as well—so if you request a wheelchair, and so on and so forth. Every carrier deals with this in different ways and has different codes for this type of data.

Q23 ***Lord Marlesford:*** I am looking at this list of 34, and data element 33 is: "any collected APIS (Advanced Passenger Information System) information", and number 27, which is SSI/SSR information. Would you like to tell us a little about these? As I say, I find the whole of this list quite bizarre. Some are obvious. How is the list compiled, perhaps, should be the first question?
Dr Hosein: The first question, the list was compiled through a process of negotiation where originally, as I stated earlier, the US Government interpreted its legal mandate, which was to gain access to PNR, as the right to log into the reservation databases of airlines and have free access, even for travellers who are not travelling to the United States. Eventually, this was curtailed slightly and the US Government said: "Okay, we're happy with 39 fields of data". That is when the EU and the US went to battle over how many fields of data. The EU Privacy Commissioner said there is no reason why they should use more than 19 fields of data, as the Australians and the Canadians have already requested only 19 fields of data. The Americans were adamant on their 39 and then somehow we ended up with 34. It was a long, tortuous process and I do not know how—is this magic with the 34 and not 32—but this is the list that we were left with. The difference between the APIS information that you are speaking about and the list of fields and, say, the SSI information is that the SSI information and the OSI information (also called SSR information) is behavioural data. It does not say anything about your identity, it says something about you. APIS information is, generally, the information collected about your nationality and the information that is on your passport and, possibly, the manifest data, such as seating, and so on and so forth. That is identity information. So it is important to recognise that the whole battle over PNR versus APIS is that PNR is all about your behaviour, and that is why the US Government wants it; it is not because they want to identify you, it is because they want to draw conclusions based on this data. Answering specifically on field 33, on any collected APIS data, APIS data is nearly 100 per cent of the time collected at the check-in point. That is when you hand over your passport to the check-in agent, they collect your personal information and that is when the manifest is created. It is not usually created before. The data in this field is for those situations where when you have spoken to your travel agent or when you bought your ticket online, if you happen to include this data in that process of purchase then it would reside in the passenger data record. Even still, that data is not highly reliable; it is not reliable upon because errors could have been entered in passport numbers. People are not really accustomed to handing over their passport number on the telephone or in the travel agency, and so on and so forth. So the APIS data is almost always collected at the check-in point, and that is the data that is considered highly secure and relevant data which is then transferred onwards.

Q24 ***Lord Marlesford:*** A conclusion one could draw from your reply is that if the alternative to the PNR system is to go back to visas, the information which the diplomatic missions will get on visa application forms would be, obviously, much less than the PNR provides, because it could not have all this behavioural stuff, which the airline might be able to put in.
Dr Hosein: That is entirely correct. It is an astute observation because the PNR would contain, perhaps, religious information, as we have discussed before, and it would contain our financial information—who paid for your flight. That type of information is never requested in a visa process. I

could not agree more. It is within the negotiations that become PNR or visa waiver, and that is what the next round of negotiations are going to focus on even more so, which is can the EU somehow give up more PNR, perhaps, in favour of visa waiver access to all EU countries. That is when the level of politics goes up a notch, because this is really about the flow of people and goods without visa, and that is a highly sensitive issue. I can predict that the Americans will make a number of promises about consideration of the visa waiver programme for the EU Member States who are not already in the programme, but I can say from my reviews of the way US Congress refers to the visa waiver programme they would love to shut it down if they could; they do not like the idea of anybody coming to the United States without having to get a visa. It is the civil servants in the United States Government who are adamant about maintaining the visa waiver programme because they understand it is good for trade, and so on and so forth, but there are other civil servants who also realise that this can be used as a negotiation tool.

Q25 ***Chairman:*** Are visa application forms for those nationalities that still require visas being amended and added to take into account the information that comes under the PNR?
Dr Hosein: I do not believe that is the case. There have been a number of changes to the visas over the years from the US Government, and they have expanded the data collection; they have gone so far as to include biometrics, as is happening in the United Kingdom as well. It is important to note that the visa programme is actually run by the State Department, the equivalent to the Foreign Office, and while PNR is being accessed by the Customs and Border Police in the Department of Homeland Security they have two very different missions and two very different views of the world. I would be surprised if they were a signatory in this area.

Q26 ***Lord Marlesford:*** In the negotiations between the EU and the United States on PNR it would not be unreasonable for the EU to say: "As these are alternatives and as you would have the right to re-impose visa requirements, if we do not accept your PNR, equally we could say that we will give you, through PNR, all the information that you could get on visa applications but no more. Or indeed if there were to be some more that would be part of the negotiations".
Dr Hosein: I believe that would be a very useful strategy. The reluctance would emerge from the airline industry who have already faced a number of burdens since September 11 2001, but they are reluctant to take on new data collection. So if the carriers were not responsible for collecting, say, the biometrics that now go into visas and additional personal information that go into visas they would be highly reluctant to do so. They already do not enjoy having to hand over this information to the United States, especially because they have to pay for these transfers themselves; they would be even more reluctant to take on new duties.

Q27 ***Baroness D'Souza:*** Does your research show that passengers are, on the whole, aware of the information that is supplied about them to the US authorities, and the use to which it is put?
Dr Hosein: We have seen our research of general holiday travellers, and they are not very aware of the practices. I have seen research and polling done of travel executives and they are very aware of the fact that transfers are going on and they do have a number—

Q28 ***Baroness D'Souza:*** "Travel executives" meaning?
Dr Hosein: Corporate travel. It is research emerging from the Association of Corporate Travel Executives, and I always shorten their name the wrong way. It is only recently, on February 15 of this year, that the Article 29 working party, which was the committee of the Privacy Commissioners of Europe, came out with draft language for a short notice that they expect that the EU airlines will present to passengers in the future, describing to them what is happening with their data and how it is being used, to the level of knowledge that they have. The Article 29 working party also released on February 15 a Frequently Asked Questions. I presume they hope that this will go on the websites of the carriers so that people who are concerned can get access to that information. Generally, we have found that the awareness of the practice and the use of that information is very low. I would say that this is also true within the US Congress.

Q29 ***Baroness D'Souza:*** As a supplementary, you have already said something about complaints and that there is no duty to actually report these complaints, but can you say something more about the complaints received from passengers and how they are treated?
Dr Hosein: There is no duty to report on the number of complaints received from foreign passengers. The Department of Homeland Security, which only recently opened up what is called a Trips Office—I am afraid I cannot remember what the acronym stands for, but it is now a front page item on the Department of Homeland Security website so it is a brand new initiative. That is the interface for people to complain about the use of their information and this was again a very recent phenomenon. The interesting thing about this trips

office and the way it deals with complaints, there are two interesting things that emerge. First, they say that your complaints data may also be used for other purposes, so the fact that you complain might be used against you at some point, and any safeguards against the data emerging from the complaint is protected by the US Privacy Act 1974 which again only applies to US persons. We have not seen any reporting on the number of complaints received from, say, EU citizens and we have not received any reporting from the various privacy commissioners across Europe regarding how many complaints they have received from their citizens as well. Unfortunately, therefore, we cannot count; it is impossible to know how many complaints there have been and it is also near impossible to know how many errors have emerged because again this entire process takes place behind closed doors, within closed computer systems, to the point where even the Government of the United States is not aware of what is going on.

Chairman: That probably negates Baroness Henig's question, but are you going to ask it nevertheless?

Q30 ***Baroness Henig:*** I will ask it anyway. I was just wondering what remedies were available to EU citizens who believe their personal data has been misused or the undertakings have been breached.

Dr Hosein: The advice from the Article 29 Working Party in their February 15 document is somewhat amusing because ironically foreigners, although they have no protection in the United States under privacy law, foreign institutions and foreigners generally can apply under freedom of information laws in the United States. Actually the US has one of the strongest, most powerful and expansive regimes of freedom of information so if you want to get answers as to how your data has been used you can go through the freedom of information.

Q31 ***Earl of Caithness:*** Is there another way that one could use PNR, for instance under an electronic travel authorisation, which would be simpler and easier?

Dr Hosein: Yes, it is possible. This is an idea that the European Parliament recently emerged with in their declaration last month. It is a process that has been going on in Australia, for instance, where instead of having to apply for a visa if you are travelling to Australia—I have never done this so if somebody who has travelled to Australia recently can correct me I would appreciate it—apparently as a British passport-holder or a Canadian passport-holder, which is what I am, I would fill out a form on a website that would then be accessible to the immigration official in Australia where they would get the necessary information. This is a much more effective process for transferring information. I have spoken to a number of airline officials who would love it if this was the process instead of the transfer of passenger name records because they want to be outside this process, they do not want to have to do anything in this entire transaction. They do not want to be immigration checkpoints and carriers definitely do not want to be liable for information that is sent onwards, so they have been calling for a number of years for a similar situation because people can fill out website forms on the US Government's website just the way they have done on the Australian Government website. As a privacy expert and advocate I would say I do not believe it is necessary to transfer this information to begin with. I believe that what has happened is that there has been a drive around the existing source of data which is passenger name records, and that is what the focus of the debate has been on. It has not been about we need to know more information about the people travelling to the United States, it is more we want to tap into this information on people travelling to the United States. If the Americans limited the information merely to identity information then it would almost be acceptable, it would be a mini-visa as you would say for the electronic travel authorisation, but it is clear that what the Americans are after is behavioural data, and that is why they have been going after the passenger name records.

Q32 ***Earl of Caithness:*** Could you just remind us in terms of the PNR agreement between the EU and America and also the similar one between Canada and America, how much of that is push and how much of it is pull?

Dr Hosein: The first agreement in 2004 was all about the Americans went into it asking for pull, and then as it emerged in the more recent agreement it was mostly about push. In the Canadian situation, the Canadian access to foreign carriers airline data is push. Every country apart from the United States that requires passenger name records it is all about push; generally countries do not want to log into BA's database to start trawling around, nor does BA normally want that to happen. The Americans are the exception because the Americans have the power they have to refuse airlines to travel.

Q33 ***Lord Foulkes of Cumnock:*** Dr Hosein, we have a copy of your joint letter to Vice-President Frattini and in paragraph 2 you say "ATS then generates a risk assessment score for all passengers." Could you amplify how that risk assessment score is calculated?

Dr Hosein: It is impossible to know; that is again the problem. ATS has not been openly reviewed by any Government agency; the Government Accountability Office of the US Government which is the most powerful investigatory body within the

US Government in all of its reporting on ATS never noticed that it was actually being used for passenger data, so there has to this date not been any review of ATS. What we have made use of in order to draw these conclusions are all the public statements and regulatory statements made by the Department of Homeland Security on ATS and, as well, the statements made about the ATS background applied just to cargo instead of passengers. In their regulatory statements the term used by the US Government is "risk assessment score". They have previously also used the term "algorithm" which hints data mining because you are trying to make sense of vast amounts of data. From discussions I have had with officials and experts in this area, my understanding is that based on the data they have come up with a number score between zero and a hundred, and based on the number score a flag is then raised and that flag is then seen by the customs official, immigration official at the border.

Q34 ***Lord Foulkes of Cumnock:*** I wonder, My Lord Chairman, if I could jump to what is the central question. You describe yourself as a privacy expert and advocate and everything you have said has been in relation to protecting the interests of individuals, but we are living in a very dangerous world. You spoke about serious crime; there is a lot of that around and there are people travelling around the world who are involved in serious crime, organised crime which you spoke about, not to mention of course terrorism and the multiple threats—not just one threat, not just potential Islamic threats—of terrorism. Do you not think that in seeking to protect the privacy of individuals you are undermining the security of nations and people generally?

Dr Hosein: Every day. Every day I wonder whether what we are defending is worth defending. Every time I come back to the passenger name records issue I ask myself why am I focusing so much on this, what is so important, and then when you get beneath the veneer, once you get beneath the surface of it you see that this is mostly just politics. We would call for effective security. This is in a sense security theatre and every parliamentary process in the United States, every congressional process that has looked at data mining has concluded that data mining is not a price worth paying. They have concluded that data mining is not effective enough and despite the age of terrorism we are not allowed to open up the records of all people to run algorithms through them to identify the few. Every time that there has been a data mining programme before the US Congress regarding the use of personal information of American citizens it has been decided that this cannot go forward. That is why I am amazed that the EU is going to give the US so much latitude over this automated targeting system when the American Congress, when they do encounter this in the coming months, when they do debate the ATS, will—I know they will—think that this is a step too far. Then there is the issue of watch lists. Again, we have this image that there is one list of bad people around the world and it is properly administered by the UN and will prevent these bad people from getting on aeroplanes and shopping across borders: one such list does not exist, there are actually thousands of lists of this nature and they apply to various levels of crime and various levels of terrorism and some people who are just merely related to terrorism and so on and so forth. We are in the process of creating a mass infrastructure of surveillance presuming that it will actually work, presuming that the data is actually valuable. Again, I will go back to the example of the no fly list in the United States: thousands of people complain that they have been unable to get an aeroplane, and let us recall that it is not just people with last names such as mine, it is people with Irish last names who still cannot get on aeroplanes. There is the classic case of Senator Edward Kennedy, the brother of the former president, who was prohibited from getting on an aeroplane or had to be searched multiple times every time he wanted to get on an aeroplane because of a similar terrorist on the former IRA list that was sent to the US Government named Ted Kennedy. Fortunately, Senator Kennedy knew the head of Homeland Security so he could get the situation rectified, but not everybody else is in an equal position. Going back to the original statement, in the war on terrorism everybody understands that effective security is needed and you need to reconsider some of your original presumptions about civil liberties. You need to reconsider them, not necessarily re-evaluate them, and it does not mean that we should just take as a given everything that is said about a scheme, everything that is said about a system, as we can count on with ID cards, as we can count on with communication surveillance and as we are carrying out data mining, every time difficult questions are asked the argument offered by the Government starts to falter and you realise that truly the emperor has very few clothes.

Q35 ***Lord Foulkes of Cumnock:*** You said theatre but, with respect, you were being a little theatrical earlier on when you said there were 80 million people who had been surveyed and they had only caught 2000, and then you said this is 0.00025 per cent, rather theatrically. If 2000 have been caught, those are 2000 people who might otherwise have been going on to commit terrorist acts, serious crime or take part in organised crime, so we are better off

that 2000 people have been caught then not caught; is that not right?

Dr Hosein: It is not right to almost reverse the burden of proof where everybody has got to present information in a way that is not actually safeguarded and then hope to not be identified wrongly, and there have been wrongful identifications that have taken place such as for every extraordinary rendition that has taken place in the United States there have been a number of errors where the wrong person was sent abroad. Is that too high a price to pay in the name of the war on terrorism? What I was saying was 80 million people have travelled to the United States border and had their biometric data collected. This data is actually collected for 100 years; this data is not safeguarded, it is not prevented from being used by other government departments, in fact it can be used by any state or local or even tribal authority across the United States. These are not clear and effective safeguards. If they really want to fight the war on terror, if they want to truly manage this information, they would introduce proper safeguards. There are not the proper safeguards in place. The 2000 people—this type of debate emerges every time we look at the DNA database in this country; ministers are always very proud of saying we have caught this rapist and this paedophile and so on and so forth—we are not given the details of who these 2000 people were; we are given the details of four of them who happened to be four rapists, there has not been one case of a terrorist being caught by this scheme. Yet they are fingerprinting everybody over the age of 18 travelling to the United States and they are moving to ten fingerprints in the foreseeable future. Is this a case of taking too large a measure against too small a problem?

Q36 ***Lord Foulkes of Cumnock:*** If we take the United Kingdom, at the moment there are some opposition politicians who criticise the Government, as you are doing, for invasion of privacy. The same people are also critical because the Government cannot say how many illegal immigrants there are in the United Kingdom. They cannot have it both ways and you cannot have it both ways and you have criticised and you have put up very effective criticism of what the Americans are doing, but what you have not said is what they should be doing alternatively to deal with what you admit is a real problem.

Dr Hosein: I will start with the second bit first. We have always called for safeguards, we have not said you must stop all transfers of all sorts, but we have identified where sometimes people are not entirely sure what PNR is and how it is actually used, and perhaps a piece of paper would be sufficient. We have advocated for strong safeguards and these measures can go forward. We are not lobbying against the transfer of data to Australia because the Australians are only asking for 19 fields of information, they are only keeping it for 48 hours. The Americans want to keep this information for 40 years so there is a lack of proportion that is going on and that is what we go after. You raised the issue of illegal immigration. The American Government is spending close to $15 billion on the US-VISIT system and there was just news this week and a Government Accountability Office report last month that said that the system was highly complex and unlikely to ever work, and they have noticed that they cannot actually check the biometrics of people leaving the United States so while they can check people coming in, there is no ability to monitor the exit process so how do you get around the illegal immigration problem at that point when you may have let the people in the country and you cannot manage to get them out. I am not going around saying all surveillance is bad, I am not going around saying the US Government is awful or the choices made by this Government are awful, I am trying to penetrate below the politics and show where there are serious problems and serious concerns and we need to debate these serious problems and serious concerns and not reside at this top level of fear.

Chairman: Can we have some quick questions relating to this from Lord Harrison, then Lord Jopling and then Lord Listowel?

Q37 ***Lord Harrison:*** Like Lord Foulkes I too hesitated when you gave the figures which were 80 million, of which there were a quarter of a million who were identified of which 2000 were then convicted or caught of whatever. Actually, a quarter of a million is many fewer people than 80 million so if it is in the right ballpark I would have thought it was of advantage to the security services. Granting what you say about the diciness of some of the data and the grounds upon which it is put, it would still be interesting, would it not, to look at that 2000 against another representative sample of quarter of a million? In other words, that may then in turn give you some indication of whether indeed the sift through the 80 million fingerprints was putting you in the ballpark of those who should fall under suspicion.

Dr Hosein: The quarter of a million I was referring to was through data mining of private sector data and government data after 9/11 to identify terrorists based on a profile. The US-VISIT system does not work on a profiling basis, it works on collecting the personal information of this individual and the biometrics of this individual, does this match any databases of concern, and then a flag will go up and say this person is a wanted rapist so stop this person, or this person has previously been convicted, send this person back home. I would be careful not to confuse the 80 million, the quarter of a million and

the 2000. When the US-VISIT system came in the US Government said do not worry about this, we are only taking two fingerprints, we are not treating you like criminals. We warned the US Government at that time that two fingerprints were ineffective and if you were really going to take the fingerprints of individuals you had to take all ten fingerprints, and the US Government said no, no, there is no such worry. What is happening in June this year? They are moving to ten fingerprints. The other concern is if you really want to verify people against the list of fingerprints held in the FBI database—and we warned the US Government of this—the fingerprints taken at the border are just simple fingerprints and not the sophisticated type of fingerprints you need to take at police stations in order to verify criminals against the fingerprint database. The US Government said that is just proof we are not actually treating people like criminals, we are just taking simple biometrics to verify people against their visas and the next time they return and so on and so forth. Now the US Government is saying the new fingerprints are going to be taken in a format that will be interchangeable with the FBI database of fingerprints. My point behind all of this is that at first the system was introduced as a nice people management system and now we are finally understanding that it is actually a criminal management system, treating all foreigners as if they were criminals. It would almost be acceptable—and I would never advocate this—if this practice was applied to American citizens, but it is not being applied to American citizens because that is considered unpalatable. Why is it palatable to apply it to foreigners? It is because we do not care about foreigners, it is because—and this happens in the politics of every country—you do not worry about the other; meanwhile the other, these foreigners coming in, they are at their least powerful status in the entire world as they are when they are right outside of a border. That is when we know that we can treat them the way we have been treating them, we know we can take any information we want from them because they do not have the right to say no. This might be the state of affairs that everybody is happy with, that is absolutely fine and I am willing to settle with that, but let us also admit that we are taking advantage of the situation, we are treating people like criminals for no reason or for a reason we would not treat our own citizens as criminals.

Lord Harrison: I will leave it there, it is an important point.

Q38 ***Lord Jopling:*** Leaving aside how you take fingerprints, I would like to allow you to put on the record your basic approach to all this. Do you regard the taking of fingerprints in a mass way like this as an invasion of privacy and, if you do, would you accept that the huge majority of us are perfectly happy to have our fingerprints taken and kept on the record for as long as anybody wants?

Dr Hosein: First, do I consider it invasive? Yes, absolutely. Maybe this is a generational thing, but I come from a generation where you were fingerprinted if you are a criminal. In today's modern society you might be fingerprinted in other ways such as gaining access to a building, but that is a very proportionate fingerprinting scheme that is actually effective. It raises a larger question, is it effective to add more fingerprints to a database to try to identify people? We watch too much crime drama on television and we presume that a fingerprint match is a simple process; in fact it is a very sophisticated process and when you actually run a fingerprint match against a database, what is being given back to you are the nearest results, but that is acceptable when the nearest results are people who are criminals because that is why their fingerprints are on the database. When the nearest results are innocent people who have never been a criminal, but their fingerprints are part of that database, problems emerge. Let me give you the example of Brandon Mayfield. Brandon Mayfield is a Portland, Oregon-based lawyer who converted to Islam a few years ago. His fingerprints were on the US Government databases because he served in the first war in Iraq, he served within the Army. After the Madrid bombings, one of the bags had not exploded and the Spanish police were able to lift a fingerprint of the bag; the Spanish police looked through their database of criminals and terrorists and could not identify the fingerprint, so they made the call out to all other police agencies around the world, does this fingerprint match yours. Both the US Government and the Algerian Government stood up and said, yes, actually we have a match, and the Americans took Brandon Mayfield, as I said, a lawyer, put him in the jail for two weeks without access to a lawyer and told the Spaniards we are willing to send this guy to Spain to face trial. Brandon Mayfield did not have a passport, he had not left the United States for a number of years, and there was a massive investigation afterwards because three FBI experts on fingerprints confirmed that it was his fingerprint, even though it was later discovered that it was not his fingerprint, and so he was kept in jail illegally, he has now sued the US Government and they recently came to a settlement, I believe somewhere in the millions of dollars. There was an investigation in the US Government that asked was this done because Brandon Mayfield converted to Islam and was actually a lawyer defending terrorists in Oregon, or was this merely because of a biometric check against a database? It is never as simple as we imagine it is, it is never as simple as 100 per cent match of one fingerprint against a massive database, it is far more complex. So the argument that we

present is that fingerprinting is not by its nature problematic, it is when you start increasing the pool of data for fingerprints that things start. Fingerprinting becomes more and more unreliable and that is why I go back to the original example, fingerprinting to get into a building is not problematic because it is just one fingerprint against a very small database and the error rate tends to be relatively small. When you talk about 80 million people, such as under the VISIT programme, or 60 million people as it would be under the fingerprinting programme in this country—which will be applied to citizens—that is when the errors actually emerge. Finally, on the issue of do I accept that the majority accepts it as reasonable, I do not accept that. I do not accept that the majority would necessarily find fingerprinting acceptable and I would note that support for the ID programme, for instance, particularly in the biometrics component, is as low as 50 per cent.

Q39 ***Lord Foulkes of Cumnock:*** You are quoting the LSE study, are you not?
Dr Hosein: No, I am not. The LSE has done no polling on this, I am quoting ICM and YouGov polls that originally showed—and this is the case with all the policies I have dealt with over the years. When a policy emerges at first, particularly when it is to do with the war on terrorism, support is 80 per cent because who would not support a measure against terrorists? The more people learn about these policies, the more they understand about these policies, the support for them actually goes down. Meanwhile, the United States support for US-VISIT is very high; there are very few people who would oppose fingerprinting Mexicans and Canadians who, ironically, are not fingerprinted on the US VISIT programme, but if it is Germans, British and French nationals they have no problems about it, but the Americans would not accept being fingerprinted by their own Government.

Q40 ***Lord Jopling:*** Sorry, you have confused me. You started answer my question by saying that you did think fingerprinting was an invasion of privacy. You then went on to say that fingerprinting is not problematic. Which did you mean?
Dr Hosein: I said that in a specific and proportionate environment fingerprinting by its nature is not necessarily a bad thing. I started by saying that my personal opinion is I equate fingerprinting with being treated like a criminal, but I do understand the modern world and the spread of biometrics which, Prime Minister Tony Blair is very fond of saying, the world has moved on, technology has moved on and biometrics are becoming a part of daily life. I do accept that people are willing to, say, use a fingerprint to get into a building, if it is a highly secure building and so on because they know that data is kept securely and so on and so forth. Do I still consider it an invasion of privacy? It depends on the situation, who is doing it and the reasons for which it is being done.
Baroness D'Souza: It is the context and proportion.

Q41 ***Earl of Listowel:*** I see in question 11 we deal with one of the concerns that I wanted to raise and it came up in the answer you gave first to Lord Foulkes, which is the worry about the safeguards; if they are not sufficient they alienate and will be unhelpful in the cause of preventing terrorism. The question I wanted to ask you, if you can help with this, is the commission that reported on the 9/11 attacks, if I remember correctly, particularly focused on lack of co-operation between the different agencies and an over-reliance on electrical information and data rather than human intelligence on the ground in Iraq and elsewhere, for instance in the Middle East. Listening to what you are saying there seems to be a sort of echo again in terms of what we have been discussing just now, so my concern is I recognise absolutely Lord Foulkes' concern, but is there a danger of displacing, in all this drama you were describing, one's energy towards gathering lots of information which may not necessarily be that helpful and not concentrating on the main problems which may be about human capacity and about the capacity of various departments within the US to work together effectively and to develop perhaps the people working at the front line to be able to detect people? I am not expressing myself very well, but do you see what I mean?
Dr Hosein: Absolutely, I see what you mean. More often than not I believe in most of the cases where there has been prevention of terrorist atrocities, most of the intelligence that led to those arrests was from human intelligence. The classic case of this is the July 7 investigations into the bombers; I heard one of the police who was the head of the investigation when he spoke at an event at Portcullis House last year. He said that they never relied on the communication records of the terrorists within their investigations, which I found amazing because the Home Secretary just a month before pushed a policy through the European Union on the collection, storage and retention of communications data of all EU citizens on the grounds that it would help prevent terrorism. There is a difference between the political debate that takes place which is very much about changing the balance, reconsidering proportionality and so on and so forth, which then provides for mass surveillance and the real fight that goes on which is the human intelligence, the people in the field trying to conduct investigations undercover and so on and so forth. Unfortunately, I have to stop there because I am not an expert on human intelligence and I worry that I

would actually end up saying something that is wrong, but I do agree with the sentiments expressed.

Q42 ***Lord Foulkes of Cumnock:*** Could I just ask one question following Lord Jopling's question? You answered Lord Jopling by saying that fingerprinting is an inexact science, and you gave that one example; I could have given you an example from Scotland and the Shirley McKee case as well. Surely that argues for increasing the amount of information to be collected because fingerprinting is not 100 per cent accurate, it might only be 99.8 per cent, and therefore you need other biometric data and when you put them altogether you get up nearer 100 per cent. Is that not right?
Dr Hosein: There are more intelligent scientists than I who could answer that, but based on the information I have seen, first of all, fingerprinting is not even close to 99 per cent. It has varied, depending on the algorithms used and the size of the databases, between 60 and 85 per cent—let us say it is 95 per cent. 95 per cent is still a very low measure when you apply it to the size of a population of, say, 60 million or 80 million. The other argument is the larger the database is the more margin for error you almost have to accept.

Q43 ***Lord Foulkes of Cumnock:*** You bring in another category of measurement like iris scanning.
Dr Hosein: Yes. I am going to refer to the work of the creator of iris scanning, John Daugman, who is a better statistician than I am. He said that we should not fall for the trap that increasing the number of biometrics necessarily decreases the fault level, it actually can compound the problem, so he argues that it is possible that instead of using unreliable fingerprints compounded with iris scans which were introduced not long ago, just use iris scans which have, arguably, a 99 per cent effectiveness rate; do not compound it with fingerprints. That is why the ID card programme in this country has moved away from iris scanning for the time being and they are focusing first on facial recognition, which has alarmingly low success rates, and moving to fingerprints which have a much higher success rate.

Q44 ***Lord Foulkes of Cumnock:*** I could go on, but I will not, I will do what I am told. Do you think the joint review procedure is appropriate to monitor the workings of the agreement?
Dr Hosein: In theory it is absolutely appropriate. The 2004 Agreement said there would be yearly reviews done by EU officials, including data protection commissioners, so we have hoped for the best. We are considering it as a bad situation with the agreement that emerged in 2004. The first review was done in 2005; as I mentioned, the report was not released until 2006, it was heavily redacted, we were not even given the names of individuals within the EU who were involved. On top of that, the EU officials who were involved had to sign a non-disclosure agreement so they could not actually openly discuss any of the other discoveries they had made in their discussions with the United States Government and they expressed their deep displeasure with this, the fact that they had to sign a non-disclosure agreement, so this is not exactly what I would call an open review. The 2006 review that was supposed to take place was cancelled because of the negotiations that were going on, and the United States Government has said that there will be no further reviews until after the next agreement has gone through. What was promised to be three reviews in three years has turned out to be one review in three years with no promise of further reviews, so it has been inadequate. The privacy commissioners across Europe are calling for more reviews; they are not going to get it but they are calling for the next agreement to have stronger review powers. I am not optimistic that this is going to be the case. Having said that, the review that took place in 2005 we discovered just a few weeks ago that that review had discovered that the United States was doing data mining—I am sorry, I should not use that word politically. There was already a targeting system and the 2005 review had discovered that this was being applied to passenger data. Nobody else in the United States Government knew this, US Congress did not know this, the US public did not know this, but the European Commissioners involved and the European officials involved knew about ATS, but they were not going to tell anybody about it because of the non-disclosure agreement. There is, therefore, a very awkward situation where the review might have been highly successful had they been given enough ability to communicate their findings and for the review to take place more periodically, but unfortunately the politics of the situation prevent this from happening.
Lord Foulkes of Cumnock: That is useful information for our visit to Brussels when we take evidence from the Commission.

Q45 ***Chairman:*** If Lord Foulkes agrees, the next question we have really covered, but I would like to rephrase it. That is, do you think there is an awareness? I should first of all say I am sure this Committee accepts that there is a serious security problem that needs to be addressed, but do you think that the public understand that one of the advantages of PNR is that they do not have to go through the sometimes rather tiresome visa procedure and, whatever the worries there are or may be about data protection, that is actually quite a significant advantage for the travelling individual?

Dr Hosein: Based on my knowledge of the politics within the United States I would openly answer by saying I do not believe that the two issues are related. I do not believe that the visa waiver programme and passenger name records are related at all. Politically they are related in that if 'you give us PNR, we will expand the visa waiver programme', but to my knowledge and my understanding there has been no discussion of throwing the United Kingdom out of the visa waiver programme because BA does not hand over PNR; there has not been that kind of quid pro quo over it, again, because different departments deal with this and there is a different level of politics that applies to it. As I said earlier, the visa waiver programme is surrounded by a level of politics that is more about immigration and not wanting anybody to enter the country without a visa, versus the PNR agreement which is a different level of politics about national security and so on and so forth.

Q46 ***Chairman:*** Do you detect—and this is probably not a fair question to ask you—a difference of attitude towards this whole subject between various EU countries? For instance, I do not know how much you know about the French attitude to PNR agreement.
Dr Hosein: The French CNIL—that is the privacy commission in France—has been very active against the PNR agreement, so much so that I know there are French commissioners who no longer travel to the United States because they do not want their PNR handed over and they do not want to be fingerprinted either. So the French have been very active. Meanwhile, some of the new Europe countries—as they are sometimes referred to—are annoyed that they are not part of the visa waiver programme and hope that they can do anything to get into the visa waiver programme, but they understand—and again this is the level of politics within the US Government and it will take years for this to actually evolve [en rule]although the United States might make promises to the EU that they will consider this, it is a much more separate process that takes place. It is the Department of Homeland Security that does the negotiations on PNR, it is the State Department that is responsible for dealing with such issues as the visa waiver programme.

Q47 ***Earl of Listowel:*** I want to go back to an answer you gave earlier about safeguards and the importance of those, looking at the importance of safeguards protecting public information from the point of view of winning hearts and minds in the battle against terrorism. We have recognised from the invasion of Iraq and other places that there is a danger of well-intentioned action backfiring in a way and contributing to ill-will towards us and other nations. Do you have enough information to work out in the balance whether the activities we have been discussing this morning are actually perhaps having a perverse effect, or is there not enough information yet to see whether that is happening or not?
Dr Hosein: I want to preface my answer by saying that I find it amazing that people are so activated by the US collection of this information and, in a sense, it is almost an anti-American attitude that has emerged over the US collecting this information. They see no problem with their own government or other governments collecting this information, but we seem to be missing the debate. This is something that is happening everywhere but we are focusing a lot on the US because the US was the first to ask for this information but they are also doing the worst job at managing this information. I will give you two examples that really link to the hearts and minds argument that you are proposing. The first is news from earlier this week from Canada about the law school exam—in order to apply for law school in North America you have to write an exam. It has emerged that Canadian citizens are being fingerprinted before they take this exam, and there is an uproar saying all these fingerprints are being sent to the US Government, they could be accessed under the USA Patriot Act, they could be abused and so on and so forth, and there is this sense of discomfort over it. Arguably, if you ask why you are taking fingerprints for a foreign exam it is to make sure you do not take the exam under multiple names and so on and so forth, so there might be a reason for it. However, there is such a concern that because this information is going to the US it is going to be abused and the US has lost its higher moral ground for collecting this information. Then it was discovered that the LSAT—that is the name of the exam—has been doing this fingerprinting process for a number of years. There was not a problem about it before when it was taking place, but now there is a concern because it is the Americans. My second example perhaps explains why there is this emerging concern, particularly in Canada, and that is the case of Maher Arar. Some of you around this table might know this story, but he is a Syrian-born Canadian who was travelling from a wedding in Tunisia—his wife's family is from Tunisia—he was flying back to Ottawa where he lived, flying through the JFK airport in New York and he was detained by the Americans as a terrorist. They kept him for a number of days; they interrogated him and said "Okay, we are going to send you back home." He said, "That's great" and they sent him to Syria via Jordan—they did not send him to Canada, they sent him to Syria where he was detained for 11 months in prison and tortured, according to his claims and according to a judicial commission taking place in Canada. Finally, the Syrians established that he was innocent and he was sent back to Canada. In investigations as to why this

had taken place, what basis did the Americans have to say that this individual was a terrorist, the Americans said that they had gotten information from the Canadian Government in a data-sharing agreement. The Canadian Government, through the Royal Canadian Mounted Police, were doing an investigation on somebody that Arar knew, so they had listed Arar in a database saying "of interest in this investigation because he knows the suspect". This information was then transferred to a different database within Canada where he was just included in a list of people of interest, there was no longer this link to somebody of interest, he was the person of interest. As a matter of custom this data was regularly shared with the US Government where it was put into their border database, the TECS database, where he was put in as a person of interest and suspected terrorist and that is why the Americans reacted the way they did and sent him to Syria, and the rest of the story is Canadian history. The Canadians are very angry about this and to this day actually he is still on the US no-fly list, he cannot board a plane that flies above the United States. The Americans refuse to acknowledge that he is innocent, but the Canadian Government has just awarded him a million dollars apologising for the entire affair. There is therefore a sense of disquiet in America about the US Government getting access to data; any transfer of data in a private scheme—like private companies doing outsourcing deals—has led to unions protesting en masse and saying how can our personal information collected by our union end up in the US where it can be accessed under the Patriot Act? Do I consider it is a serious concern? I do not believe that the US Government is dying to use the Patriot Act to get access to all this information, but as you say it is a hearts and minds issue. There is a level of disquiet which is alarming and the lack of confidence in transport data flows is again alarming to the point where it could lead to a breakdown.

Q48 ***Lord Marlesford:*** This is going back to Lord Jopling's question and Lord Foulkes' questions, because I am not absolutely clear on them. First, do you accept that a democratic state does need to know and know for certain who people are? Secondly, if biometrics are a method of identifying people and you have one biometric which gives a hit, that may merely raise a question, not be certain, but if you have a second biometric that makes the same hit that must really produce a very considerable degree of certainty?
Dr Hosein: In a democratic state is it necessary for individuals to be known and identified? I would say that that is absolutely correct; I would say not just in a democratic state but in a modern economy personal information and identity information is very much a currency in its own right and can lead to more advanced economies, more advanced markets and so on and so forth. I do not believe there is much doubt over this. I believe that doubt emerges on how this is actually realised, so your argument about biometrics and the various uses of biometrics within, say, the national identity scheme, there is a scientific argument to support what you are saying but that is not the reason why we have fingerprints being proposed for the ID card scheme. There are two reasons why fingerprints are being proposed for the ID card scheme: first, because when they were proposing the ID card scheme the Government was adamant about it being an international obligation, and the international obligation says that fingerprints may be collected. The EU said that two fingerprints should be collected for biometric passports, so that is why we are moving down the route of fingerprints. The other reason why we are moving down the route of fingerprints when it comes to the national identity card scheme is because the police were sold on the idea that one of the benefits of the scheme would be that there are 900,000 fingerprints left at scenes of crime over the years that have not been matched to a criminal, so the police were told if we run this identity card scheme, we will fingerprint the entire population and you can verify those 900,000 fingerprints against the British population of fingerprints once we have the national identity card scheme off the ground. It was not really about the effectiveness of the technology, it was not about the 99 per cent (which is 95 per cent) effectiveness, it was really, first, about a way of getting the bill acceptable through the creation of an international obligation and, second, a way of getting the bill to be acceptable to the police who had previously voiced a number of concerns about identity schemes but were happy with the fact that there was this benefit of the fingerprints left at scenes of crime.

Q49 ***Lord Foulkes of Cumnock:*** Do you accept that no one is obliged to visit the United States, not even Canadian citizens, either to transit or to go to the US for a visit, and therefore every non-US citizen can choose to retain totally their privacy if they wish?
Dr Hosein: Do I accept that you do not have to travel to the United States? No, I do not; this is a line of argument the Government tried to use with the ID cards saying the ID cards are voluntary because you do not need to get a passport, it is not mandatory by law that I get a passport, but it was soon accepted that if you want to be a functioning part of the economy you need to have a passport, you need to travel, so therefore you are going to have to get a ID card with a fingerprint. It is the same idea with the United States; I travel to the United States about 12 times a year, never for a vacation, it is always for work. A lot of people do, the amount of people

travelling between the United Kingdom and the United States is something like 10,000 a day are transferring back and forth between the US and the United Kingdom; are these all just people going on vacation? A large majority of people are business travellers, who really have no choice over this. But even if it was just voluntary, it does not mean that you can voluntarily give up all of your rights just because you want access to a specific environment. The rule of law requires that countries implement a number of safeguards to prevent abuse, and we all accept that that is the way governments operate. That is the way the EU operated when it created the EU directive on data protection, saying you can process information but there are certain safeguards. The US is free to fingerprint foreigners coming in because, look, it is not the say of the UK Government to influence how the US Government fingerprints people, but when we are talking of the transfer of data that originally resides in the United Kingdom or across the EU, that is protected by the laws of this country and the EU, which is then sent in breach of these laws to the US where it is processed in breach of those laws, we are talking of an issue of sovereignty between countries and it is perfectly reasonable for the EU and the United Kingdom to ask that the data that was collected in this country under the laws of this country ought to be protected when it is transferred elsewhere, and the fact that it is not is a serious concern to both sides. I will give you the example of the Swift case. Swift is an international banking co-operative which collects information on our inter-bank transfers and enables inter-bank transfers. It was discovered in June last year that the intelligence agencies in the United States had been getting almost all the data from Swift regarding transfers of money around the world, and it was being handed over to the intelligence agencies for their data mining purposes. This was a shock to the global community; it was a shock that our banking transactions—even inter-bank transfers between, say, France and Germany—are being sent to the US Government for scrutiny. Some would say what is the sovereignty of the US Government to do that, but the EU was saying "Hold on, that is actually illegal, why are you collecting this information?" It was the same with PNR; when PNR was originally being discussed it was about the US Government getting access to the reservation systems to look at all PNR, not just the PNR of people travelling to the United States. That is why I would say that this debate really is about civil liberties generally; it is not about the ability to give up your rights just in order to get access to one specific situation because it is not about you getting access to that specific situation, it is about the mass surveillance of mass activities.

Lord Harrison: My Lord Chairman, given our interest in fingerprinting this morning I feel we should all re-read Mark Twain's *Pudding Head Wilson* which I think was the first ever novel written on fingerprinting, and it might give us some wit and wisdom there.

Chairman: We will read it into the record.

Q50 ***Lord Harrison:*** Two very quick questions, if I may, Dr Hosein. First of all, is data collected on no-shows as opposed to go-shows, because I would have thought that might be quite interesting; secondly, in the negotiations for the new agreement there are likely to be requests for more data to be put to wider use and kept for longer. What do you think are the main dangers against which the negotiators should guard?

Dr Hosein: Passenger name records are collected when somebody decides to book a flight and even if they cancel that flight that PNR is still in the reservations system. If they do not show up at the airport as a no-show, it just gets logged within the no-show, they did not show up, they did not fly. This happens a lot and it happens mostly to business travellers; I have been a no-show on a number of flights around the world, just because you are too late to get to the airport or you decide to take the train instead and so on and so forth. This information is useful, but at the same time why is it that useful to be transferred to the United States on passengers who have not travelled to the United States. The mere fact that they have booked a flight and did not show up, that is not interesting, that is only of interest to the carrier who is possibly losing money or charging somebody for a service that was not given. On the future negotiations, the secretary of the Department of Homeland Security in late August last year wrote an editorial in the *Washington Post*. It was after the arrest of the liquid bomb case in this country and he declared that the intention for Passenger Name Records was for greater access and greater use. The United States Government does not understand why the data can only be retained for three and a half years. They say that as a matter of custom data in the United States Government is kept for at least four years and, as I said, the fingerprint data that is collected is kept for 100 years and the PNR of most other countries is collected for 40 years. Secretary Chertoff's point was that he is going to push for at least eight years retention, so that is what you can expect in the next round of negotiations. What are the dangers? The danger is going to be this confusion over the visa waiver programme; I think the US Government is going to offer to the EU a lot more than it can actually deliver in exchange for the EU agreeing to keep quiet over PNR. Already I had a call from a journalist yesterday who is running a story tomorrow; she said that the mandate given to the negotiators from the EU—which was just handed down a couple of weeks ago—includes demanding reciprocity, not only reciprocity from the US on PNR

information, but also information derived from PNR. This is an interesting situation, because of course the classic example of this is a KLM flight to Mexico—I believe it was last year—was bound to fly over US territory and the Americans had identified a problematic passenger and ordered that plane to turn around and return to Europe, which is entirely within the rights of the Americans to do. That plane landed back in Europe and everybody got off the plane and went their separate ways. The Americans never notified who was on that plane who was problematic, never notified the officials to perhaps stop this person in Europe. I was speaking to one Member of the European Parliament yesterday and she said it was quite shocking. Of course we would love to know if there are suspected terrorists on planes, and if the Americans could share that information with us when that person returns we would investigate the situation. That is one way of looking at the problem. The other way of looking at the problem is that the EU does not collect PNR generally. There is some collection in this country by Customs and Excise, but it does not collect PNR generally. It does not process this data because it is problematic and possibly illegal and the collection of PNR that the Americans want is possibly disproportionate and there is a whole debate about this. What the negotiators have a mandate to do now is say to the Americans yes, you can have our PNR on the condition that whatever you do with it, such as the automated targeting system you apply to it, the data profiling you apply to it, can you send us that data back so we know if it is problematic in the future. In a sense this is the rendition of data, this is like the EU saying we cannot process this information in the EU, we cannot data-mine it, so how about we outsource that to the United States, the United States does all the dirty work for us in a way that we cannot do and they will give us back the data. I worry that these kinds of promises, these kinds of trades, will be part of the next round of negotiations and that is how the Americans might very well get their eight years of retention if not 40 years of retention, the use of data-mining which was not properly enabled within the first agreement and the wide uses of the data.

Chairman: Dr Hosein, you have been extremely helpful and I want to thank you very much indeed for your very full but fluent replies. I am sorry that you found yourself having to speak for two people, but may I congratulate you on the way in which you admirably covered the agenda. Please convey our regrets to Simon Davies and, indeed, if we are at fault in our transport system convey our apologies to him. I am sorry that we were not able to see him, but thank you very much indeed for doing the work of two with admirable care and helpfulness.

Baroness D'Souza: Hear, hear.

Chairman: I wish you all the best; thank you very much.

WEDNESDAY 7 MARCH 2007

Present
Caithness, E
D'Souza, B
Foulkes of Cumnock, L
Harrison, L
Henig, B
Jopling, L
Listowel, E
Marlesford, L
Teverson, L
Wright of Richmond, L (in the chair)

Examination of Witnesses

Witnesses: JOAN RYAN, a Member of the House of Commons, Parliamentary Under-Secretary of State, and MR TOM DODD, Director of Border and Visa Policy, examined.

Chairman: Minister, we would like to ask you a few questions about Passenger Name Record on which, of course, we shall also be taking evidence from Baroness Ashton of Upholland. I believe you have very kindly agreed to answer some Home Office related questions on PNR. I will ask Lord Listowel to open the questioning.

Q51 ***Earl of Listowel:*** Minister, what contribution do you think this PNR Agreement between the European Union and the United States makes to the fight against counter-terrorism and other serious crime? Could you briefly comment on any dangers there may be of antagonising citizens and perhaps losing some hearts and minds in this process? Also, is there enough being done in terms of exchange of personnel between this country and the United States to build, not just using technical means, but human resources effectively?
Joan Ryan: I think it is extremely important that we can exchange this data. We should not underestimate how important it is to the fight against counter-terrorism. The data that we exchange under this Agreement is a most valuable source of data for risk assessment and intelligence purposes. It helps to determine if any passenger or passengers pose a threat to the aircraft or to the other passengers on the aircraft or whether they are believed to be involved with terrorism or with trans-national criminal activity. I think it is very important information for us to be able to exchange; it is very important that that agreement is in place.

Q52 ***Lord Foulkes of Cumnock:*** We are providing the Americans with 34 pieces of information; is there any corresponding legislation for us to be provided with pieces of information on flights into the UK or into Europe? If not, should we have this?
Joan Ryan: We are indeed facilitating effective transmission of PNR data between EU carriers and the US. We do have information that we receive; we are, as you know, pursuing a policy to establish our e-borders and within that we have a pilot called Project Semaphore that operates on certain long haul routes and we receive PNR data through that. We are on the road to developing a full e-borders policy where this kind of PNR data is exactly what we require.

Q53 ***Lord Foulkes of Cumnock:*** Why only certain long haul routes?
Mr Dodd: Semaphore is a pilot which is building up to a full e-borders solution where we aim to collect passenger information on all air routes into the UK. This year we will collect data on about 30 million air movements and, for example, on PNR we are collecting PNR on about 130 routes into the UK, including a number from the USA.

Q54 ***Lord Foulkes of Cumnock:*** When you get that information it goes to the Home Office; does it also go to the Cabinet Office, to agencies that the Cabinet Office has responsibility for, to the DCA or, if your boss has his way, to the new Ministry of Justice?
Joan Ryan: Obviously in terms of that information being useful we need to be able to use that information across our law enforcement agencies, so we need to be able to work together and to share information.

Q55 ***Lord Foulkes of Cumnock:*** You will do that?
Mr Dodd: It does at the moment go into a joint border operation centre in West London where immigration officers, police officers and customs officers sit together to share the information. The information is then routed to particular parts of government that have an interest. For example, if there were a CT interest then that information would go through to the security service.

Q56 ***Lord Marlesford:*** Dr Gus Hosein from the American Civil Liberties Union told us that data mining for profiling has been shown to be largely ineffectual and unproductive. Would you like to comment on that view?
Joan Ryan: I did have a sheet with me about Semaphore which is, as I said, our pilot in developing our full e-borders coverage.

Q57 ***Chairman:*** Could I say at this point that on Project Semaphore or indeed anything else, if you wanted to send us a supplementary note that would be extremely helpful. I see you have now found your piece of paper.
Joan Ryan: I have indeed but I will of course send you any further information. Just in terms of Semaphore—I think you could scale it up and think about the provision of data through PNR with the US—wanted for murder, 7; wanted for burglary, 26; wanted for theft, 61; assault, 71; possession of offensive weapons, 14; wanted for sexual offences, 27. These are arrests and interventions from February 2006 to January 2007 by offence and it continues on: wanted for road traffic offences, 108; wanted for drug related crimes, 36. I hear what you are saying but we have evidence which shows us just how useful this is. This policy is evidence based and I think it is as well to bear that in mind.

Q58 ***Lord Marlesford:*** Could you tell us what is the Commission's position as set out in the Council mandate? Is that mandate going to be made public?
Mr Dodd: The mandate is a confidential document. The Commission is engaged in negotiations with the Presidency and with the USA to achieve a long-lasting PNR agreement which extends beyond the temporary one which expires in the summer.

Q59 ***Lord Foulkes of Cumnock:*** Do we agree that we are going to get a note on Project Semaphore because that would be really helpful.
Joan Ryan: Yes, of course.
Chairman: Minister, can I thank you and your colleagues very much for the very helpful way in which you have answered us. I particularly thank you for agreeing to answer questions on a subject which I know primarily falls to your colleagues in the Department of Constitutional Affairs whom we expect to see in a few minutes' time. Thank you very much indeed.

Supplementary memorandum by Ms Joan Ryan MP, Parliamentary Under-Secretary of State, the Home Office

During my appearance before sub-Committee F (Home Affairs) on 7 March I undertook to write with some additional information on the e-Borders Programme, Project Semaphore and our successful use of passenger data.

e-Borders is a medium to long-term initiative to re-shape the UK's border co-ordinated by the Home Office Immigration and Nationality Directorate (Border and Immigration Agency from April 2007) in partnership with other border agencies (HM Revenue and Customs, the Intelligence Agencies, the Police Service and UKvisas). Other departments and agencies such as the Department of Work and Pensions and the Identity and Passport Service are involved as major potential beneficiaries of the e-Borders data. The programme contract award is scheduled for 2007, with significant operating capability planned for July 2008, and full e-Borders capability in 2014.

Project Semaphore was launched in November 2004 as an operational prototype to trial e-Borders concepts and technology in order to inform and de-risk e-Borders. The pilot has been capturing passenger information on selected routes, and assessing it against watch lists. Based on the assessment, where a passenger is of interest, an alert is usually issued to the relevant partner agency for appropriate action to be taken. The Joint Border Operations Centre (JBOC) is the operational hub of Project Semaphore and manages the data captured and generates alerts to the border security agencies. Significant operational successes have been achieved, including the arrests on arrival or departure of those wanted for serious crimes, such as murder, rape, drug and tobacco smuggling as well as passport offences. To date nearly 900 arrests have been made.

The two key types of data received by project Semaphore are Advanced Passenger Information (API) and Passenger Name Records (PNR). API is usually used to refer to the information contained in a passenger's travel document, including the name, date of birth, gender, nationality and travel document type and number. PNR data is a term specific to the air carrier industry and relates to information held in a carrier's reservation system and consists of a number of elements which may include date and place of ticket issue, method of payment and travel itinerary.

We are currently collecting passenger data from 40 carriers, amounting to 20.9m annualised passenger movements. Project Semaphore currently receives API data on flights from 72 non-UK arrival and departure points. Recent API checks have led to a number of police national computer matches, including the identification of three men wanted for murder during riots in Birmingham last year. They were arrested at

7 March 2007

Heathrow and have since been convicted and sentenced to life imprisonment. These checks have also led to immigration service matches, such as the identification of holders of fraudulently obtained passports who have consequently been refused leave to enter the UK. We are negotiating with carriers to expand our data access in order to achieve the IND Review target of 30 million movements by April 2008.

PNR data is used in Semaphore to identify "associated passengers" on bookings. It is also used to identify passengers who are in-transit through the UK rather than arriving (thus reducing unnecessary alerts). In January 2007 23 successes were recorded by Project Semaphore as a result of automated profiling based on passenger data. For example, HMRC were alerted by PNR data to a passenger whose booking was made the day before travel and paid for in cash, who had an overnight stay in the UK before onward travel to Houston. The check of onboard details by a JBOC analyst showed a change in the routing to depart from Gatwick to Houston, which matched a previous successful HMRC profile. The alert was passed directly to HMRC at Heathrow, where he was intercepted on arrival and four kilos of cocaine was found in his baggage. He was arrested and charged.

I would also like to advise you that a future EU common framework on PNR data is being considered by the European Commission. An informal consultation has been carried out and a draft framework decision may be brought forward later this year. There is no set date. We look forward to this proposal, and hope that it will be as flexible as possible to maximise the benefits of PNR data.

30 March 2007

WEDNESDAY 7 MARCH 2007

Present	Caithness, E	Jopling, L
	D'Souza, B	Listowel, E
	Foulkes of Cumnock, L	Marlesford, L
	Harrison, L	Wright of Richmond, L (in the chair)

Examination of Witness

Witness: Rt Hon Baroness Ashton of Upholland, a Member of the House, Parliamentary Under-Secretary of State, Department for Constitutional Affairs, examined.

Q60 ***Chairman:*** Minister, welcome back to this Committee. It is very good of you to fit in this meeting in your extremely busy diary. I apologise on behalf of some of our colleagues who have had to leave early and will not be here, but we very much look forward to hearing your replies to our questions and indeed anything else you want to say. I should just say for the record that this is on the record, it is being broadcast and a full record is being taken of this meeting. You will of course be sent a transcript in due course. We would like to ask you questions about the Passenger Name Record Agreement. I will start by referring to an e-mail received by the Commission on 11 October 2006 adding "frequent flyer" data as a new data element. Mr Baker of the US Department of Homeland Security says, "With this letter the US has consulted with the European Union". Can you say what opportunity the Council, Commission or Member States had to comment on this proposed addition?

Baroness Ashton of Upholland: Thank you very much for inviting me back; it is always a pleasure to come and see the Committee. There have been a number of meetings at EU level and I believe the e-mail was discussed at several meetings. I cannot say that ministers in Member States have been directly involved, certainly the Presidency would have been and officials would have been. I would just say that one of the important aspects of those discussions has been the reaffirmation of the importance of data protection within all that we do in these negotiations.

Q61 ***Lord Jopling:*** I have your note to Lord Grenfell of 16 February in which you say that "any EU Member State or the Commission or individual airlines can refuse to supply PNR data if they are not confident that appropriate data protection is being provided". How easy do you believe it would be for any of the individual member governments or the Commission or airlines to discover whether data protection was being abused and would it not in practice be extremely difficult to demonstrate it? If there had been transgressions which were denied they would be almost impossible to prove and, even if you could prove it, what do you think would be the consequences of such a refusal on the Agreement if it was in place?

Baroness Ashton of Upholland: First of all I begin with how do you find out that something has happened. First of all, the role of the information commissioner is very important. The individuals who believe that they had their data misused can complain to the information commissioner in this country and indeed in any of the Member States. The information commissioner can go directly to the Department of Homeland Security and of course come to the Department for Constitutional Affairs and ask us to act which we would do in conjunction with the Commission. Because of the Article 29 meetings between all of the other information commissioners this is also an opportunity for information to be received by those commissioners—our concerns, worries, complaints in other Member States—so they could act in concert if they so wished to actually make representations individually or collectively to the Commission or to the Department of Homeland Security. We also have at the present time—this of course will be subject to the new negotiations—an annual review. That review is conducted by the Commission and by experts from different Member States. We have representatives from the Home Office who sit on that group and part of that review is to make sure that everything is working properly. From my perspective there are a number of different ways in which information could come to light. If there was a complaint about the airline, for example, the information commissioner can investigate and act and compensation can be awarded to the individual. If the information commissioner is satisfied that there is a problem then that can be either direct representation through the UK Government or through the Commission to the Department of Homeland Security and we reserve the right to prevent information going to the US if we felt that that was necessary. Having said all that, our challenge and our issue would be being able to get to that point and, if we were concerned, to try to rectify it as quickly as possible. I would envisage that if we

were concerned, if there were complaints, we would want them investigated very quickly but with the clear objective of trying to get those resolved in order to continue the flow of data; disrupting the flow is not what we would want to see happen. While I accept from the Committee's perspective you want to be clear that there are mechanisms in place, I think the way in which this has been set up between the role of the commissioner, the Article 29 group, the Commission, the UK Government and of course the responsibility in the US itself there are clear points at which any concerns could be addressed.

Q62 ***Lord Jopling:*** Would you agree that it is absolutely vital to get all the structures in place to deal with transgression because once somebody starts refusing to provide information that could easily lead to a domino effect which could bring the whole thing clattering down?
Baroness Ashton of Upholland: I am sure that is right, Lord Jopling. One of the key questions for the negotiations will be the relationship between the EU and the US in terms of the contact that they make and the way in which these issues will be dealt with. What I was trying to describe were sensitive mechanisms and how they fit internationally and how they would be triggered. I think all our objectives would be to make sure that the data is transferred properly and effectively. We trust the Americans to do that. They have good legislation in place; the evidence thus far is that they go further than they need to to consider issues of data protection and so on therefore the relationship does work well and I think these negotiations will be very successful.

Q63 ***Lord Marlesford:*** Minister, could I ask you about this data mining or profiling which we know the Americans have been using as a means of targeting people or finding out how they might behave. Dr Gus Hosein from the American Civil Liberties Union expressed great concern about it in terms of its legitimacy or ethical justification and also said that it is quite ineffectual anyway and he quoted various figures to show that. I just wondered whether you think it is a lawful and legitimate use of the data and do you have any comments on whether it is worthwhile anyway?
Baroness Ashton of Upholland: I do think it is important but the critical element of that is that it is only to be used for areas of serious and organised crime, the ability to disrupt serious and organised crime or anti-terrorism. The evidence that I have seen is that the United States have been successful with using the information to disrupt, for example, people trafficking. There have been circumstances where they have been able to develop information that has led to successful arrests of people who are involved in the trafficking of individuals which is a terrible crime as we know. I do not have the details of that but I am very happy to supply them to the Committee. Certainly the main thing to give you comfort is that it can only be used for those circumstances and thus far there are cases that have been successful in ways that we would be keen to applaud in terms of what they have been able to disrupt. They cannot be used generally, only for that.

Q64 ***Chairman:*** Thank you for that offer and I should say that if at any point when you see the transcript you think there are other points that need to be put in writing we would be very happy to receive them.
Baroness Ashton of Upholland: I would be happy to do that.

Q65 ***Earl of Listowel:*** Minister, when a Joint Review of the working of the Agreement was carried out in September 2005, access by the European data protection authorities to files was restricted on security grounds. Do you think the Joint Review procedure is adequate to monitor the working of the Agreement? Will a similar provision be incorporated in the new Agreement?
Baroness Ashton of Upholland: I think the Review is important. As I said previously in response to Lord Jopling, the combination of the Commission and experts is, I believe, the right one. I have indicated that the Home Office supplies expertise to the Commission. Certainly the Review has been important in establishing how well the Americans have treated the data. As I have indicated, they have gone further in terms of data protection than is required which is again, I think, of great significance. I would anticipate that during the next set of negotiations this will be a significant part of ensuring that we keep up to speed with what has happened and reviewing it—I have always believed in reviewing everything—to make sure it works effectively and to take account of current circumstances. Yes, it is an important mechanism; yes, I think it has worked well; yes, I think it should be part of the next stage.

Q66 ***Baroness D'Souza:*** We have talked a bit about remedies at the national level but I wonder if you could say something about what remedies are available to the EU citizen who believes that personal data has been misused or the Undertakings breached? For example, what remedies would be available to an individual if they complain of being on a no-fly list?
Baroness Ashton of Upholland: First of all I think I have indicated that if it is a national question the ICO can require compensation from the airline if the airline were at fault. As an EU citizen they can complain directly to the Customs and Border Organisation that is part of the Department of Homeland Security and ask for that to be reviewed. The Americans have also recently started what is called Travel Redress Inquiry Program (TRIP) which is an on-line system where you can go on-line and ask

for your information to be checked and reviewed because you have been treated badly, you have been delayed on a flight and so on. It is a very open system that anybody can access and say they are concerned about the use of their data and ask for it to be reviewed. That is again helpful rather than having to write in and wonder if your letter has been seen. I also know that they have been looking at the watch list and going through and reviewing name by name who is on that list, which is also very, very important. There is an increasing move of openness to allow citizens of the EU to be able to go directly to the United States authorities if they have concerns, but of course they also have the ability to go to their own information commissioners and their own governments and ask them to pick it up as well. If that happens then the information should be checked and reviewed very quickly and redress will be dealt with as appropriate.

Q67 ***Baroness D'Souza:*** Given that a lot of the information will already have been dispersed to various other organisations in the case of America, as far as you know would there be a guarantee that the remedy or the redress would affect all those other organisations?
Baroness Ashton of Upholland: Data protection rules mean that if the information is incorrect and is corrected you have to correct it everywhere; the information will be sent on. That will be very important because if they have the wrong information it is actually of no value to them so it is very important that they get the right information.

Q68 ***Lord Harrison:*** Minister, could you tell us the Commission's negotiating position, as set out in the Council mandate? Is the mandate going to be made public? I should advise you that another member of this Committee asked that question of Minister Ryan 15 minutes ago.
Baroness Ashton of Upholland: We do not publish negotiating mandates for the reason that if they are in the public domain then everybody else knows what our negotiating position is and I have always learned that in negotiations you keep your cards close to your chest at least to begin with. What I can say is that I have seen the mandate and it is very balanced. I am sure when everything is concluded we will be able to share more detail about that, but for the moment I cannot say what it is because otherwise everybody would know what it is, including those we are negotiating with.

Q69 ***Earl of Caithness:*** Can you reveal a little more from the cards in your hand as to whether the system is going to be a push or a pull system? I understood it was going to be a push system but in the recent papers that I have read it seems that the Americans still have the right to pull whatever information they want, whenever they want and how they want.
Baroness Ashton of Upholland: It is moving essentially and the ambition is to move it to a push and not a pull system. You are right, at the present time it is more pull than push. The ambition will be, by the time we have finished the negotiations, it will be a push system, so push from airlines out, not pull from the Americans in.

Q70 ***Earl of Caithness:*** Push only, no pull at all.
Baroness Ashton of Upholland: That is my understanding, a move to push.

Q71 ***Earl of Listowel:*** You say that in negotiations with the Presidency and the Commission the US is likely to press for material changes to the Agreement and Undertakings, and that the negotiations will be challenging. Should the UK not use its special relationship with the United States to attempt to balance the rights of UK citizens against the use of data to combat terrorism?
Baroness Ashton of Upholland: This is very much part of being in the European Union and the key negotiations when you are operating in this way are between the Commission and the Presidency. Indeed, in our Presidency we undertook and participated with the Commission on behalf of other Member States. It is quite important that we do not get cross wires. It is quite important in my view that negotiations are conducted in that way. The Commission's responsibility is to be mindful, which they are, of the views of all Member States in this and of course we have a part to play in that. There are obviously bilateral negotiations and discussions that go on all the time. The Home Secretary and Secretary Chertoff have met and they have had discussions frequently. There is no doubt that the UK has a role to play in relation to the US but the negotiations are specifically EU and I think that is right and proper.

Q72 ***Chairman:*** Could I just ask about something that has been of interest to this Committee. We talk about the rights of UK citizens and I think it is right to remind ourselves, if you agree, that there are also some benefits to UK citizens in the system, which is that it avoids the need to apply for visas. I know this is primarily a Home Office question but can you tell us, perhaps from your personal view, is it a significant advantage in the PNR Agreement that it removes the need for us all to go to the United States Embassy and apply for visas?
Baroness Ashton of Upholland: I am sure it is an advantage. The big advantage of PNR is that it keeps us safer and that applies to UK and EU citizens and American citizens. The fundamental principle behind what we are doing is trying to identify those who would destroy us or who would create havoc through serious and organised crime. That for me is a much bigger advantage than having to queue for two hours outside the American Embassy.

Q73 ***Lord Foulkes of Cumnock:*** We have heard from Joan Ryan that there is a pilot scheme, Project Semaphore, in relation to PNR information being provided to the British Government on flights into the United Kingdom. Why is it not part of this Agreement? Why is there not a reciprocal agreement?
Baroness Ashton of Upholland: I do not have the detail of that because that is very much to do with the Home Office but a lot of the way of looking at what we are doing on PNR is that we always looking to see other areas that we might cover and other ways of approaching how we share information. You will know from the Prüm Treaty that there are a lot of incidents where we take particular aspects of what we are doing, pilot them, have a look at how they work and then if they seem to be effective they might well be part of future negotiations. As I understand it we are still at the very early stages of that, so the prime negotiation on PNR is to renew the agreement that we already have with the safeguards that we already have.

Q74 ***Lord Foulkes of Cumnock:*** Some of the criticism we have had is that it is a one way agreement and would it not be better for it to be reciprocal and for us to make it more widely known that we are trying to move in that direction?
Baroness Ashton of Upholland: We have to consider what the advantages are of the reciprocity. I have not seen anything that demonstrates the benefits there would be to us. There may well be some and I think what this pilot project may look at is precisely what advantages there would be to us. One of the problems about data sharing that I encounter domestically and nationally is that you have to be able to use the amount of data that you get effectively. You can end up with huge amounts of data that you simply cannot use properly and therefore you miss the thing you are looking for. The way that we would want to look at this is what advantages would there be, what are the threats we are trying to address, where do we want to have the data from and what would we use it for and who would need to know. It is not that it is a one way system because we have not bothered to look at it; the question is what advantage would it be to us in terms of our own security.

Q75 ***Chairman:*** Do you happen to know whether those people who still have to apply for visas to go to the United States, are they now required to answer 34 questions on their visa application forms?
Baroness Ashton of Upholland: Do you mean 34 questions because there are 34 fields? There are 34 possible fields but I do not think there is anyone who actually fills them all. People might answer four or five. I have not obviously filled in a visa form but as far as I know there are 34 possible things that you might supply but an individual would probably supply four or five.

Q76 ***Baroness D'Souza:*** It is likely that during the course of these negotiations that the US will ask for more data elements to be included in the PNR? Could you say something about what you think the dangers might be in those extra elements apart from overkill in terms of information? In a sense what I am really saying is where do you think you might draw the line in terms of reciprocity et cetera?
Baroness Ashton of Upholland: There is a balancing act to be done here. It is not about danger to me, it is more a question of balance (which I think is a Moody Blues album from my youth!) between being absolutely clear why this information is necessary. You can get a lot of information you simply cannot use and the question is to determine which information could be valuable, particularly if you are trying to profile or work out from patterns of behaviour what may or may not happen. We will need to balance requests and consider them carefully in any EU negotiations between that need for information and our need to look at fundamental rights that people have, data protection and privacy. All of those things come into play. What I believe the negotiations will do and the EU will be very keen to make sure is that we have that balance right. It does not mean that we cut off information at this point; it says that when you look at all the information that is required, can we justify that information and have we taken into account our need to make sure that data protection is in play, privacy is in play in the US and also that we have thought about people's rights.

Q77 ***Earl of Caithness:*** Minister, you say in your letter of 16 February that the data transferred under the current Agreement "will continue to attract a data retention period of thrde and a half years". Conversely Mr Baker from America points out that the Agreement will expire before the end of three and a half years and the questions of when to destroy data collected in accordance with the Undertakings "will be addressed as part of future discussions". Clearly those statements are not together; which is correct?
Baroness Ashton of Upholland: The correct one is three and a half years; that remains.

Q78 ***Earl of Caithness:*** Mr Baker is wrong.
Baroness Ashton of Upholland: I would hesitate to say that Mr Baker is wrong; I would simply say that I checked and the current position is three and a half years. When I read those words I am not entirely certain that we were referring to quite the same things but for your purposes three and a half years is the correct position.

Q79 ***Lord Foulkes of Cumnock:*** Now I am confused. We were told that the Americans retain the data for 40 years. I am not sure how that relates to the three and a half.
Baroness Ashton of Upholland: The Agreement is three and a half years.

Q80 ***Lord Foulkes of Cumnock:*** In the new Agreement are we seeking to change that?
Baroness Ashton of Upholland: At the moment the position is three and a half years. If the Americans, as part of the negotiations, wish to argue that data should be retained for a longer time then they will have to make that case and that case will then become part of the balancing between the importance of keeping data for the right length of time based on experience and knowledge that they will acquire and we will all have as Member States of the value of information and how far back, versus the accumulation of data you simply cannot use because you have too much, versus what seems an appropriate length of time. That will be part of the negotiation.

Q81 ***Lord Foulkes of Cumnock:*** Is the EU seeking for that to be reduced?
Baroness Ashton of Upholland: The EU is saying that we go in with three and half years and should the Americans say they would like to retain the data for longer then they must make the case, that will be part of the negotiation.

Q82 ***Lord Foulkes of Cumnock:*** Once the negotiators are concluded, are the European Parliament and this Parliament going to be able to comment before it is signed or will we be commenting after the signatures?
Baroness Ashton of Upholland: It is a bilateral agreement so the rules, as I understand it, are that the governments sign. We will want to keep you informed and will do so about what is happening and I undertake to do that, to have our usual correspondence on it. It is a Pillar Three measure, that is why we have to do it again from the European Court's ruling last May, therefore the parliaments have only limited roles under the Third Pillar. I am quite sure the European Parliament will wish to debate this at length and will no doubt give us its views, but it is not part of the decision making process in that sense.

Q83 ***Lord Foulkes of Cumnock:*** Could I ask another question as a new member of this Sub-Committee (everyone else here probably knows the answer)? We are talking about machinery of government beyond this Committee in relation to the Home Office and the DCA, why is this currently a DCA responsibility?
Baroness Ashton of Upholland: Because this is about data protection and data sharing and that is my responsibility within DCA, but I am also the minister who sits on the European Council of Justice and Home Affairs Ministers on behalf of the Lord Chancellor.

Q84 ***Chairman:*** Minister, that is very helpful. Before we conclude this session is there anything else you want to say?
Baroness Ashton of Upholland: No, only perhaps to reaffirm that we will keep you in touch with what happens and obviously I would be delighted to come back and talk further once the negotiations have been completed if there is anything further that you want to discuss.
Chairman: Thank you very much indeed.

Supplementary memorandum by Baroness Ashton of Upholland, Parliamentary Under-Secretary of State, Department for Constitutional Affairs

When I gave evidence to your Committee about the EU-US PNR agreement on 7 March, I referred to the benefits of PNR profiling with regard to identifying and disrupting human trafficking activity. I offered to provide the Committee with further details of how data profiling can be used in this way and I am pleased to provide a detailed example below.

The US Immigration and Customs Enforcement Field Intelligence Unit (ICE FIU) used PNR profiling to uncover a human smuggling operation during the spring and summer of 2004. This work resulted in the arrests of seven smugglers and one previously deported adult, 10 expedited removals, and the disruption of an organization responsible for successfully smuggling 37 individuals.

On 13 March 2004, CG was arrested at Newark International Airport for attempted human smuggling. She was escorting a Dominican national who had been supplied with her own son's valid Puerto Rican birth certificate as his travel document. CG admitted this was not the first time she had smuggled people in this way and an analyst from the North East Field Intelligence Unit (NE FIU) began researching her previous travel.

PNR information from CGs two known arrivals in the US revealed that in each case she had traveled alone on the outbound section of her trip from the US to the Dominican Republic, but returned on the inbound portion of her reservation accompanied by travellers passed off as her children. These children had been supplied with round trip tickets indicating they were returning to their point of departure, but the outbound segments of their reservations had never been used. The NE FIU analyst identified three associates of CG who had each traveled several times with her from the US to the Dominican Republic. Their PNR data revealed the same pattern: all three returned to the US with travellers identified as their children, but these children had not travelled outbound from the US before "returning". When the Advanced Passenger Information System

7 March 2007

reported that the three associates were scheduled to return to the US on separate flights within 48 hours, the NE FIU analyst ensured the travellers were intercepted.

MP was arrested on 29 April 2004 at Miami International Airport for attempting to smuggle three Dominican children. All three had been supplied with valid Puerto Rican birth certificates and MP posed as their mother. MP was indicted on human smuggling charges and is currently awaiting sentencing. On 30 April 2004 MT was also arrested at Miami International Airport after attempting to smuggle another three Dominican children. Once again, the children were in possession of valid Puerto Rican birth certificates. MT was indicted on human smuggling charges and has since been sentenced to five years in prison. After MP and MT were arrested, CGs third associate changed her flight reservation. She had also been scheduled to fly into Miami International Airport with three children who had not been with her on her outbound flight. Instead, she arrived at San Juan International Airport alone, but had three extra suitcases after a one-week trip, indicating a probable last minute change of plans.

The NE FIU analyst described the smuggling operation in an Intelligence Alert, identifying the steps that Customs and Border Protection (CBP) officers could take to reveal similar human smuggling activity. CBP officers in San Juan later informed the analyst that the information in the Intelligence Alert was responsible for the discovery of three more smugglers, again using PNR information. QC was arrested at San Juan International Airport on 24 May 2004 while attempting to smuggle a Dominican child with a valid Puerto Rican birth certificate. QC was indicted on human smuggling charges. YS was arrested at the same airport on 13 June 2004, attempting to smuggle two Dominicans with Puerto Rican birth certificates and was also indicted on smuggling charges. One of the Dominican nationals was in fact not a minor, but a previously deported adult; he too was arrested. On 16 July 2004, MC was arrested at San Juan International Airport while attempting to smuggle a Dominican child, once again supplied with a Puerto Rican birth certificate. MC was indicted on human smuggling charges.

In addition to illustrating the benefits of PNR profiling, the human smuggling cases also highlight the value to the US of being able to share PNR between different agencies with law enforcement and counterterrorism missions. If the smuggling ring had operated out of the EU, the US would not have been able to identify its ring members via PNR profiling: in 2004, the US interpretation of the Undertakings annexed to the Agreement was such that Immigration and Customs Enforcement could not obtain PNR data unless it was in relation to a specific case.

You may also be interested to know the details of a drug smuggling operation, also exposed via PNR profiling. In January 2003, CBP in Miami used PNR data to disrupt an internal conspiracy within an airline in which an employee was smuggling cocaine between Venezuela and Miami. A corrupt ticket counter agent would identify low risk travellers (typically families) and add an additional bag, filled with cocaine, to their reservation details after they departed the ticket counter. Corrupt airline employees in Miami were primed to remove the extra bags prior to inspection by CBP in Miami. By noting the change in bags during connecting flights, CBP was able to identify those passengers whose reservations were being abused and so identify the corrupt ticket agent.

I hope this letter provides you with the information you were seeking and reassures you of the benefits of PNR profiling. As ever, I am very happy to discuss any aspect of this matter further.

3 May 2007

WEDNESDAY 21 MARCH 2007

Present	Bonham-Carter of Yarnbury, B	Jopling, L
	D'Souza, B	Listowel, E of
	Foulkes of Cumnock, L	Marlesford, L
	Harrison, L	Teverson, L
	Henig, B	Wright of Richmond, L (Chairman)

Memorandum by Professor Elspeth Guild, Radboud University, Nijmegen, Senior Research Fellow, Centre for European Policy Studies (CEPS)

Introduction

1. The collection, retention, manipulation, exchange and correction of personal data in Europe has once again become a matter of substantial interest. The last time data use constituted an important political issue in Europe, in the 1970s, the result (at the European level) was the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data opened for signature in 1981. This Convention, to which all EU Member States are parties, still sets the standard for data use in Europe.

2. The EU adopted Directive 95/46 on data protection, based largely on the Council of Europe's standard, which had to be transposed by the Member States by 25 October 1998.[1] The Commission prepared a first report on its transposition in 2003. The European Data Protection Supervisor was created in 2001 to provide an independent body to ensure that the fundamental rights and freedoms of individuals—in particular their privacy—are respected when the EC institutions and bodies process personal data or develop new policies.

3. Since the attacks in the USA of 11 September 2001, data use has once again moved up the political agenda. The combination of very substantial technological advances in the collection, retention, use and storage of data and the enhanced concerns about security provided a new environment for data issues. One of the outcomes of the new environment was the decision by the US authorities to collect and retain data on individuals coming to the US by air a measure intended to increase US security.[2] This US legal act, however, had consequences for data protection in the EU. In order to provide a common basis for the transmission of personal data by EU transport companies to the US authorities, an agreement was entered into between the EU and US on 28 May 2004 regulating the field. The agreement was attacked before the European Court of Justice by the European Parliament on a number of grounds, not least the inadequacy of protection of individual data. On 30 May 2006, the European Court of Justice found that the agreement had been adopted on the wrong legal basis and gave the parties until 30 September 2006 to adopt a new agreement on the correct basis.[3]

4. On 6 October 2006 the Council adopted a decision to enter into a new agreement with the USA regulating PNR and the new EU US agreement was published on 11 October 2006 (though subject to language checks).[4] In this note I will address some of the issues which arise as a result of the new agreement, in particular, as regards difference between the first agreement and the new one which affect the protection of data.

The Key Issues Regarding the New Agreement

5. The EU and US took the opportunity of the necessity to adopt a new agreement to include a number of changes to it, notwithstanding the fact that the agreement is a temporary one and new negotiations are to commence to replace it. For the EU, the original PNR provision consists of three main documents—the Council Decision approving signature, the agreement and the Undertakings of the Department of Home Land Security of 11 May 2004. The new provision includes the Council Decision, which is now substantially developed, the Agreement which remains substantially the same (though there are some changes of

[1] It has now been augmented by Directive 2002/58.

[2] The US Aviation and Transportation Security Act 2001.

[3] For a detailed discussion of the issues of the PNR decision see E Guild and E Brouwer, The Political Life of Data: The ECJ Decision on the PNR agreement between the EU and the US CEPS, Brussels, 2006.

[4] Council Document 13216/06.

significance) and a letter of interpretation dated 11 October 2006 from the US Department of Homeland Security which effectively unilaterally amends the Undertakings in so far as the letter states how the US authorities interpret the provision of the Undertaking and states certain changes to the Undertakings. Twelve issues were identified as key regarding the new agreement and its interpretation.[5]

6. *Push-Pull:* under the first agreement, the US authorities (in the form of the Homeland Security Department) had the power to enter the data bases of carriers and to pull out information (limited to the 34 specified items in the Undertaking) which it wanted. The reason for this was that European carriers did not have in place the technology to deal with the preferable (from the perspective of data protection) system of push—where the US authorities would have to make a request and the carriers would provide the specified information. It was agreed in 2004 that the system would move to a push one as soon as the technology was in place. According to the EU's Working Party on Protection of Individuals regarding the Processing of Personal Data, report dated 14 June 2006, all the technical requirements are in place for a push system to be implemented. Nonetheless, the new agreement states that US authorities should be allowed to access data directly.

7. *Time Limits and Frequency:* under the 2004 agreement the US authorities had only 72 hours before a flight to seek data and a limit on the number of times it can check data. Under the new agreement the 72 hour limit is no longer final and there is no limit on the number of times the US authorities can check the data.

8. *Purpose Limitation:* the purposes for which data could be use were already fairly wide in the first agreement, including of course preventing and combating terrorism, related crimes, serious crimes that are transnational in nature, flights from warrants or custody for the designated crimes. In the second agreement as augmented by the letter of understanding, the data may be used also in the context of infectious disease for the protection of vital interests which itself is subject to a wide scope.

9. *Sharing data:* the new agreement and its various associated documents widen substantially the number of agencies with which the US authorities may share data. It is not entirely clear whether the EU authorities have a clear description of the agencies which may be provided with data on EU citizens.

10. *Number and nature of the data:* the letter of understanding states that the US authorities must have the option to seek additional data, particularly if the system moves to a push rather than pull format (this of course raises questions as to whether the US authorities have been strictly complying with the limit on the data they are permitted to obtain under the pull system). The Working Party on Protection of Individuals with regarding to the Processing of Personal Data in its report of 14 June 2006 specified that only 19 data items were, it its opinion appropriate for sharing (and the list of 19 differs not only in number but in elements from the list of 34 under the current agreement).

11. *Data Retention:* Under the initial agreement data had to be destroyed after 3.5 years (at least in principle). In the new agreement's letter of understanding, the US authorities indicate that as no data will actually have had to be destroyed before the end of the current agreement "questions of whether and when to destroy PNR data collected in accordance with the Undertakings will be addressed by the United States and the European Union as part of future discussions".

12. *Evaluation:* A joint evaluation took place in May 2004. The report of this evaluation is not public, though it would be very helpful if it were released as no doubt it would reassure EU citizens as to the propriety of data use by the US authorities. In the new agreement doubt is cast over whether there will ever be another joint evaluation.

13. *Data Protection:* the Council in its Decision deems the US authorities to be satisfactory for EU data protection purposes. This raises questions about whether this is in fact the case.

14. *Legal status:* it is very unclear what the legal status of the letter of understanding is. It appears not only to interpret the agreement and the Undertakings but to amend and change them as well as to point to changes the US authorities will seek in the future.

15. *Democratic and Parliamentary Scrutiny:* this is a very intra EU issue, the result of the European Court of Justice Decision. The new legal base for the agreement does not provide a role of the European Parliament. As preparations are already taking place towards the negotiation of yet another agreement to replace the current one, the European Parliament is much concerned about how its views will be taken into account.

16. *Implications for transfer of other data:* there are concerns about the consequences of the PNR agreement for other data transfer agreements.

[5] Letter 10 October 2006 Sophie in't Veld, MEP, rapporteur for the EU-US agreement on PNR to Commissioner Frattini.

21 March 2007

17. This provides an impressive list of concerns which have been raised by the European Parliament's Rapporteur, however, it does not cover all of the issues which the new agreement raises, in particular, redress and protection of the individual.

Protecting the Individual

18. As a result of the transfer of faulty data from the Canadian authorities to their US, counterparts Mr Arar, a dual Canadian/Syrian citizen was stopped when in transit in New York on his way to Canada on suspicion of terrorist involvement in September 2002. He was sent to Syria where he was detained and tortured for over a year. When he finally returned to Canada in October 2003 a Federal Inquiry led by a retired Supreme Court judge was established to determine how this had happened. The Inquiry published its findings in September 2006 which exonerated Mr Arar of any suspicion of involvement with terrorist activities and found serious flaws in the manner by which data had been transferred by Canadian services to their US counterparts on the basis of which Mr Arar was suspected by the US authorities of involvement with terrorism. On 26 January 2007 the Canadian Prime Minister issued a formal apology to Mr Arar and offered him compensation in the amount of CAN$10.5 million.

19. Inaccurate data transmission can have horrifying consequences for the individual, as in the case of Mr Arar. It can also be very expensive for governments.

20. The new EU—US PNR Agreement contains an innovation over its predecessor in that it states "this Agreement does not create or confer any right of benefit on any other person or entity, private or public". Is this to be understood as seeking to deprive someone like Mr Arar from obtaining redress in the event that his data are improperly transmitted and used? If so this is a very unfortunate attempt by the parties to deny responsibility for their acts.

21. The new Council Decision approving the Agreement also contains a new article 4 which states that Member States may exercise their existing powers to suspend data flows to the US authorities in order to protect individuals with regard to the processing of their personal data in two cases:

- Where a competent US authority has determined that the Department of Homeland Security is in breach of the applicable standards of protection; or
- Where there is a substantial likelihood that the applicable standards of protection are being infringed, there are reasonable grounds for believing that the DHS is not taking or will not take adequate and timely steps to settle the case at issue, the continuing transfer would create an imminent risk to grave harm to data subjects, and the competent authorities in the Member States have made reasonable efforts in the circumstances to provide DHS with notice and an opportunity to respond.

22. The first part of this article moves responsibility for determining data breaches on the US authorities in accordance with their laws. As the person who will be affected is the EU citizen, this may not be entirely satisfactory. As was the case for Mr Arar, the US authorities have refused even to entertain the request by the Canadian authorities for information regarding his treatment, let alone participate in determining the truth or compensating Mr Arar for the damage which their action caused him.

23. The second part of the provision moves responsibility for protection of citizens of the Union to their national governments. In terms of EU solidarity, this is very unfortunate as it clearly and unambiguously breaks the common responsibility of the Member States to protect their citizens. Further, it places the bar exceeding high in respect of a decision to cease to participate in the data provision system. Further, it permits one Member State to determine that the US authorities are not applying a standard of protection which is required but it does not provide for any solidarity from the other Member States. If this is a common agreement, then the commitments must be common as well.

24. If the citizen of one Member State is at risk of treatment like that which the US authorities meted to Mr Arar, all Member States should be engaged in the protection of that citizen and act in solidarity to protect all citizens of the Union against harmful use of personal data.

20 February 2007

21 March 2007

Examination of Witnesses

Witnesses: Professor Elspeth Guild, Centre for European Policy Studies (CEPS) and Mr Tony Bunyan, Director, Statewatch, examined.

Q84 ***Chairman:*** Professor Guild, Mr Bunyan, thank you very much for coming. It is very nice to welcome you back to this Committee. As you know, this session falls into two parts: we want to question you first on the Passenger Name Record Agreement and then move on to the Prüm Treaty. I believe you have both indicated, very kindly, that you are prepared to answer questions on both but it is entirely up to you to decide which, or both, of you will answer the questions. The meeting is on the record—you are very familiar with our procedures—it is being broadcast and a note is being taken. You will, of course, both be sent a transcript in due course to check that you are correctly quoted. Although you are both very familiar with this Committee and we are delighted to welcome you both back, some Members of this Committee have not met you before, so I wonder whether I could ask you both, perhaps Professor Guild first and then Mr Bunyan, to introduce yourselves and tell us who you are. I know it is a rather complicated story in your case!
Professor Guild: Thank you very much, my Lord Chairman. It is a pleasure to be here and I congratulate you on two excellent and very timely reports. My name is Elspeth Guild, I am a Professor of European Migration law at the Radboud University in Nijmegen in the Netherlands. I am also a solicitor in private practice in London at Kingsley Napley and I am also a senior research fellow at the Centre for European Policy Studies in Brussels. So I have three hats for the evidence which I have sent you here. It is primarily with the policy hat on that I will speak.

Q85 ***Chairman:*** Thank you very much. Mr Bunyan, can I ask you not only to introduce yourself but also Statewatch.
Mr Bunyan: I am Tony Bunyan, I am a Director of Statewatch, which was started in 1991 to look at civil liberties in the European Union, which meant that our work increasingly became concerned with the European Union. So, as a journalist, which I am, I found myself in the early days going to justice and home affairs councils and getting hold of documents, by the backdoor very often, and coming back to the Chair of this Committee, Lord Tordoff, and others, saying: "Look, we need to get this information out into this Committee". So it has been a long relationship and I have spent a long time travelling round Europe speaking at meetings.

Q86 ***Lord Foulkes of Cumnock:*** My Lord Chairman, *apropos* that, is Statewatch a membership organisation? Who do you represent?
Mr Bunyan: No. We are a research organisation. We are a registered charity and we are a research institute.

Q87 ***Lord Foulkes of Cumnock:*** Who are you speaking on behalf of?
Mr Bunyan: Our job is to conduct research, publish documentation and provide analysis, but we are not a campaigning group.

Q88 ***Lord Foulkes of Cumnock:*** Who are you funded by?
Mr Bunyan: Rowntree.

Q89 ***Chairman:*** Thank you both very much indeed. We are starting with PNR. Perhaps I could ask the first question. What is your assessment, both of you, of the necessity, effectiveness and proportionality of the transfer of PNR data under the current Agreement with the United States? Does it, in your view, get the right balance between the rights of travellers and the use of data to combat terrorism? Perhaps you might add a word about the agreement with Canada, although that is not, of course, the subject of our inquiry. Who would like to start?
Mr Bunyan: I think we should deal with Canada. The Article 29 Working Party has looked at the initial agreement in the European Union, that is the committee of all the data protection authorities from the Member States, and it looked at the practice and, partly because of the number of datasets that Canada was asking for but, also, because of the protection given to EU citizens in terms of their rights, declared it was happy with the agreement with Canada, unlike its view over the agreement with the United States. On necessity, effectiveness and proportionality, I dug out some evidence from the United States which is, in a sense, general evidence, but it makes one wonder. The Acting Director of the US Visit Programme, which of course records all visitors going in (and, theoretically, going out), said that they had, so far, processed 63 million entries and they denied entry to 1,200 "criminals and immigration violators". It seems quite a small number. We do not know the breakdown of criminals and immigration violation, but out of 63 million this seems small. Another concern over it is the report of the Government Accountability Office which looked into how this Passenger Name Record data was being used. In other words, could it lead to errors? They said that whereas the complaints and the numbers going to them (this is the central co-ordinating organisation of the United States) were under control and quite small—in fact, they only had 112 complaints—on the

frontline checking and the use of PNR, which is done by the airlines themselves, in terms of complaints, there were thousands, they report, and they say that half of the tens of thousands of potential matches sent to them over December 2005–06 were mis-identifications. I think what this points out is that it is not just a question of data which is being gathered and used, but how is it being used? Is it really useful? Is it proportional to the threat that we are told exists?

Q90 ***Chairman:*** Were the complaints about the information that had been sent, or were they complaints about misidentification?
Mr Bunyan: It was misidentification in some cases. In some cases it would be refusal to travel. In other words, you might get a mis-identification—i.e. you are not the person you say you are, or they think you are another person because of the similarity of name, which is the most usual. We had a case recently where somebody from Belfast was flying to a European Union country and was refused permission to board by the airline. They would not tell him why but the next day he booked with another airline without any problem at all. So that there is a problem of what identification happens, if you like, which is going to increasingly happen, by the airlines themselves, because that is where the first line checks will take place.

Q91 ***Chairman:*** Do we have any evidence that the 1,200 that you referred to—have I got it right?
Mr Bunyan: Twelve hundred out of 63 million.

Q92 ***Chairman:*** Do we have any evidence to, as it were, sub-divide the 1,200 into misidentification or—
Mr Bunyan: These are the numbers actually denied entry. We do not know. This is the Acting Director of the US Visit Programme in September of last year, in a speech in Brussels.

Q93 ***Chairman:*** That figure is not broken up into misidentification or otherwise?
Mr Bunyan: It is not, unfortunately, no.
Professor Guild: I find everything that Tony Bunyan has said very important and very interesting. I would only add that it would be much easier to make an assessment of necessity, effectiveness and proportionality if one had access to the report of the joint review. Without information about how the PNR is actually taking place it is extremely difficult to assess necessity, effectiveness and proportionality. We have claims on one side, but we have no mechanism to assess; we have nothing against which to judge necessity effectiveness and proportionality.

Q94 ***Chairman:*** Just for the record, could you tell us what the joint review is?
Professor Guild: The joint review was a review under the initial agreement between the EU and the US to examine the application of the Agreement in the US, and it was undertaken in September 2005. The European Data Protection Officer was not included in the review and its report was not made public. There have been rumours about what may have come out and what may be in the joint review, but there is no official information.

Q95 ***Chairman:*** I am sorry, I interrupted you. Do carry on, please.
Professor Guild: I would only add that I think at the heart of the question is a matter which Professor de Hert has raised in his written evidence to you, which is the use of commercial data for law enforcement purposes. You have a mixing of data which is collected for commercial purposes, which is then sought to be used for quite different law enforcement purposes. The quality of data which is collected for commercial purposes, the standards which are applied, are very different from those which are required for law enforcement, in particular, where law enforcement is tied into the whole criminal justice system, and what you are seeking is information which will lead to criminal prosecution, we would hope, if there is a genuine threat.
Chairman: Thank you very much.

Q96 ***Earl of Listowel:*** The current Agreement with Canada has 25 data elements. In these negotiations there are likely to be requests from the US for more than the current 34 data elements to be made available. What, in your view, are the main dangers inherent in the collection of more information?
Mr Bunyan: I did compare the PNR data required by both, and so I marked the ones that the US is asking for which Canada is not asking for. They are: the address of the person, the code-shared PNR information, travel status, the email address and then, of course, the worrying categories, like number 19, "General Remarks". What does that mean? Then I had to look up some others because it says: "Received information"; "Historical changes"; "Number of travellers". Then, 26 is OSI information, and this is also "General Remarks", whereas SSI/SSR information are open fields. The one that almost floored me was the last one, which is "ATFQ fields", and I thought: "What is 'ATFQ fields'"? I used Google, of course, and "ATFQ fields" means "Answer the Freaking Question". So they are the categories which are not in the Canadian one. Clearly, the worrying side for me, from a data protection point of view, is these "general remarks" and "open fields". The concern here, of course, is that what is happening is that they want to create these fields in order that when that template comes into their systems they can add data within those fields. It

is not that those fields will necessarily be filled in by the airlines—they may be, they may have a personal point of view of an individual—but they can be filled in later. Earlier on, one looked back in the process, and somebody I know from Spain applied for his data records, and in fact at that time it was even longer; there were 43 categories being asked for—just to travel within Europe. I have to say, I think there is a worrying aspect here. I do not know, because I was looking at the Home Office Border Programme, what PNR data the UK Government is using because they are using PNR data as well as API data. API data is the international standard agreed by the ICAO, which we can call the basic standard, and that is simply that the data in the machine-readable zone on the bottom of your passport page must be transmitted. So we have got standards which are ICAO standards of API, and then we have got the Canadian standard 25, the US standard 34, and I do not really know how many datasets the UK is collecting. It is a question that you might ask, because it certainly is a concern that even when you try and book a ticket to travel within the United Kingdom with British Airways online you cannot book a ticket online for British Airways unless you agree for your data to be passed to the United States. That is for internal flights within the United Kingdom. I do find that extremely strange.

Q97 ***Chairman:*** Professor Guild, do you want to add to that?
Professor Guild: I would just add that a further concern is that the larger the number of data elements which are included the greater the risk of inaccuracy. We have a PhD student at my university who has examined the reports of the Data Protection Supervisors in three different Member States on data held in the Schengen system (of course, it is different to this one but comparable) and according to the Data Protection Supervisors in some of the *Länder* in Germany, in France and in the Netherlands, in up to 40 per cent of random cases examined, the quality of data in the Schengen Information System, which is data collected for law enforcement purposes, was either inaccurate or improperly used.
Chairman: I find that rather surprising because, surely, in logic, the more information you have the more likely it is to be a correct identification.

Q98 ***Baroness D'Souza:*** Because you can cross-check all the time.
Professor Guild: There is another problem on that. The more data you have, if it is very, very carefully controlled and produced for law enforcement purposes, it may well assist in identification, but the difficulty is that this is data which is collected for commercial purposes and the accuracy level diminishes. So comparing three commons fields—you may get the surname right, you may get the gender right, you may get the middle name right, but then mistakes may start to creep in: e.g. address—the person has moved; credit card—the credit card has changed; e-mail address, telephone number—a digit is wrong. The more information you collect the greater the risk of error occurring. It happens very easily. Anyone who books an airline ticket online will know how easy it is to get the gender wrong. You have to book as Mr or Mrs or Miss; it is very easy to click the wrong box. Do you travel or do you not travel? By and large you do travel. Nonetheless, you have gone into the PNR system with the wrong gender, and that is with only a small number of boxes, which are elements of information which one would have thought would be very straightforward to collect.
Chairman: Lord Foulkes, apologies, I think I have shot your fox, but just before you follow up on this, Lord Harrison.

Q99 ***Lord Harrison:*** I did want to go back to Mr Bunyan because I think you compared, first of all, the 34 and the 25 of the US and the Canadian data, respectively, and you then mentioned 43 items from the Spanish colleague for the EU. I know this is a difference of apples and pears but in those 43 were there other interesting categories that began to emerge that the Committee might be interested in?
Mr Bunyan: Not really additional ones. There were the same problems of the general remarks and open fields. To add to what Elspeth has said, I think there is a distinction. When one uses the term "information" (this will crop up under Prüm as well) one really has to distinguish between hard factual information, and even then there can be mistakes, and what is called intelligence, which may be hard and may be pure supposition, maybe reliable, maybe unreliable. I think the term "data" on its own, or "information" on its own is not sufficient to tackle problems in this field and, indeed, the field we are going to discuss later.

Q100 ***Lord Jopling:*** Surely, it cannot be a surprise to anybody that mistakes occur with all these millions of tickets being sold. What do you say when somebody says to you: "Well, so what? Mistakes are made and inconvenience is occasionally caused out of all those millions, but, surely, that is a very small price to pay for the overall benefit given the terrorist threat that faces us"? Listening to what have said so far, if somebody said to you: "Well, all right, we hear what you say but you are scratching around on the periphery of all this", what would you say to that? I know I am being aggressive.
Mr Bunyan: It is a question one is often asked, and if the purpose of PNR is to tackle terrorism, fine, but it is wider than that. It is wider in terms of organised

crime, money laundering and, in some cases, other crime. What we have got to do (and this, again, goes into the second subject as well) is be much more targeted. If it is just to do with terrorism then the numbers would be much smaller on the watch lists than they are. In the United States the watch list is 132,000; we do not know how big our UK watch list is but we know what theirs is, and that I can understand. However, when you start to say: "While we are collecting information to stop terrorists coming we are going to stop criminals (undefined) and illegal immigration people (undefined)"– it may be a minor offence or a major offence, we do not know—

Q101 ***Lord Jopling:*** Why not?
Mr Bunyan: I suppose you might want to live in a different kind of society where everybody is checked for everything. I think in a democracy one has got to actually say that if the intention is to tackle terrorism let us have measures to deal with terrorism, and let us have guidelines and accountability in relation to that. If we want to extend it into crime, let us have that discussion.
Lord Harrison: Is there not overlap? My instinct is that if you were to look into this—and I understand from what you are saying that we have not got the kind of breakdown which would be very useful to us—I guess in that penumbra of those who fall into the category of criminal activity, they may well draw from that number, on occasions, potential terrorists.
Lord Teverson: Terrorists are probably the most law-abiding people in society!

Q102 ***Lord Marlesford:*** I want to go back to Professor Guild's 40 per cent. What did that 40 per cent figure refer to? You may have told us and I missed it.
Professor Guild: There are two categories. These are from the reports of the Data Protection Supervisors in three EU Member States on random checks which they have carried out regarding information in national Schengen Information System files. In their reports, over the last three years, they have been reporting that of the controls which they have carried out on information which they have checked there have been factual errors, incorrect storage or storage of data which should have been deleted in up to 40 per cent of the cases which came before them.

Q103 ***Lord Marlesford:*** That 40 per cent figure does not mean very much unless you split it up.
Professor Guild: The vast majority of the problems were inaccuracies in the data.

Q104 ***Lord Marlesford:*** What you are saying is that the vast majority of the 40 per cent had an inaccuracy, or one or more inaccuracies in the data?
Professor Guild: That is my understanding. I have not read the reports myself.

Q105 ***Lord Marlesford:*** Out of 36 questions (whatever it is) there might have been one inaccurate one in 40 per cent of the cases.
Professor Guild: That could certainly have been the case, but it could also have been more.

Q106 ***Lord Marlesford:*** Or more than one.
Professor Guild: More, yes.

Q107 ***Lord Marlesford:*** In other words, going back to the Chairman's point, the more questions you ask the more information you are going to get, both accurate and inaccurate. On that basis, it seems to make the opposite case to that which you are making.
Professor Guild: There is another issue which comes back to the question of risk. When you collect data, when information is collected by airlines and passed to governments, how many spelling errors are tolerated before the person is refused the right to travel by the airline? If you type in your first name incorrectly, are you refused access to the 'plane? If you type in an extra letter in your surname, does it prevent you travelling? If your gender is incorrect because you ticked "Mr" instead of "Miss", are you prevented from travelling? The information which is passed on is the information which you typed in online, with all of the human inaccuracy which is inevitable. If that is the information against which checks are being made, the question is: is this a system which helps law enforcement or, in fact, has any effect on risk? If you are intending to blow up an aeroplane with a suicide bomb, if you have one letter wrong in your surname and your gender wrong and you still travel, the information which has been sent is the information which you provided. Is this an effective way of dealing with the question of risk? Will that information be associated with the name on the watch list?

Q108 ***Lord Marlesford:*** You are still making the same point that I was making. If you only ask people their name and you decided whether or not to let them in on the basis of their name and they got it wrong, and you decided you would not let them in on that basis, that would be a much greater risk to people than asking them 40 questions on which they might make one or more mistakes.
Professor Guild: Increasing the number of elements, of course, will increase the risk of error. These checks are being done automatically by computer programmes, there is no individual who can say: "That is clearly not an important one, but let's look at that".

Chairman: The well-publicised case of Edward Kennedy presumably arose because there was another Edward Kennedy. The passport numbers and the dates of birth, and so on, must presumably have been wrong. Anyway, I will ask Lord Foulkes now, please.

Q109 ***Lord Foulkes of Cumnock:*** I travelled halfway round the world as Mrs Foulkes, but I do not see what relevance that has to what we are discussing today. What worries me, my Lord Chairman, is that a number of statements and alleged facts are being made, particularly by Mr Bunyan, without giving us corroboration. Who says there are 132,000 on the US watch-list? Where did you get that figure from?
Mr Bunyan: Most of my information is coming from the Government Accountability Office of the United States, which is a highly respected organisation. So respected, in fact, that Congress shuts down a measure if they come up with a bad report, as it did over CAPPS II.

Q110 ***Lord Foulkes of Cumnock:*** From whom?
Mr Bunyan: The Government Accountability Office of the United States.

Q111 ***Lord Foulkes of Cumnock:*** As a government?
Mr Bunyan: It is a bit like our National Audit Office except it does a lot more, in my view, detailed and important work. It is very similar to our National Audit Office except it has far more resources and goes really into depth about the effectiveness of privacy and data protection issues.

Q112 ***Lord Foulkes of Cumnock:*** You said earlier that when I book a flight from Edinburgh to London by British Airways I am agreeing to all my information being passed to the United States authorities.
Mr Bunyan: I have to tick a box or I cannot book online.

Q113 ***Lord Foulkes of Cumnock:*** I book online regularly, and I have never ticked such a box. On what basis do you say that?
Mr Bunyan: Maybe you are a frequent flier. All I know is that that particular page we have actually got on our website. I am telling you my own experience, and maybe you have a different experience. I am merely giving information, and we do have a copy of that page on our website, so I could send you the URL if you doubt what I am saying. We may just have had different experiences; that is possible.

Q114 ***Lord Foulkes of Cumnock:*** Professor Guild, the 40 per cent figure that you said was from three studies, what is the basis for that? I was not clear. Maybe I did not hear it.
Professor Guild: The national reports of Data Protection Supervisors over the last three years in France, certain *Länder* in Germany and in the Netherlands.

Q115 ***Lord Foulkes of Cumnock:*** Where did you get that figure from?
Professor Guild: It is a study which has been carried out by a researcher at my university who has examined . . .

Q116 ***Lord Foulkes of Cumnock:*** Where did she get the information from?
Professor Guild: The public, annual reports of the data protection authorities in France, some *Länder* in Germany, and the Netherlands.

Q117 ***Lord Foulkes of Cumnock:*** You can let us have a copy of that report?
Professor Guild: Of course.[1]

Q118 ***Baroness D'Souza:*** The Home Office Minister told us that the PNR data is a valuable source of data for risk assessment and intelligence purposes. She mentioned also a pilot project that is currently being undertaken by the UK e-borders programme. Could we have your views on that?
Mr Bunyan: As I said earlier, it would be good for this Committee to know and to ask the Home Office what PNR data the UK is collecting so this Committee could compare PNR data being collected by the UK, Canada and the United States. I think that would be a logical question to ask. The pilot programme she is talking about is a Semaphore programme which is targeted at flights in and out of particular countries. One might guess and expect them to be countries like Sri Lanka and Pakistan, where they are profiling people to a much greater degree than general travel. This is what that scheme is, although, on the profiling concept, if you look at the Home Office plan published in December, while it is currently being used for targeting flights from what they call "risk countries" they do intend, in the longer term, to profile all passengers. They are profiling these people for what, is known as APIS, Advanced Passenger Information System, which is the red, yellow, green system, which is operated in Australia now. Red, you cannot get on a 'plane, basically, and green you can get on a 'plane. Again, the studies from the United States, the Government Accountability Office, show that the yellow category is the biggest problem area, in that people are misidentified or wrongly

[1] See supplementary evidence from Professor Guild, p 39.

identified. We also have a problem down the line in the UK and the EU that all the studies show, as does Peter Hustinx's view as a European Data Protection Supervisor, that the bigger these databases get the error rate increases. That holds for both the data that is being checked or indeed for fingerprints themselves, which are meant to be exclusively biometric. All the evidence shows that the error rates, in other words being wrongly identified as being someone of risk, or not being identified, which one could argue is even worse—I am a risk but they have not found out I am—increase. So, for all the biometric tools, we have got to look at it very carefully and draw on experiences from the United States where they have, in my view, much more detailed information than we have available in the European Union.

Q119 ***Baroness D'Souza:*** Surely biometric data is not subject to the same rate of error as other data?
Mr Bunyan: No, but, again, all the studies show—and the first ones were done about the Visa Information System, which in the European Union is eventually going to grow over ten years to 70 million (ten fingerprints of 70 million)—that as it gets bigger the error rates are going to grow. The error rates on fingerprints will not be as great as the errors on data, or intelligence, but there are error rates which have to be taken into consideration. We ought not to think that these are totally infallible systems which the bigger it gets it is going to work. I give you another example: at the moment we have what are called digitised pictures in our passports—they call them "biometric" but all they are is a digitised copy of the normal passport picture; they are not a biometric—

Q120 ***Chairman:*** We will be seeing Mr Hustinx's deputy in Brussels tomorrow, so we will be able to pursue that with him.
Mr Bunyan: So our Government is claiming they can check this against a main database. The National Audit Office report in January said that using that passport picture digitised on a chip would not be accurate on any database holding more than 10,000 items. Excuse me, they have got more than 10,000 already, so there is a problem over which technology we are talking about—the picture or the fingerprints. All I am saying is there is a risk and one must not think of those as being absolutely accurate systems.

Q121 ***Chairman:*** Professor Guild, do you want to add to that?
Professor Guild: I am not particularly familiar with the E Border Programme so I would not address that particular question.

Q122 ***Baroness Henig:*** The current US data retention period is 40 years. Would a period considerably longer than 3.5 years cause any problems?
Mr Bunyan: I think the US Visit Programme, I may be incorrect, is longer than 40 years, but we can look into that.

Q123 ***Baroness Henig:*** At least 40 years.
Mr Bunyan: The 3.5 years one is quite interesting, because why 3.5 years? The Data Protection Working Party, again, in the European Union has looked at this issue, so this period of 3.5 years is only 3.5 years because that is the length of the EU/US agreement; it has no other basis to it whatsoever, other than it is going to run out next July. People are not aware that there actually is an EU PNR scheme being constructed. We have our own scheme, which is concerned with the entry of people into the European Union. That is not just visa people; if we go out of the European Union we are going to be checked. That set of data may be held, but the limit on that data (this is an EU Directive in April 2004) is that it may be held for 24 hours, unless there is a specific reason why it can be held for longer. In other words, you cannot hold this mass of information for longer than 24 hours unless you have a reason for holding it for longer than 24 hours. I would go on that advice, at the end of the day, because I do have great respect for Peter Hustinx and for the Article 29 Working Party, if you look back at the history of their reporting. They do look at each measure individually, which may have different purposes: some may be entry systems, some may be what has been discussed as a European Union entry and exit system, which is obviously a more complicated system. So I do not think we should see 3.5 years as being set in stone; I think we have got to look at the new proposal when it comes up, which has to be reached by July next year, see what extra information the United States wants to have and make a decision about how to set some limits. Where they may need to hold it for longer, what are the limits on that? I would leave that question open until we see the new draft agreement, presumably some time later this year.

Q124 ***Baroness Bonham-Carter of Yarnbury:*** Can I ask a supplementary to that? You are saying you would agree that 3.5 years is too short a period?
Mr Bunyan: I do not know. I would start out with the EU Directive of 2004, which is the only one we have got, which says it may only be held for 24 hours.

Q125 ***Baroness Bonham-Carter of Yarnbury:*** Is that sensible? What can you do with information that you are only holding for 24 hours?

Mr Bunyan: As Elspeth says, it is being collected for commercial purposes, is made available for other purposes, and the first purpose is to check should that person be allowed to travel. The second purpose is, if that person does travel, are they a threat to whichever country they are travelling to? So the purpose of collecting this data is, firstly, to book a ticket, and the second purpose is to judge whether that person is a threat on that 'plane or is going to be a threat in the country they arrive into. Now, if you want to have a third purpose at some point in the future you have got to show good reason to do it, which is what the Article 29 Committee is saying, because you have collected for one purpose, you are already using it for one other purpose, which is to guarantee airline security, which I totally agree with, which is to stop terrorists entering your country, which I totally agree with, but if you want to start using it for other purposes then you have to show good reason, and we have got to see a proposal in writing. That is what they are saying. So the 3.5 years is a bit artificial because it just happens to be the length of time of the present EU/US agreement. There is no particular reason why it is 3.5 years; it could have been ten years, it could have been two years; it was just set to fit the length of time of the agreement.

Q126 ***Baroness Bonham-Carter of Yarnbury:*** The Minister has told us that Member States may refuse to supply PNR data if they are not confident that departments with which the Department for Homeland Security shares PNR data provide adequate protection. This is a question for Mr Bunyan because we know what Professor Guild feels. Surely the power could never be exercised if all Member States had to agree?

Mr Bunyan: Quite clearly, you have got to have an EU-wide agreement. There are a number of other areas—like disagreeing with the US over its open skies policy, or whatever—where what we see is the US trying to negotiate bilaterally, particularly with the newer Member States of the European Union, and trying to undermine the EU having a position on it. We have to have a process here where the EU has to agree with the United States that it has got to have proper data protection, we need to know who is getting access to that information and we need to have a proper review process. Only in that way can we start to build up our rights in terms of why is our data being collected, what is it being used for and who is it being passed on to? It would not be a good idea for Member States to individually have agreements.

Professor Guild: I would say it is clearly illusory to suggest that power could be exercised by one Member State. Therefore, even to include such an option is to create an illusion of possibility of an exercise of a power. If we have concerns and if we genuinely think that information should be refused, it must be done on a common basis; it has to be done on the basis of solidarity. I would only add one other point on the question of retention periods, which I think is important. I agree entirely with Tony's position: data must be collected for a purpose, the purpose must be clearly stated and the period of retention must be proportionate to the purpose which is intended. That is the first step. The second step is that the retention period of any particular set of data may be shorter or longer, depending on who is going to have access to that data. So, for instance, banking data is collected and retained for very long periods of time but there are extremely strict rules on access to that data. Therefore, who gets to look at the data affects also the legitimacy of the length of time for which it can be retained. However, the first question is the purpose—what purpose is this for—secondly, what data is collected, and, thirdly, who gets access to it?

Q127 ***Lord Teverson:*** It seems to me that one of the areas around this is that everybody wants to prevent terrorism and organised crime, or whatever, but for an operation to be successful and to keep public confidence there has to be confidence in the review process. There was quite a bit of controversy about the review that took place in 2005, and on conversations which have taken place on the American side I think we would say there is probably some indignance that they feel hard-done-by by the criticism that was levelled at them in the process of that review. Could you tell us whether you think the review process is adequate at the moment, or how that should be changed?

Mr Bunyan: The point is that if the EU has an agreement with the United States I make the presumption that that is an agreement between equal partners. If you have a detailed agreement, many pages long, which was examined in the Parliament by the Council and subject to criticism but, in the end, there was agreement, and now there is a new agreement, if we are entering this as equal partners you cannot have one partner (and the team which went from the EU was a high-level team of officials) in a situation where they say that there were a number of records where access was limited and they were not given hard copies of certain procedural advice. You cannot have that situation. To add insult to injury, the EU team was actually, and I quote, "required to sign confidentiality agreements exposing them to criminal sanctions for any breach". This is not the way you work when you have two equal partners. So I think the EU needs to put its foot down and say: "If we are equal partners you can have access to our data but we must have access to your data. Here are our officials, let us

have the names of your officials, and let us be full partners, for goodness sake".

Q128 ***Lord Foulkes of Cumnock:*** Who are you quoting from there?
Mr Bunyan: The quote is from the European Commission report on this joint review process.
Professor Guild: Of course, we do not know if there will be ever be another review. At the moment it seems quite unclear. Without a review we have no idea how we are going to provide any kind of assurance to anyone on what is being done with the data. I think there is quite an important difference of perspective, clearly, from the EU side and from the US side, in the EU data protection is considered an important job of the state; it is not the job of the individual to enforce their privacy rights, it is the duty of the state to protect the data of the individual. Therefore, we have Data Protection Supervisors who have these roles which are particularly important. The US perspective has always been that it is the individual's right to enforce the right of privacy, the private sector against the state, so of course you are going to have a different way of looking at what a joint supervisory body should be doing and what the role of a European data protection authority should be.

Q129 ***Lord Teverson:*** Could I ask five simple points? What do you think should be the basis of a review clause in a new agreement? What are the headline things that need to be in that?
Professor Guild: Clearly, there must be a full review of the correct application of the agreement; any issues in respect of differences in interpretation on the meaning of the agreement and the application of the agreement need to be specified in the report which both sides put forward; the report needs to be made public with, of course, if necessary, sensitive data removed or controlled, (we have many computer systems for doing that); it needs to be published, it needs to be timely and it needs to provide an opportunity for additional opinions by those who have been responsible for carrying out the review.

Q130 ***Lord Harrison:*** Let us pass on to another possible disequilibrium. Dr Gus Hosein has told us that travellers who are not US citizens are not covered by the US data protection laws but can apply under the freedom of information laws in the US if they want to know how their data have been used. In your view, is that an adequate and effective means of redress? Are there other ways of challenging misuse of data by the US authorities? If there are, what are your positive suggestions about strengthening?
Mr Bunyan: I know Gus Hosein and, indeed, I have worked with him and others actually in putting a freedom of information question in the United States on other issues. I do think it is a little difficult because certainly we needed a bit of help about which department to send the questions to, etc. One of the biggest problems we have here is the United States has never been prepared to tell the European Union exactly which agencies get access to this data. In other words, they are unable to tell us, although there are lots of agencies at federal, state and local level. A figure was mentioned in relation to the first agreement that something like 1,500 agencies might get access. Last October, in the middle of the re-negotiation, it was a bit worrying (this is the point I am making about how many agencies) because the US law was changed and it turns out if the agreement is there and the US changes its law then so does the content of this agreement, apparently. According to the executive order enacted on, number 11388, the Department for Homeland Security was told, basically, to extend the number of agencies and: "the US may not be impeded by a certain provision in the undertaking in the EU/US agreement to restrict information sharing amongst US agencies. The undertaking should be interpreted and applied so as not to impede the sharing of PNR data by the DHS and other authorities". So there is a problem here: who are you giving the information to? We would have a competent authority in each EU Member State you could go to which would then be responsible for finding out where that data had been passed to and had been further processed. The problem for us is we do not know how many agencies have access to it.

Q131 ***Lord Harrison:*** At the moment, what does Joe Bloggs do?
Mr Bunyan: There is a provision within the agreement to make a complaint. The problem is, what are the powers of the body you are complaining to? Are they able to find out what has happened to the data?

Q132 ***Lord Harrison:*** There is no posting box, as it were, to lodge the first complaint.
Mr Bunyan: There is in the information which is circulated; there is an address in the United States to which you can complain, but it is one that has been set up as an administrative measure not as part of US law, if I can put it like that. The US law is the 1974 Privacy Act which protects the data protection rights of all US citizens. However, that Act does not extend to non-US citizens. We have to remember this issue is not just cropping up on the Passenger Name Record, it is cropping up over the whole Swift scandal—the access to banking data. I have seen the minutes of some of the EU/US high-level meetings,

and I am quite surprised that so much time has passed and the EU has not finally put its foot down a little bit and said: "Look, we have got Swift, we have got PNR and there are other things coming up. You really must get a law, like Canada has got or other countries have got, in order that we do not keep having this problem."

Q133 ***Lord Foulkes of Cumnock:*** Surely, my Lord Chairman, the freedom of information laws in the US, as I understand it, are far more extensive than they are here, are they not? You can get lots more information; we can get information even about things that are happening here from the United States.
Mr Bunyan: In the main. It is not necessarily true when you are talking about the justice department when you are getting this kind of information. Yes, they do have good freedom of information laws, but it does take time and you have still got to know who to write to and you have still got to know how to frame the question. You may have to write to a number of agencies. Let us remember the case which came before this Committee before: there was the famous case, many years ago, of two Welsh football players (this is under the Schengen system) who were arrested in Luxembourg, went on to a system, then got arrested again, and it took them three years to get their names off the record because they had done nothing wrong. They had to get the European Commission to track down that Belgium was holding information, and the United Kingdom which passed it to various embassies around Europe.

Q134 ***Lord Foulkes of Cumnock:*** That is nothing to do with the United States.
Mr Bunyan: The point I am making is that once data is being held on you and can be passed to innumerable agencies how do you find out what data those innumerable agencies have got? If it is wrong, how do you get it corrected? I use the EU example because it is one of the rare examples we have got of how difficult it is for an individual, once they get on to a list or get wrongly on to a list, to get off the list. I do think that bears example. At least here we know there is a Schengen authority, at least we have got national contacts and can do something, but in the United States where do you begin?

Q135 ***Lord Foulkes of Cumnock:*** You mentioned 1,500 agencies. Where does that figure come from?
Mr Bunyan: From the United States themselves.

Q136 ***Lord Foulkes of Cumnock:*** But whom in the United States? You just read out a quotation—
Mr Bunyan: You are asking me to remember exactly which official from the United States said this about four years ago. I do not know. I can certainly find the reference to it, and there was a figure supplied as part of the negotiation.[2] We are not just inventing these figures; they are as a result of us having studied this over the last five years.
Lord Foulkes of Cumnock: My Lord Chairman, I think it is very important, when evidence is being taken by a Committee of Parliament, that sources are quoted and figures are not given, because figures get repeated and repeated and repeated, and people start believing they are accurate without any justification at all.
Chairman: I entirely take your point and I think that if you can track down the answer to that question it would be very helpful if you could let us know in writing later.
Lord Marlesford: Going back to Mr Bunyan's first question, I think, you mentioned that out of 64 million—how many was it—

Q137 ***Lord Harrison:*** Twelve hundred.
Mr Bunyan: This was the Acting Director of the Visit Programme, and he said that 63 million passengers were processed and entry denied to (and I am quoting here) "1200 criminals and immigration violators".

Q138 ***Lord Marlesford:*** You were saying that was a rather small number.
Mr Bunyan: This is an opinion, obviously. I was giving you the facts and then offering an opinion that this seemed quite a small number, especially as it is not broken down, especially when we are talking about trying to deter terrorists from this.

Q139 ***Lord Marlesford:*** Can you just remind us how many non-American citizens were involved in the 9/11 hijacking?
Mr Bunyan: I do not know that figure.
Lord Marlesford: I think it was 19.
Chairman: We must move on. Have either of you any last point you want to make on this subject? In which case, thank you very much indeed. I should have thanked you earlier, Professor Guild, for your written evidence. Also, just to let you both know, we do have a copy of the Commission's staff working paper on the joint review. That is also a useful part of our written evidence. Thank you both very much.

[2] See supplementary evidence from Mr Bunyan page 39.

21 March 2007

Supplementary memorandum from Professor Elspeth Guild (CEPS)

In evidence to the Committee on 21 March, I explained that a research student at my university had examined reports on data held in the Schengen system, and that according to the Data Protection Supervisors in some of the German Länder and in France and the Netherlands the quality of data in the Schengen Information System, which is collected for law enforcement purposes, had an inaccuracy or improper mechanism of use of up to 40 per cent.

I undertook to provide the Committee with the sources of the reports of the Data Protection Supervisors. They are as follows:

— The reports of the French Data Protection Supervisor can be found at: www.cnil.fr. In particular, see 25th Rapport d'Activité CNIL, 2004, published 2005, pp 46–47.

— For Germany see for instance the Annual Report of 2003–04 Datenschutzbericht no. 17, NordRhein Westfalen, or the 20th Annual Report of the Federal Data Protection Commissioner: 20 Tätigkeitsbericht 2003–04 para 3.3.2.2.

— For the Netherlands see the Annual Report of the Data Protection Authority 2004 p 53.

23 April 2007

Supplementary memorandum from Tony Bunyan, Director, Statewatch

When I gave oral evidence to the Committee on 21 March, members asked for the source of my statement that some 1,500 US agencies at federal, State and local level might get access to data sent under the PNR Agreement.

This figure comes from paragraph 11 of evidence given to the Committee in October 2004 by the Europol, Eurojust and Customs Joint Supervisory Authorities in connection with its inquiry into terrorism, and published on page 148 of its report *After Madrid: the EU's response to terrorism* (5th Report of Session 2004–05, HL Paper 53).

17 April 2007

THURSDAY 22 MARCH 2007

Present	Caithness, E	Marlesford, L
	D'Souza, B	Teverson, L
	Foulkes of Cumnock, L	Wright of Richmond, L (Chairman)
	Listowel, E	

Examination of Witnesses

Witnesses: Mr Jonathan Faull, Director-General for Justice, Freedom and Security (JLS) and Ms Cecilia Verkleij, DG JLS policy lead on PNR and data protection policy, examined.

Q140 ***Chairman:*** Director General, can I welcome you, and thank you very much for coming. As you know, this is an evidence session in two parts and I think you have kindly agreed to answer some questions for us, first of all, on PNR and, secondly, on Prüm. Depending on how the conversation goes, I suggest that I might be quite rigorous in trying to divide the meeting into two separate hours. As you know, this is a meeting to consider two subjects on which we are proposing to report. This meeting is on the record and a note is being taken of the discussion and you will, of course, as before, be sent a transcript for any comments you may have. Without any further ado, I wonder if I could start by taking PNR as the first of the subjects. What contribution do you think the 2004 and 2006 Agreements have made to the fight against terrorism and other serious crime? Has an assessment ever been made of the effectiveness and proportionality of the transfer of PNR data?

Mr Faull: I think it makes sense to think of the two Agreements as one. The 2006 Agreement was an interim agreement, which will expire in July and we hope will be replaced by a new one but, essentially, it carries over the 2004 Agreement which, as you know, was struck down by the Court on essentially procedural legal grounds and was put back in place. I know we will have a discussion a little later on about the precise effect of the letter interpreting the Undertakings, but the Undertakings remain the same, the Agreement remains the same, and I think its impact should therefore be judged across the whole period. That having been said, we are given to understand by our American partners, first of all, that they continue to believe that Passenger Name Records provide a very useful source of information when used in conjunction with other information they have in the fight against terrorism and serious crime. They have given us some specific examples of the use to which PNR has been put to that end and stress, for understandable reasons, two things, in fact, one that European agencies have also benefited from their work using PNR data in our own fight against terrorism and serious crime and, also, of course, the other thing I have to say is unfortunately the examples they give, which even to me are only sometimes in outline, are very highly confidential. That has been repeated over the months and years during which we have been discussing these issues with the United States. The second point to make in this respect is we carried out a very thorough Joint Review in September 2005 of the way in which the Agreement and Undertakings had been applied until then, "we" meaning the Commission, plus Member States, including data protection experts. There is a version of the report of the Joint Review in the public domain. In summary, the result of the Joint Review was, firstly, that the Agreement had been complied with rigorously, the Undertakings had been complied with rigorously, and the PNR data were being used, therefore, properly in the way in which they were supposed to be, and they had been instrumental in allowing the US authorities to identify high risk passengers who, when other information was added to the analysis, could be identified as engaging in or suspected of engaging in terrorist activities.

Q141 ***Earl of Listowel:*** Director General, when a Joint Review of the working of the Agreement was carried out—we have been discussing that—access by the European data protection authorities to files was restricted on security grounds. Did the European team feel at that time they had sufficient facts to assess the working of the Agreement? Will a similar provision be incorporated in the new Agreement? From what you have just said, it suggests that did not seem to be a particular issue for them but perhaps you might expand a little bit further on what you said before.

Mr Faull: As I said, the team on the Joint Review was composed of Commission officials and representatives of national authorities, both national data protection and national law enforcement authorities. The common view of all the participants was that they had had access to sufficient facts to carry out a proper assessment of the implementation of the Undertakings and that is what the report says. Will there be a similar provision in a new Agreement,

that is very much a matter for negotiation with the Americans, and we have barely started negotiations under a new set of negotiating directives given to us by the Council only a month ago, and we have not reached that issue yet. I think it is fair to say that the Americans found the Joint Review useful, important, but also extremely cumbersome. It occupied a lot of their time, and I would not be surprised if they sought in the negotiations a somewhat lighter form of review in a new Agreement. That is my impression from what they said during the discussions of the interim Agreement, but we shall certainly want to have a proper system for making sure that whatever Agreement is entered into is properly applied.

Q142 ***Chairman:*** There has been reference to security grounds for a restriction on the Joint Review. In general, did you get the impression that the Americans were wholehearted in taking part in this Joint Review?
Mr Faull: Yes, they were, there was no doubt about that, so much so, I think, that they devoted considerable resources to doing it properly, engaged lots of their people for several days on the spot in Washington and at airports, plus all the preparation which went on beforehand. That is probably why they want something a little lighter this time because they did take it so terribly seriously. There may be other ways to make sure they take it seriously, we will have to look at all of that.

Q143 ***Baroness D'Souza:*** If I could go back to the first question. I understand that once you have got the information you have got, and I understand also the confidentiality, that the Americans had found PNR to be extremely useful. I wonder did you get any information at all about false positives or even whether they expected to have a great deal more information on individuals than they got?
Mr Faull: The PNR contain a wide variety of data, some of which can be misleading or confusing. I think they would say the more PNR you have, the lower the risk of making mistakes.

Q144 ***Chairman:*** Shall I stop you there for a moment and welcome your colleagues. It is very nice to see you here, and I apologise for having started the meeting before you arrived.
Ms Verkleij: Not at all, we apologise for being late.
Mr Faull: Cecilia Verkleij is the official in charge of the PNR file in my Directorate General and Chiara Adamo is my assistant. We were all in Washington recently for the first round of the new negotiations, to which we will return later, and I think Cecilia was in the Joint Review team.
Ms Verkleij: Yes, I had the pleasure of drafting the report. (Off the record)

Q145 ***Baroness D'Souza:*** Could you say whether your impression was that the Americans expected to get rather more information than was actually the case?
Mr Faull: Yes, perhaps. There are 34 items in the list of PNR attached to the current Agreement and not all of those PNR are always made available because when we fly we do not always give all that information to the airline. Most of the time, we understand, airlines send the PNR, or the Americans take PNR from our airlines depending on whether we are pushing or pulling, and we will come back to that no doubt, and fewer than the 34 are actually there for most people on most flights. Do the Americans want more information? It was the result of negotiation, there will be another round of negotiation and they may well ask for more information. Our view at the moment is that the 34 PNR items are probably sufficient and may even be excessive in number, and we will certainly at least wish to negotiate very seriously with our American partners about each individual item of information.
Chairman: Incidentally, I should have said at the beginning, we have just gone off the record while you were recapping, but if at any point you want to go off the record, you are very welcome to and we will ensure that is respected.

Q146 ***Baroness D'Souza:*** What I am interested to know is about the level of mistakes, false positives, mistaking identities, whether that was greater than they expected or less?
Ms Verkleij: That is a different issue.

Q147 ***Baroness D'Souza:*** It is a slightly different issue.
Ms Verkleij: It is important that you raise it but the false positives is the issue of comparing your passport data with the no-fly lists, the watch lists; with PNR you do not have false positives.

Q148 ***Baroness D'Souza:*** It is only when you use the two together?
Mr Faull: Exactly. If I am Jonathan Faull—I will use a very uncontroversial name—and flying to the States and all my information on the PNR gets there, that can only be mine because it is way beyond just a name, it is what seat I am in, my credit card number, who booked the flight, which travel agent, that really narrows it down. The problem arises if they have a list of people they want for some reason and a Jonathan Faull is on that, who happens not to be me because somebody has written my name down wrong or there are two of us, that is where a false positive can arise, but it should not arise from 34 maximum PNR items.

Ms Verkleij: It does not arise from your PNR because in your PNR your name may be written in different ways. Therefore, in terms of data quality, your name as appearing in your PNR is not accurate enough for customs and border protection authorities, they compare the no-fly list with your name as written in your passport and that is the match which is being made. That may result in a mismatch, but it is a different set of data which the US compares in order to make sure that certain people are not even allowed to board a plane.

Q149 ***Chairman:*** Are there particular concerns with open-fields' categories of data?
Ms Verkleij: Yes, because they may contain sensitive information.

Q150 ***Chairman:*** The Canadians do not have those?
Ms Verkleij: No, they do not, they have excluded them from the list. (Off the record)

Q151 ***Baroness D'Souza:*** I still do not have an answer to what I said about the percentage of false positives when you put the new databases together, but let us park that for a while. We have been told that travellers who are non-US citizens do not have the protection of the data protection laws but they can apply under the Freedom of Information laws in the US if they want to know what data is being held on their account. Do you think this is an adequate and effective means of address? Are there other ways in which you can challenge the misuse of data?
Mr Faull: Yes, I do think the current system with a recent addition, which I will explain, is satisfactory. First of all, the current Undertakings provided in paragraphs 37 to 42 for a system of redress and access for data subjects, including, of course, Europeans, so therefore non-Americans, apply to us, not only to US citizens. A data subject may have access to his or her PNR data contained in the Department of Homeland Security databases. He or she may apply to have data rectified, first to the Department itself and then, secondly, to the Department's chief privacy officer. The Undertakings provide the data subject with an additional right of complaint to national data protection authorities back here in our Member States, and those authorities may in turn lodge complaints with the United States authorities. Most recently, the US has introduced a new redress system known by the acronym TRIP. I am trying to remember what it stands for, do you remember?
Ms Verkleij: No.

Q152 ***Chairman:*** That is the trouble with acronyms.
Mr Faull: I will find out. We were asked by a member of the European Parliament whether that system applied to EU Member State citizens. We asked the question directly to the Department of Homeland Security and the answer was a resounding yes. They have set up a dedicated redress system for the Department of Homeland Security's databases like this one and that definitely applies and is open to all of us.

Q153 ***Baroness D'Souza:*** And it works within a timeframe?
Mr Faull: Yes, certainly there are time limits. This TRIP system is a new one, so I am not sure that any assessment has yet been made of it but I have no reason to think it does not.

Q154 ***Lord Foulkes of Cumnock:*** Mr Baker of the DHS sent you an email on 11 October and in it he said, and I quote: "With this letter the US has consulted with the EU". That sounds a bit peremptory and does not smack of an equal partnership. Can you tell us what real opportunities you had to make comments on this before it was added?
Mr Faull: Perhaps he should not have phrased it quite that way. What he meant was the letter followed, and it did, extensive discussions and consultations. This may be an American usage of English, I do not know, but he wanted to record, as he did in that email, that we had had extensive discussions and consultations on the specific issue, which we had.

Q155 ***Earl of Caithness:*** Let us stick with Mr Baker for a little bit, shall we, in that in effect he was giving a unilateral explanation of how the US authorities intend to interpret the Agreement. Should not the terms of the Agreement be clear enough so there is no doubt about their meaning and how they should be interpreted?
Mr Faull: In an ideal world agreements would be crystal clear and you would never need to have other pieces of paper interpreted. What we did was when the Court of Justice struck down the first PNR Agreement we went back to our American friends and said, "We need to put something back in place using a different legal basis". We had to explain to them our wonderful world of pillars and all of that, which we did, and the Americans said to us, as they were perfectly entitled to do under the Undertakings, that various things had changed in the law of the United States in the intervening period of which they wanted us to take account in the way in which the Undertakings were

understood. We, and when I say "we" it is important to remember because we are acting under the European Union Treaty, therefore the third pillar, and it is the Presidency in the lead on negotiations assisted by the Commission so we,—the Presidency at the time Finnish, now German for the new negotiation—and the Commission received negotiating directives from the Council which essentially asked us to maintain the status quo, not to change the Undertakings, and to conclude the Agreement on a new basis. That was what we were asked to do.

Q156 ***Chairman:*** You mentioned that you have just been to Washington, were you chaired by the Presidency?
Mr Faull: Yes.

Q157 ***Chairman:*** They were in charge of the negotiation, were they?
Mr Faull: Yes, always, absolutely

Q158 ***Chairman:*** I am sorry, I interrupted you.
Mr Faull: We said to the Americans, "The Undertakings are untouchable. The Agreement should simply be recast in the new legal framework", but they said, and I think we had to recognise some force in this, "Things have changed in Washington in the last couple of years". This was 2006, the Agreement was 2004. It is true that the United States had introduced a number of new items of legislation and, above all, had enshrined in law, both in an act of Congress and in an executive order by the President to the Executive Branch, of which the DHS is part, of course. The change can be summed up as the introduction of what they call an "Information Sharing Environment" ISE. In America part of the Department of Homeland Security is called ICE, and I forget what that is.
Ms Verkleij: That is a special branch.
Mr Faull: Customs?
Ms Verkleij:. ICE is US Immigration and Customs Enforcement.
Mr Faull: The Information Sharing Environment is ISE. What is ISE? ISE is, I think we can understand this, one of the principal lessons that the US authorities have learned from 9/11 and from the 9/11 Commission Report, which is that intelligence information should be shared between all the law enforcement agencies that are likely to find it useful. The criticism made of the situation which prevailed until 11 September 2001 was an excessive compartmentalisation of intelligence and law enforcement agencies, an issue not unknown in some of our own countries, and no doubt lessons have been learned on this side of the Atlantic as well. They explained to us in Washington that the main lesson they learned was you must share information. If information enters the US system, the US Government, a US agency in one place, it has an obligation to make sure that all the other members of what is a rather large community and a rather large body of agencies at federal and state level in the United States should also know. I think that is a matter of fact. That law was enacted. The President gave the orders to the Executive Branch to follow this very carefully. Meanwhile, it has to be acknowledged that our PNR Undertakings proceeded on a very different basis, that one part of a government department, the Department of Homeland Security's Customs and Border Protection Department, should receive the PNR and, in principle, should not show them to anybody else.

Q159 ***Chairman:*** They are protected.
Mr Faull: And only under very specific rules, in very specific circumstances, should they be able to share them with other people. The Americans said to us, "Look, things have changed over here. We need to have this reflected", and we said, "We cannot change the wording of the Undertakings, but the Undertakings do provide, which explains Mr Baker's email in part, that following consultation and discussions the way in which the Undertakings are interpreted and applied may be reviewed by the parties in the light of changes in the law or policy of one of the parties" and, to be fair, I think that has happened. What we agreed was we would discuss the interpretation of the Undertakings in the light of these recent intervening events and that those interpretations, which were agreed largely amongst us, would be recorded in an exchange of letter. Mr Baker wrote to me and to my counterpart in the Finnish Ministry of Foreign Affairs and on behalf of the Council we wrote back saying, "We acknowledge this. Thank you very much". All of that is published in the official journal of the European Union and that is the basis from on we operate today.

Q160 ***Lord Marlesford:*** My question follows on from that. We have been told that data mining and data profiling have been used by the US on the basis of the PNR and, for example, for its Automated Targeting System. Do you regard this as lawful and legitimate use of PNR under the Undertaking? If not, what are you doing about it, if anything?
Mr Faull: The purpose of collecting PNR data is to identify potentially high risk passengers on the basis of certain characteristics or a combination of characteristics and to that extent there is what is often called "profiling" taking place. They are looking for patterns of behaviour. It does not mean that anybody is a criminal or even necessarily suspected of committing a crime, but they are

building up a pattern about the passenger behind the Passenger Name Records and then cross-checking that information with other sources of information. I do believe that is lawful and is in compliance with the Agreement and Undertakings.

Q161 ***Lord Teverson:*** The system at the moment is a pull system from the United States, whereas I think it was intended that it should be push. Where has that got to at the moment agreement-wise? I think the barrier was a technological one with the airlines. Is that likely to be solved by the time this new Agreement comes into effect?
Mr Faull: The situation now is already mixed, there is pushing and there is still pulling as well. Some European airlines have switched to a push system because they have got the technical interfaces in place between their computer systems and the Department of Homeland Security's computer system. Others are still in the stage of developing and testing themselves and with DHS their push system. The Americans say they are perfectly happy to go to push. There is nothing legal or ideological here, it is a purely technical question. The question is how can we get the data reliably from one place to another? We attach importance to moving to push as quickly as possible because it is for our airlines to comply with the law as long as we can arrange things here in such a way that they can comply with US law without falling foul of European data protection law, and that is the purpose of all of this. We would rather that be the situation than the long arm of the American law stretching across the Atlantic into our computer databases and pulling the information out. Therefore, it is widely agreed, and we are under considerable pressure from the European Parliament on this, that push is the way to go. What we cannot do, of course, is arrange the technical work which has to be done by computer specialists, no doubt, at either end. The people designing the computer interface also need an absolutely secure regulatory environment because they need to know what information they are providing, what information they are not providing and what filters have to be put in. For example, we are very insistent that sensitive personal data relating to religion or ethnic origin or medical conditions be filtered out, those filters have to be built in. All that is being done and there are talks going on all the time. The European airlines have been in to see us recently, individually and through their various associations, and I understand we are not very far from putting most, and ultimately all, European airlines into a push system. I cannot tell you exactly when this will be done.

Q162 ***Lord Teverson:*** Presumably, to a certain degree, if something like the National Security Agency really wanted to know, it has the means of getting into these systems anyway, does it not, outside all of this within a context?
Mr Faull: I would not know. I hope that airlines' computer reservation systems are secure.
Lord Teverson: Unhackable.

Q163 ***Earl of Caithness:*** Data transferred under the current Agreement attract a data retention period of three and a half years. Mr Baker points out that the Agreement will expire before the end of three and a half years and that questions of when to destroy data collected in accordance with the Undertaking will be addressed as part of future discussions. Should not data transferred on the understanding that it will be retained for three and a half years be destroyed after that period?
Mr Faull: It depends what rule is finally provided for. Of course, if it is a rule which says the data shall be retained for X, then after X they should not be retained, which means they should be destroyed. The three and a half year period was an issue which, as Mr Baker said, did not need to be addressed in the interim Agreement for the simple reason that no three and a half year period was going to expire during the life of the interim Agreement. Of course, that does not solve the problem for the longer term, and there is no doubt that it will be one of the difficult areas for negotiation in the new Agreement. The Department of Homeland Security has not hidden its view from us that it finds three and a half years too short a period because they believe that PNR data may still prove useful thereafter. Where thereafter ends is a matter which we will be negotiating, and I imagine there will be some rather difficult discussions on this issue before we find the right balance between the needs of security and law enforcement, for which, no doubt, information is the basic raw material, and the needs of data protection, which require that data not be kept for any longer than is absolutely necessary for the legitimate purpose for which they are collected.

Q164 ***Chairman:*** Can you recall for us, why three and a half years?
Ms Verkleij: I would almost say it was by accident. The US started with 50 years at the time and that went down to seven, the Commission just wanted one year and then the compromise between seven and one year was three and a half years. The idea was the first Agreement would last three and a half years and the data retention would be as long as the first Agreement. Also, the idea was that the three and a half years should be used in order to gain a lot of experience and then come back and renegotiate and see whether three and a half years

would still be the right period, the number of data, so all these things will be back on the agenda again.

Q165 ***Baroness D'Souza:*** As you say, you are going to be negotiating this, but could you say something more about the rationale upon which a decision will be reached eventually? What evidence is there that data should be kept two, three, ten, 50 years?
Mr Faull: First of all, I think there are data and data. There are data which are in active live use in an investigation and I think everybody agrees that they should not be destroyed as long as they are needed for that particular investigation. When the investigation is finally and irrevocably over the information may not need to be kept anymore or should not need to be kept anymore. That is not controversial, what is controversial is the duration of conservation of data which does not seem in isolation to be particularly interesting but may prove useful one day because someone is under investigation, of whom very little was known before, and you want to reconstruct a pattern of that person's life, the clean skin issue, for example.

Q166 ***Chairman:*** Sorry, what is that?
Mr Faull: I thought that was widely in use in Britain.
Chairman: We do not understand you.

Q167 ***Baroness D'Souza:*** We are longing to know!
Mr Faull: My understanding of clean skin, but I only get this from newspapers, is it is British police usage, no doubt, meaning someone with no police record at all, not known to the authorities in any way, who suddenly features in a terrorist attack and has a clean record. In that event, everybody immediately wants to reconstruct that person's life.

Q168 ***Chairman:*** Everything known about them.
Mr Faull: Exactly. What can we find out about this person? One of the interesting things people are usually looking for is where has that person been travelling and therefore PNR come into the picture. If PNR are discarded after three and a half years—say the American law enforcement people—we may be missing important tricks. Would seven years be enough or 70 or 50, whatever they started with, I do not know. To answer your question directly, the rational basis on which a decision will have to be made on this will be finding out all we can about the genuine needs of law enforcement and counter-terrorism investigators based on their past experience and, as a starting point, taking that the period must be the shortest reasonable period possible to allow them to do their work properly. That is abstract, of course, and it will come down to a figure in negotiations and I do not know today what it will be.

Q169 ***Lord Marlesford:*** Following that up, it sounds to me as if what you are really saying is data should be kept for as long as is operationally necessary for the purposes of fighting crime and terrorism. If that is the case, it seems to me pretty absurd to start fixing dates.
Ms Verkleij: Yes, I see what you mean.
Mr Faull: It can be done that way. It can be written down in that sort of abstract way without putting a period on it. But the data protection systems we have usually require or at least have had the habit of putting numbers on things because people need to know. In a police station the people in charge of a particular database in a government department need to know precisely what to do, someone has to give a clear instruction. If you negotiate a rather broad form of words in an international agreement of this sort, which no doubt is a more accurate reflection of what we need, striking the balance, as long as possible for law enforcement and as short as possible for data protection privacy concerns, what are the poor people at the coalface supposed to do? Somebody has to give them a number at some stage. It has been thought so far that it would make more sense to try and agree a number in the first place, perhaps with exceptions. Cecilia Verkleij tells me that for Europol's database system, which one?
Ms Verkleij: I do not know for which information data they are using it.
Mr Faull: They have a review every three years, and on the basis of a more abstract form of words someone has to decide whether to delete or not delete.

Q170 ***Chairman:*** Basically, as with so much on this subject, it is a question of judgment or balance as to what is, (a) necessary and (b) proportionate, is it not?
Mr Faull: Yes, entirely.

Q171 ***Lord Teverson:*** If you take the clean skin example, surely on that you would want to know, exactly as you say, about bringing together the whole life of that person. Is that not done in a completely different way? Is that not done on much more co-ordination by security agencies because by then you have got a name, have you not, so if the problem was in the United States they would come back to European agencies and find out through law enforcement because a PNR profile would only give a very small part of that, would it not?
Ms Verkleij: Yes, but an essential part.

Q172 ***Lord Teverson:*** Surely it is much more effective to do it on all those other connections which go on rather than through this system?

Mr Faull: That would happen but if the data were just not available anymore they would be very limited in what they could find out to share with each other. Yes, of course you would have a name but PNR tells you a lot more than a name. PNR tells you with whom the named person has been reserving flights, next to whom he or she has been sitting on planes regularly, where they have been flying to and from, et cetera.

Q173 ***Lord Teverson:*** I understand all of that, but what I am saying is that information is much more comprehensively held within the airline, within wherever that is held?
Mr Faull: No, they delete as well.
Ms Verkleij: The airline deletes your information.
Lord Teverson: The issue is them not deleting their data here, not keeping it over in the United States where it really only will be partial because a lot of those fights that person might have taken might be on other airlines, do you see what I am saying?

Q174 ***Lord Foulkes of Cumnock:*** They get rid of it.
Mr Faull: The airlines delete it almost immediately. The airlines' interest in the passenger is commercial. Once you have got on the plane and landed safely on the other side they do not care about you anymore and they delete because you have paid your bill. Why are they interested in your credit card number? Only because they want to get the money from you.They have got the money and they have delivered you to your destination. If you are a frequent user of their services and they need to know more about you, you have got a frequent flyer card and information will be in there, that is separate, otherwise they clear their computer and move on to the next one.

Q175 ***Chairman:*** Surely the answer to Lord Teverson's question, as indeed he has suggested himself, is that the national intelligence and security and police agencies can find out very quickly by other means whether the clean skin person is actually as clean as suggested?
Mr Faull: Not necessarily because they are looking for the same information. If it is just not there, it is just not there, whether you are in Washington or in London.
Ms Verkleij: I think you should bear in mind that PNR is a very specific set of data which they may not get otherwise. It is a small part of a jigsaw puzzle but it helps them construct the jigsaw puzzle. Sometimes without a PNR they cannot make the link between this set of information and that set of information.
Mr Faull: Known associates, known travel parties.
Ms Verkleij: That may make a difference.

Q176 ***Lord Foulkes of Cumnock:*** I understand from what you said that you agree with Lord Marlesford that it would be unfortunate if someone like the shoe-bomber was missed because of an arbitrary date put on deleting information and that information was no longer available, is that right?
Mr Faull: Unfortunate would be an awful understatement. If any bomber were missed, of course and, therefore this is an extremely difficult subject and we have to get it right.

Q177 ***Lord Foulkes of Cumnock:*** You said that this retention period is going to be one of the difficult areas for agreement, although it sounds as if you have some sympathy with the American point of view, but our Minister told us that there is going to be a number of areas which will be difficult and the Americans are going to be pressing for fairly substantial changes in the Agreement. Would it be helpful to mobilise Member States to help you in any way in these negotiations?
Mr Faull: Of course, in negotiating with the United States the Union benefits greatly from the united strengths of its Member States. We would hope very much that all Member States would press, in their bilateral relations with the US Administration, for the positions which we are defending on their behalf. We have a unanimous—it has to be unanimous—mandate from the Council and that circumscribes what we do and gives us our marching orders, so we expect all Member States to be in there behind us at all times.

Q178 ***Earl of Listowel:*** When these important negotiations are concluded, will the European Parliament and national parliaments have an opportunity to comment on the draft Agreement or will they first see it after its signature, as happened with the current Agreement?
Mr Faull: The legal position is that using the procedure of the European Union Treaty there is no consultation of the European Parliament or of national parliaments before the Agreement is concluded. What we have agreed, and what we did previously, and what we have agreed to do again informally, is to provide throughout, on our part and on the Council Presidency's part, a constant flow of information to the European Parliament, and I am sure that ministers will want to keep their parliaments informed in national capitals as well. I personally, with the Council Presidency, report regularly to the Committee of Permanent Representatives, so the Member States are kept informed through that channel. After all our discussions in Washington we debriefed the embassies of the Member States on the spot. Even

though the legal framework is not very parliament-friendly, to be frank, we go out of our way—I hope people see this—to keep our Parliament informed here in Brussels and in Strasbourg and I am sure Member States do likewise as well.

Q179 ***Lord Marlesford:*** At the moment it seems all this information flows one way to America. Should we be aiming to change that to have a reciprocal flow of information?
Mr Faull: The Commission's view is that it would make sense to have a PNR system for ourselves in the European Union on the basis of which we would then have very good grounds for saying to our American partners, "This must be completely reciprocal. We have our PNR system, you have yours". We are at fairly early stages still in assessing whether and what to propose by way of a European PNR system. I think it should be realised that the Americans see planes flying into their territory as a potential threat.

Q180 ***Chairman:*** And over?
Mr Faull: And over. Whereas, I am not sure that all European governments see planes flying into their territories from North America in quite the same way. Therefore, there is a lack of symmetry between the public perceptions perhaps, but also official perceptions, of what is needed to provide for national security. I am not saying that anybody has made up their minds definitively and we have not and we have not made a proposal yet but, I have to say, I do not sense any great enthusiastic demand among Member States for creating a European PNR system. Member States that need such information have set up national systems which may not be called PNR but have similar objectives and I hope results. We are thinking about whether the whole of the EU should have one but until it does we cannot operate on a reciprocal basis with the United States. They want this information, they have enacted laws requiring it and we have to find a way to enable our airlines to comply with foreign laws, the purposes of which we fully understand and respect, without falling foul of our data protection laws.

Q181 ***Chairman:*** Would you expect the European Parliament to have an active interest in reciprocity? Is it an issue for them?
Mr Faull: Yes, it is. They believe, and I think in general they are right, that our international relations should be governed by reciprocity and we should not do things for others where others will not do them for us. That all makes sense in an abstract way but, as I said, as long as we do not have a PNR system there is nothing to be reciprocal about. What is important, and this comes back to a point I made earlier, is the intelligence work, the analysis made of PNR data, particularly in relation to transatlantic travel, should be of benefit to our security as well as to theirs. Afterall, a plane between here and the United States has our citizens on it as well as American citizens, our security interests are absolutely identical in that respect. If we can show, and I think we can, the European Parliament, for example, that European security is also benefiting from this arrangement I think the European Parliament will accept that argument.
Earl of Caithness: I have two questions, one is the Canadian one. Is there any reason why we cannot have a shorter Agreement like the Canadians have? Does the fact that our Presidency leads negotiations and the Presidency changes every six months weaken our negotiating position?

Q182 ***Chairman:*** I am sorry, we have not given you notice of this question.
Mr Faull: It is a good one though. There is no reason why the Canada Agreement should not be a reference point, a starting point, but each country is different. We do not expect the United States to have exactly the same security, law enforcement, privacy laws or concerns as Canada. They are similar countries in some ways and different countries in some ways, as we all know. It is not just a question of toping and tailing, crossing out Canada, putting in the United States, I think that would be different. We are well aware of the Canadian Agreement and so are the Americans, of course, and it will be one of the items which we will refer to in the discussions when we are looking for solutions, but they will not be identical because of the different history, structure and outlook of the two countries. The change of Presidency: what I can say so far is that in the successive and very different presidencies which we have worked with on this, we have always found excellent co-operation and a high degree of professionalism. We provide continuity and this is one of the Commission's roles, in fact, to assist each successive Presidency in doing this and, no, it has not been a problem. We have had presidencies with, the current one for example, lots of direct flights to the United States, a very obvious and real concern for the subject matter. The Finnish Presidency, I cannot remember if there is a direct flight between Helsinki and the US, maybe once a week or something.
Ms Verkleij: I do not think so.
Mr Faull: A big country and a small country and so on, one can think of all sorts of ways of characterising the Member States. Perhaps, surprisingly, it does not make much practical difference to our work. They are highly professional, they put good teams of people on the case, it reflects a wide range of government departments: we have had foreign ministry people, interior ministry

people, justice ministry people, the embassies on the spot in Washington have been very helpful in all cases, so it works well. If you are asking me whether more broadly the Commission is in favour of the ideas expressed in the draft Constitutional Treaty about the way the Presidency of the Union should be executed, well, of course, the Commission is in favour of the Constitutional Treaty signed by all Member States but not yet ratified by all.

Q183 ***Chairman:*** This is quite a difficult question to answer, but do you expect the Portuguese Presidency to have this subject high on their agenda?
Mr Faull: We were in Lisbon recently to start preparing for the Portuguese Presidency and they were very keen that this be settled by the end of June but, of course, they said, as one would expect, if that were not the case they would do their very best to bring it to fruition. They would like to see it out of the way under German Presidency.

Q184 ***Lord Teverson:*** We have the US and the Canadian Agreements, are we likely to have a whole string of these agreements because the principle having been set, that the EU negotiates on behalf of all its airlines, then are we going to have a Brazilian Agreement at the end of the day? Certain countries like China or Russia might be more—
Mr Faull: They do not have PNR systems as such. The one country keen to negotiate an agreement with us at the moment is Australia, and we will come to Australia I hope in the not too distant future. The real problem at the moment is the United States and we will do that first.
Lord Foulkes of Cumnock: When I went in to Australia they asked if I had a criminal record and I said I did not think it was still required!

Q185 ***Chairman:*** Can I ask you one final factual question, do you know how many people there are on the no-fly list?
Mr Faull: I do not offhand.

Q186 ***Chairman:*** Really my question is whether you know it rather than how many there are.
Mr Faull: I have seen it. The latest figure I have is 30,000.

Q187 ***Baroness D'Souza:*** 30,000?
Mr Faull: 30,000 entries on the no-fly list.

Q188 ***Baroness D'Souza:*** That is far more than I thought.
Ms Verkleij: But they have different lists.

Q189 ***Chairman:*** Is that public knowledge? Is it usable?
Mr Faull: Can we check that?

Q190 ***Baroness D'Souza:*** When you say there are different lists, what do you mean by that?
Ms Verkleij: They have a watch list, a no-fly list, which contains the names of those people who are considered terrorists.

Q191 ***Baroness D'Souza:*** That would be completely independent of PNR?
Ms Verkleij: Yes, it has nothing to do with PNR.
Mr Faull: It has nothing to do with PNR but PNR are checked against it.

Q192 ***Baroness D'Souza:*** But do we know the size of the watch list?
Ms Verkleij: That was what it was at the time, it changes every day.

Q193 ***Baroness D'Souza:*** You are giving me no-fly, but the watch list, does that automatically mean no-fly?
Ms Verkleij: Yes, normally the two are used together but they have a second list and that list contains the names of people who are considered to assist terrorists.
Chairman: Director General, thank you very much indeed.

Memorandum by Mr Peter Hustinx, European Data Protection Supervisor

The EDPS would like to focus on the following elements, taken from the list of issues in the request for evidence:

1. On the position to be adopted by the Commission in the coming negotiations with the United States on a new agreement.

- It has to be kept in mind that according to Article 24 of the EU-Treaty, the Presidency of the Council is the primary negotiator, assisted by the Commission.
- The objective of the negotiations should be: a long-term agreement that applies throughout the European Union and that ensures the privacy of the citizens as well as their physical security.
- A clear and adequate legal framework is needed, in order to provide EU citizens with a satisfactory level of legal certainty. This includes remedies before a court. Such a legal framework also benefits to the legal certainty of the airlines. It clarifies their obligations.

22 March 2007

— An agreement with the United States can only be concluded after an a priori assessment of the necessity, effectiveness and proportionality of the transfer of the data.

2. Whether the existing agreement with Canada can (with a change of legal base) be used as a model.

— On earlier occasions, the EDPS as well as the Article 29 Working Party approved to the agreement with Canada. Indeed, this agreement could serve as a model.

— An attractive element of the agreement with Canada is that it covers different types of passenger data: not only PNR but also API-data (Advanced Passenger Information system: the data from the machine readable zone of passports).

3. Whether the EU has any realistic prospect of securing agreement on any provisions which the United States authorities are reluctant to agree.

— According to the EDPS, this is not a right question to pose. It wrongly suggests that the EU is the weaker party in the negotiations with the US. It has to be kept in mind that the background of the agreement is a request of the government of the United States to receive information, originating from the territory of the European Union.

4. On the weight to be given in the negotiations to the views of the European data protection authorities.

— The EDPS has presented his views on the negotiations mandate (not in a public way, not to harm the negotiations).

— The Article 29 Data Protection Working Party, in which the EDPS actively participates, is working on a strategic approach in order to give an effective input to the negotiators. An essential part of this approach is to start the dialogue with other EU-stakeholders. It aims to find a liaison with other important interests and find common ground within Europe with politicians, policy makers, law enforcement and the private sector (mainly airlines).

— It goes without saying that the EDPS expects that the views of the data protection authorities, as they are being developed in this way, are given weight.

5. Whether the provisions of the agreement are to be binding on the parties, or whether the United States authorities are to be able to give a unilateral explanation of how they intend to interpret them.

— It is crucial that the provisions of the agreement are binding on the parties (in particular the US). Otherwise, the protection of the privacy of the EU-citizen can not be effectively guaranteed.

— In itself, there is no objection to the United States authorities giving a unilateral explanation of how they intend to interpret the provisions, as long as this does not affect their binding nature.

— On several occasions, the EDPS has expressed doubts whether the Undertakings of the Department of Homeland Security Bureau of Customs and Border Protection—attached to the 2004 Agreement with the United States—are legally binding and could be effectively invoked by citizens before a court. However, there are no doubts about the importance of an instrument like the undertakings as such, precisely describing the obligations of the parties.

— The binding nature of the agreement on the parties must be laid down in clear and precise wordings, but this is as such not enough. The agreement should also foresee in a mechanism to effectively monitor if the obligations are complied with. The instrument of a Joint Review, part of the 2004 Agreement, has proved to be helpful in this respect.

28 February 2007

Examination of Witnesses

Witnesses: Mr Joaquin Bayo Delgado, Assistant European Data Protection Supervisor, and Mr Hielke Hijmans, Legal Adviser, EDPS, examined.

Q194 ***Chairman:*** Welcome, Mr Bayo Delgado and Mr Hijmans. Thank you very much indeed for coming to give evidence to us. We are on the record now but if at any point you want to go off the record, as indeed we did in the last session, you are very welcome to. As you know, we are conducting an inquiry into the Passenger Name Record and I propose to give half an hour to this subject. I will try and preserve order but with this very lively Committee it is quite difficult but, nevertheless, I will try to do it. I wonder whether very briefly you would like to introduce yourselves. Before you do, can I ask you to convey our greetings to Peter Hustinx who has given evidence to us in the past and has been a good friend of this Committee.

Mr Bayo Delgado: I will. Thank you for inviting EDPS to give evidence. I am Deputy EDPS and I am pleased to be here. Mr Hijmans is one of our legal advisers in the office and he is a specialist in the two areas on which you want evidence about, so we thought it would be a good thing to have him here. For certain detailed or technical aspects he can be of help to all of you.

Q195 ***Chairman:*** I should have said, we would like to thank you very much for the very helpful written evidence which you have given us on both subjects. Perhaps I could open on PNR. In these negotiations there are likely to be requests by the United States for more data elements to be made available. You and the Article 29 Committee have said that the 25 elements in the Agreement with Canada should be enough. Can you say which of the existing 34 data elements you think should and could be removed?
Mr Bayo Delgado: You can imagine that we could discuss specific elements but I would like to focus on the main element, which is indeed an item that is not in the Canada Agreement and has a lot of meaningful aspects. This is specifically the item labelled, "general remarks" which, in fact, is an open text. In the negotiations this gave a lot of problems to the European data protection authorities because this open text allows any type of comment.

Q196 ***Chairman:*** Can you give us some examples?
Mr Bayo Delgado: For example, if in this open text it says a specific food, halal food, or any comment which the person who is introducing the record thinks is relevant, it can really touch on what are defined in the Directive as sensitive data and this is quite a concern for the European data protection authorities.

Q197 ***Chairman:*** It is described as general elements, is it?
Mr Hijmans: It is good to know that this PNR data has everything you would register when you book a flight, either with a travel agency or through the internet, so everything you put on your special wishes on your flight can be kept.

Q198 ***Chairman:*** They are described as what, as general elements?
Mr Bayo Delgado: As general remarks.
Mr Hijmans: There are two others items which, in fact, have the same effect in that they are not just a yes or no but they give the client as well as the travel agency the possibility to add something.
Mr Bayo Delgado: A whole system of filtering that data was put in place because, of course, you have to avoid too wide access to this sensitive data, but you could imagine that the filtering of those data is very difficult because you never know what will be there, so filtering open text is difficult. This is special and meaningful too in the context of the so-called pull system. You know that the American authorities pull the data, the data are not being pushed by companies to the United States, so that means the filtering aspect is also important. In fact, in the Joint Review of the Agreement, the only one which has been done, this was an issue which was analysed quite a lot to make sure that this filtering was taking place in an effective way.

Q199 ***Baroness D'Souza:*** Would you agree that the more information which is collected and recorded the easier it would become in time to eliminate certain people and, therefore, make it easier for travellers generally, but particularly business travellers?
Mr Bayo Delgado: No, certainly not. To be very precise, no, because I think this reasoning is contrary to all data protection principles. If you have got a huge amount of data, then the risk of inaccuracies, the risk of others matching this data which has been introduced is very problematic. Of course, a huge amount of data is not needed for the purpose of what it is required, so to my mind this would be excessive. Of course you can also look at what has been called the "positive profiling", that would be people who are profiled positively, because they do not represent a security risk. However, things are not so easy because, first of all, this type of positive profiling means, in fact, that you have got the risk of identity thefts and you would have to produce a system also to make sure that those who are positively profiled are the people they are supposed to be.

Q200 ***Baroness D'Souza:*** Would you not agree though in that context, it is argued by many, that the more data stats you have got the less the likelihood is that you will have false identities?
Mr Hijmans: Why?
Baroness D'Souza: I agree with you, but it is said because of the matching.

Q201 ***Lord Foulkes of Cumnock:*** Can I follow up on this because Lady D'Souza and I had a discussion about this on the way over. Surely the more information you get the more accurate your identification is. Supposing, for example, which happened to me with my car licence, my name was spelled wrongly with an "a" instead of an "o". All the other information coming together would say, "Hey, wait a minute, this chap is the fellow who lives at this address, that is his date of birth, therefore it is George Foulkes", even though it is spelled wrongly, so that makes it much more accurate, that seems to be obvious. Can I give you another example. If you are trying to find a location then you get directions and different ones, so you get two directions and they cross, you get three and

they cross, you get four and they cross, 15 cross and then there is one which does not, that is the one that is wrong because all the others are pointing in the right direction, so you get a much more accurate identification of the exact person.
Mr Bayo Delgado: It is true that the more data you have, the more accurate identification you have, that is obvious because of what you said, but that is not the issue at stake in this case. You have to take into account that the amount of data which are gathered is not precisely to identify only. The gathering of these data has many other purposes for security reasons. Therefore, if you have excessive data you are going beyond what is necessary for the true purpose of the gathering of data, which is not only identification but you may profile people in a discriminatory way, you could have possible inaccuracies, et cetera. From the identification perspective you are right, but I do not think these are identification issues. The main one is what do you do with all the data which have been gathered, and then with those data the authorities try to guess other types of implications, not so much identity but intentions, terrorist intentions, et cetera.
Mr Hijmans: It is good to understand that the gathering of PNR data by the United States is not so much for the identification of the person because they would not need these data because everyone has their passport data, which is called API data, as you know, so it is more to combine all kinds of information.

Q202 ***Chairman:*** To cross-check.
Mr Hijmans: Yes, and then of course if you cross-check it is useful to have more data because cross-checking is easier but, also, the risk from the other side to abuse the data, to secure it, it has all kinds of risks, mainly because if you combine all kinds of data about people you get to know things about people which go far beyond the purpose.

Q203 ***Baroness D'Souza:*** Is there a greater risk of error?
Mr Bayo Delgado: I think so and also you have to bear in mind that this gathering of data is done in a way which is not transparent as to the use of that data, therefore I think errors are more likely to happen.

Q204 ***Chairman:*** The rather shocking case of the Canadian, Maher Arar, who was taken to Syria and spent a year there, what went wrong in that case? Do we know? Why was he misidentified?
Mr Hijmans: I do not know.

Q205 ***Chairman:*** Is it known?
Mr Hijmans: It is not known in any case.

Q206 ***Lord Foulkes of Cumnock:*** On the data retention periods, we have been exploring the three and a half years and we found out that was the result of negotiations. The Americans have a period of 40 years. Why does there need to be a fixed period, or would 70 years not work? Why would it create any problems for you?
Mr Bayo Delgado: Again, this is a question of focusing on the purpose of that data. In fact, in our mind the three and a half years are already excessive, but it came to be like this because the period was first agreed and when you are negotiating, of course, you come to a term which is something in between. Again, here, the aspect of data retention has a lot to do with what we were saying before, there are problems with such a long period, if we are talking about 40 years or even more, as you mentioned. Why? Because, for example, the security of the data, to keep the data in a secure way, poses a tremendous problem if it is not decided to keep the data for a short period rather than a long period. Secondly, the more data you have which belongs to the past, old data, the accuracy of the data, which is one of the principles of data protection has to be warranted and it is difficult to warranty the accuracy of data which goes back years.
Mr Hijmans: If you think about yourself, if it is about your flying behaviour on a flight 20 years ago, would you remember what happened 20 years ago? Would you remember exactly what happened on that date, at that moment?

Q207 ***Lord Foulkes of Cumnock:*** That does not matter. I can understand, you are data protection officers and you are looking at it absolutely rightly and professionally, but can I ask you to put yourself in the position of a counter-terrorist officer. You know we have experience in Britain, particularly, of Muslims who are sleepers, who are there not doing anything for many years, maybe ten or even longer. Their pattern of movement around the world, between Pakistan and Britain, back to Pakistan, to Afghanistan, to Iraq or wherever, could be absolutely vital in identifying terrorists but we may need to keep it for more than three and a half years. Is that not vitally important? As citizens, as opposed to data protection supervisors, do you not think that is an important thing which needs to be done?
Mr Bayo Delgado: It is important to take all proportionate measures to make things more secure and have parameters, but I have doubts that this way of thinking of saying, "Let's keep data for as long as we can, endlessly with no limit", really gives you the results which you were suggesting. I am not so sure that this is the case for the reasons we have already mentioned. There is enormous disproportion between the effectiveness of that long

period of retention and the results of that retention, it is absolutely disproportionate.
Mr Hijmans: The amount of data you need, the amount of data you have to gather and the amount of data you have to secure for a "maybe", and of course it is true there is always the possibility that once you find someone who travelled 15 years before between Pakistan and Afghanistan, several times up and down, there is always the possibility you will find someone. On the other hand, the amount of data you will need to check all movements of all people around the world and the risks with that for not only data protection officers but also for citizens are large.
Mr Bayo Delgado: You will always have the problem of N number of years and N-plus one will always be the one which is missing, so we have to put a limit on it.

Q208 ***Earl of Listowel:*** What are the main differences in the Data Protection Framework between the US and the European Union? What role have these differences played in previous negotiations, and how are they likely to influence the current ones?
Mr Bayo Delgado: The first thing we should point out is that data protection in the European Union is seen as a fundamental right and it has horizontal legislation on it, not only covering the private sector but also the public sector, so it is common legislation with general principles. The concept in the United States is quite different because legislation is only in a specific sector for a specific data processing aspect, so there is no such general overview of these principles. Another important thing that I want to underline as a difference is that one of the basic elements of the conception of data protection in the European context is specifically the existence of an independent supervisory authority. I think this is crucial and is one of the key elements of how we understand these fundamental rights, which is not the case in the United States. This conception is not like this which is also a difference when comparing the US and Canada. In Canada you have such an independent authority, so that is very important to underline in this respect.

Q209 ***Chairman:*** Surely the principle of freedom of information is almost more important in the United States than in Europe, is it not?
Mr Bayo Delgado: We also have this idea of freedom of information. Indeed, the perspective EDPS takes on this is an approach which combines the two possibilities.

Q210 ***Chairman:*** The availability of intelligence information, for instance, in the United States under the Freedom of Information Act goes far wider than anything in Europe, does it not?
Mr Bayo Delgado: Yes. It is true that the conception is also different in this respect and this is the perspective also that is taken in this area of what we call "the right of access" of the individual concerned. The right of access is seen from the perspective of freedom of information in American law. Also, if I were to resume in a word what the more crucial aspect is, it is the need for proportionality. In the European conception many of the principles relate to the idea of proportionality and we have already referred to this idea, the data retention periods, the amount of data which has to be gathered, they have to be proportional and non-excessive to the purpose they are collected for. This is something which is crucial and, therefore, when we have dialogue with our American partners we have common grounds of legal understanding, but when it comes to data protection, these are substantial differences in the way we see things and this is a fact, which it has been and will remain.
Mr Hijmans: With this PNR Agreement, the most important thing is the fact that that under European Community law, or at least under the law of the Member States, it is an essential part of data protection that you also have protection against the national government, the national law enforcement agencies, who want to know information about you. Of course, there is no protection that they cannot enter a database but there are certain safeguards. In the US, privacy rights, data protection rights, do not apply in general terms vis-a[acute]-vis intelligence and police.
Mr Bayo Delgado: Here again we come to proportionality, there is not this idea of being proportional.

Q211 ***Chairman:*** The difficulty of proportionality is when you come to define the proportions.
Mr Bayo Delgado: Exactly. That is always the case. These concepts which are very difficult to define are always problematic, but that does not mean they do not exist and they have to be applied.

Q212 ***Lord Marlesford:*** In September 2005 when you carried out a joint review in monitoring the 2004 Agreement did you feel that you got sufficient information to be able to do it properly or were you limited by security considerations as to what you could see? If so, did this matter in terms of the effectiveness of your review?
Mr Bayo Delgado: The first thing I should clarify is that this joint review was conducted by a team in which data protection authorities were involved. The EDPS did not take part among those authorities. The competence of the authorities who were involved was to supervise the data protection

rules in the Member States, so they took part in this review and we have the information which has been published and explained by these authorities. It seems that they were reasonably satisfied with the facts they got, although if you analyse the report then you could find some aspects which could be there. I want to emphasise two things on this: first of all, this review is fundamental, the fact that a mechanism of revision has to take place periodically is fundamental because it is the way to make sure that things are going the way they should go. Secondly, there has only been one review at this point and the second one has not yet been scheduled, so that is something to worry about. In any case, in a future agreement this mechanism should be present even with problems if they should exist, but the mechanism has to be there, it is crucial.

Q213 ***Lord Teverson:*** We have been told on occasions that travellers who are not US citizens are not covered by the US data protection laws but can apply under the freedom of information laws if they want to know how their data is being used. First of all, I would be interested to know whether you agree that is how you see it but, also, is that an effective means of redress, and are there ways of challenging the misuse of data by US authorities? This is talking about us as individual citizens who want to have an issue about that data with the United States?
Mr Bayo Delgado: In fact, you are right. I am not an expert in American law and I am not supposed to be, but I think it is the citizens and residents who can apply the freedom of information law to get this information. I do not think this is enough for the citizens, the key issue is not enough, because we are talking about getting the information but when you get the information about your data being processed imagine that there is something to be rectified, so the problem does not end with the possibility of accessing the information, it goes beyond the access of information and this is what causes problems. It is true that in the Undertakings there is mention of the possibility of rectifying data which are not accurate but for an EU-citizen who goes to the US it is difficult to imagine how he will go through all this somewhat cumbersome system to get the information on his data. Then if he thinks those data are not accurate and he wants them to be deleted, for example, it is doubtful that he will be able to do so.

Q214 ***Baroness D'Souza:*** There are agencies that can do that but it is a question of how long it would take.
Mr Hijmans: Also, the European agencies could play a role in it as well. As a European citizen you could go to your national data protection authority and they would help you. In fact, you can also go to the CBP, the border authorities of the US, and you can ask for rectification but it is mainly what is foreseen, which is not the best system. You would go to the administrative authority but there is no judicial review on it, what we would always have in our countries is a judicial review of the Decision.
Mr Bayo Delgado: An important aspect to add, with our parameters is that the limitations, the exceptions to this right of access and this right of rectification, we think they have to clarify in which cases these can be the exception to the general principle of giving this information. In the present situation it is very vague as to which cases it can be denied. If you combine this possible denial with this lack of judicial recourse, then for the citizen it is difficult to act in a reasonable way to have his right.

Q215 ***Chairman:*** I think we ought to move on to our next inquiry but, on behalf of Lady D'Souza, can I ask one quick factual question? Do you know how many complaints have been referred by the European information commissioners?
Mr Bayo Delgado: We do not have figures but my guess is very few. It is no wonder why it has been like this for the reasons I have mentioned, and because of the situation of a citizen who wants to go to the US, you can imagine that these figures are, I would not dare say how many, in any case few.
Chairman: Thank you very much indeed for that.

Written Evidence

Memorandum by the British Air Transport Association

The British Air Transport Association (BATA) welcomes the opportunity to submit evidence to the Committee's inquiry.

BATA is the trade association for UK registered airlines. Our members cover a wide range of airline services and produce over 85 per cent of UK airline output.

Current Position

1. A number of UK airlines provide Passenger Name Record (PNR) access to US Customs, Canada Border Services Agency and Project Semaphore in the UK.

2. At present US Customs "pulls" PNRs ie they have direct access to reservations systems. In line with the present EU/US agreement, moves are being made to replace the 'pull' system (where PNR data is pulled by the requesting authority) with the 'push', (where it is pushed by the carrier).

3. The EU/US Agreement allows for US Customs to operate an "ad hoc push", ie in addition to four scheduled "pushes" per flight, US Customs can request PNR data at anytime. This is delaying the cutover to push as it is not clear how the ad hoc push will operate. The US has access to all data within the PNR.

Preference

4. BATA would prefer to see a 'push' model operated. Not only does this meet the wishes of the EU data protection authorities, it provides an advantage to the carrier in that carriers have some control over costs.

Costs

5. At present, with the exception of Project Semaphore, all development and transmission costs are borne by carriers. BATA believes that the costs of providing the data should lie with the requesting control authority and that this should apply to the UK e-Borders programme.

Current Agreement

6. The current EU/US Agreement is fairly ambiguous in what it requires in terms of the mechanism for providing data and there is much debate between carriers, the Commission and the US on whether a 'push' solution is mandated, whether an 'ad hoc' mechanism is required, and when this needs to be implemented.

Value of PNR Data

7. Carriers in general feel that PNR data is so sketchy at times that it is of limited use to the authorities. However, in the UK, e-Borders would argue that they have successfully used PNR data to identify criminal activity through the Project Semaphore trials, directly resulting in arrests.

US Requirements

8. An Annex was attached to the back of the Agreement which stated that the US required access to all data, at any time. By attaching this to the Agreement, we have never been clear on whether this is officially accepted by the EU.

9. We are also concerned that the US requirements include departure control data (bag tags and seat numbers) which are not available from the reservations systems. The US has also requested frequent flyer information which is held in completely separate systems.

EU Position—"Push"

10. BATA members understood, after meeting with the Commission, that they needed to change the process from "pull" to "push", in order to meet the requirements of the Agreement, or would otherwise be exposed to legal action from passengers regarding the way data was provided.

US Position—"Pull"

11. The US wish to retain their current mechanism for obtaining data (a data "pull"). However, the EU feel that this does not afford adequate protection as data is freely available, is not filtered and is not restricted to relevant flights. This means that we are trying to implement a solution that the US does not really want, and hence it is difficult to progress with clarity on how this should work. Any new Agreement needs to clearly resolve these issues and provide adequate time for compliance.

Canada—single "Push"

12. We would prefer to see a similar approach to the one adopted by Canada, which defines a single "push" of data at departure and places far less burden on the airlines than the four "pushes" required by the US plus a mechanism for obtaining additional "ad hoc pushes" on request.

Summary

13. To summarise, BATA feels that the following is required:

- clarity on the mechanism for providing data;
- a batch mechanism only, with no "ad hoc" requirement;
- a restricted set of defined data items, that are available in reservation systems;
- a restricted number of data accesses to keep costs to a minimum;
- adequate protection to ensure that carriers are not exposed to legal action through data protection issues;
- an agreed implementation timescale to allow for system development; and
- an agreed global standard on PNR data provision.

March 2007

Memorandum by Department for Transport Aviation Directorate

1. The Department for Transport Aviation Directorate has actively engaged in the negotiations on the EU/US PNR agreements and similar negotiations with Canada. The Department's aim has been to ensure that such regimes are clear, robust and proportionate; that air carriers have legal certainty about their obligations both in the EU and the US; and that transatlantic air travel is not disrupted. In this work, the Department also appreciates that there are important data protection, privacy and security interests, and so works closely with the Department for Constitutional Affairs and the Home Office to ensure that these are taken into account.

2. Led by the United States, sovereign states wishing to protect their borders are increasingly exercising their perceived legal right to place statutory requirements on transport operators to provide advance information about intending passengers. The operators typically face heavy fines, prosecution and/or the diversion of their craft (at considerable cost to them) if they do not comply. However, the collection and supply of such data through reservation and departure control systems raises legal data protection concerns. The Department has, therefore, been anxious to ensure that a robust EU-level agreement is in place that sets out the terms of the data transfer, and to ensure that it complies with UK and EU data protection law. Otherwise there is a risk that air carriers could be in breach of US law if they do not transmit the data, and other relevant legislation, if they do.

3. If this situation arose it would cause considerable uncertainty and disruption to UK-US air travel, which forms the biggest international market for UK airlines with 18 million passengers carried a year between the two countries. Anything that would disrupt this traffic flow would inconvenience many passengers, would be seriously harmful to UK aviation interests and would be very damaging to the wider economy.

4. The Department is also working with air carriers to raise awareness amongst passengers of PNR data requirements, and to explain the basis on which data are collected and transmitted. For example, the conditions of carriage of the main UK airlines now contain references to the PNR requirements; this additional information to passengers about how their data will be used is helpful in complying with the data protection principle that data must be processed "fairly". And their on-line booking processes now allow passengers to enter the data directly, and to give their consent to the transfer.

5. Our objective in the forthcoming negotiations will be to ensure that this balance between security, data protection and minimising disruption to traffic is maintained.

6. The Commission's position, as set out in the proposed Council mandate, is therefore acceptable to us, although we would have preferred the mandate to include wording about the cost to airlines of providing the data. We raised this at an EU level, but it was not included in the final text.

7. The existing EU/Canada PNR agreement could be used as a model text with a change of legal base. But it makes sense to use the current EU/US agreement as the starting point for negotiations.

8. We have been asked to comment on the sanctions that the US could employ if PNR data is not transmitted, for example if the UK is unhappy with the conditions under which it will be used. The US authorities have sanctions, in the form of fines, available to them if airlines do not provide PNR data as required. If an airline continuously failed to provide PNR data the US could suspend the airline's permission to operate in the US. US operating permits, like the UK's, are conditional on airlines abiding by US law.

9. Our view is that the best way to ensure acceptable standards of data privacy is to engage constructively in EU-level negotiations with the US to ensure that the Department of Homeland Security provides appropriate safeguards concerning its use of PNR data. An attempt to link data transfer to landing rights in Europe in a negotiation with the US almost certainly would not receive any support from member states. It is also likely to be in breach of the member states' obligations under the Chicago Convention which governs international air transport, and their individual air services agreements with the US. And any restriction on US airlines' ability to operate to Europe would result in reciprocal restrictions on EU airlines. As was made clear at the start of this evidence, one of DfT's aims in its involvement in the EU/US PNR agreement is to avoid such disruption to aviation traffic.

March 2007

Memorandum by the Information Commissioner

1. The Information Commissioner has responsibility for promoting and enforcing the Data Protection Act 1998 and the Freedom of Information Act 2000. He is independent from government and promotes access to official information and the protection of personal information. The Commissioner does this by providing guidance to individuals and organisations, solving problems where he can, and taking appropriate action where the law is broken. The comments in this evidence are primarily from the data protection perspective.

2. The Commissioner has been involved in the data protection issues arising from the transfer of airline passenger data from the EU to US authorities for their own purposes from the time that the US authorities first imposed such a requirement on UK airlines. His work in this area has primarily been in the context of his membership of the Article 29 Working Party established under the EU Data Protection Directive and consisting of the national data protection authorities of each EU member state. Given that the issue affects personal data held by all airlines flying from EU member States to the US, an EU wide solution to the problem has always been seen as the most effective approach. Annex 1 provides a full account of that involvement including the data protection issues that arise and the various solutions that have been adopted.

3. At the heart of data protection concerns is the need to balance the legitimate interests of states to control who enters their own territory and ensure the safety of their own citizens and visitors with the need to ensure that this is undertaken in a manner consistent with necessary data protection and privacy safeguards. This has centred upon whether the arrangements put in place amount to an adequate level of data protection. Key data protection concerns focus on the following areas:

- A proper legal basis for requiring the information.
- Minimising the data transferred to that strictly necessary and avoiding sensitive personal data such as information on religious beliefs.
- Limiting the purpose for which the data can be used to areas of pressing need.
- Limiting wider disclosure to where strictly necessary.
- Appropriate retention periods guaranteeing that data is only kept for the minimum period necessary.

— Transparency for passengers though adequate information when they book flights.

— Redress for individuals if problems occur and their right to access information held about themselves.

— Appropriate security to safeguard against unauthorised access.

— Appropriate technical solutions for the transfer of data (a "push" system of airlines sending the necessary data rather than a "pull" one where the US authorities gain access to reservation systems and draw down the information they require).

— Effective inspection and review mechanisms to ensure safeguards are being applied in practice.

4. The Commissioner and his colleagues on the Article 29 Working Party have always worked together to try to ensure that the agreements signed between the EU and third countries such as the US have these essential safeguards in place. They are keen that any new agreement with the US should be negotiated on the basis that safeguards will be included to ensure that all the matters listed in paragraph 3 above are addressed. In particular there should be no reduction of the level of protection afforded by the current arrangements.

5. The Article 29 Working Party has made clear that an agreement with the US at EU level is preferable to bilateral agreements between the US and particular member states. An EU level agreement will help ensure a consistent and harmonised approach to personal data protection. The Working Party has already identified key areas where attention should be paid during negotiations on a new agreement (WP 122).[1] These are:

— At the very least, the preservation of the current level of protection and the further integration of the US undertakings into the agreement itself.

— Taking account of the previous opinions of the Working Party. These include the need to reduce the number of specified data items collected to those that have proved of true value based on experience.

— Mandatory use of a "push" system now that technical arrangements are in place (the delays in moving to a push system are of major current concern to the Working Party as the appropriate technical measures now appear to be available but a "push" system remains in place with the airlines and the US authorities holding each other responsible for the failure to move to a "push" system).

— Strict purpose limitation to ensure that data is only used for the limited purposes for which it was transferred and also that it is not transferred subsequently to third parties for wider unconnected purposes.

— Continuation of the annual joint review mechanism to help ensure compliance with the specified safeguards.

6. The Commissioner and his EU counterparts have noted with concern that mechanisms provided for at paragraph 7 of the Undertakings for consultation by the US with the EU on the expansion of the data items appear to have been used in practice as a basis for unilateral declaration by the US side of their intention to expand the items. This is not what the Commissioner and his counterparts envisaged by a consultative arrangement. (Exchange of letters between the US DHS and EU expanding data elements to include further frequent flyer information-2006/C259/01 & 02).

7. The Commissioner and his EU counterparts are concerned to ensure that the safeguards in any agreement are complied with in practice. As mentioned in paragraph 5 above, the continuation of the annual joint review mechanism is an essential safeguard that will help ensure compliance with restrictions such as those on wider use. One joint review took place under the previous arrangements and the continued delay in undertaking a further joint review can only undermine confidence that the safeguards are effective. The concerns that some have expressed that EU PNR data may be used outside the terms of the current undertaking, in that it is processed on the US "Automated Targeting System" could more readily be addressed if timely reviews were to are take place.

8. The Commissioner and the Article 29 Working Party believe that as international air transport operates on a global basis, a global solution to the PNR issue is desirable. An instrument established under the auspices of the International Civil Aviation Organisation (ICAO) could set out a common set of data items and procedures that all states could follow. This would be preferable to each state specifying its own requirements and then concluding an ever increasing number of bilateral agreements. Achieving a common international instrument with appropriate data protection safeguards would ensure a consistent approach and reduce confusion for airlines and passengers.

[1] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp122_en.pdf

9. The different approaches taken by individual states are already apparent. The agreement concluded by the EU with Canada in response to their demands for EU PNR data is a case in point. This differs from the US requirements in a number of respects. An obvious example is the data items required. There are 34 in the case of the US and 25 in the case of Canada. Furthermore with Canada the "general remarks" text fields are excluded. This appears to be a more proportionate approach to the problem. The Article 29 Working Party concluded that the arrangements put in place did amount to an adequate level of data protection as compared with the US where, in their view, they did not (WP103).[2] Other significant factors included the mandatory use of a "push" system and the existence of an independent data protection supervisory regime in Canada.

10. The Commissioner and his EU colleagues are eager to help inform the forthcoming negotiations with the US on a new agreement by providing advice and assistance. The Article 29 Working Party has established a dedicated PNR sub group to work on passenger data issues in which the Information Commissioner's staff participate. The sub group, on behalf of the Working Party have organised a workshop on PNR issues on 26 March in Brussels to help inform the forthcoming negotiations. A wide variety of participants and speakers have been invited including the Chairman of Sub Committee F. The sub group has worked in close cooperation with the European Parliament's LIBE committee who are also organising a connected event.

11. The Information Commissioner believes that it is vital that as states seek to protect their citizens from terrorist and other criminal acts they adopt a considered and proportionate approach to the collection and processing of personal information. The acquisition and retention of a wide range of personal details, many of which prove to be of no more than marginal value, only serves to undermine public confidence. There is risk that excessive data collection and use will start to erode the very freedoms that the states are seeking to protect. The Commissioner believes that the twin pubic policy objectives of public safety and data protection are reconcilable and should be achievable in any agreement concluded with the US authorities.

Richard Thomas

5 March 2007

Annex 1

THE INFORMATION COMMISSIONER'S INVOLVEMENT IN THE EU /US PASSENGER NAME RECORD AGREEMENT

1. Background

Airlines operating scheduled air services record what is known as passenger name record data (PNR) on passengers who make reservations on their flights. These records are usually maintained on central shared customer reservation systems (CRS) operated by third parties on the airlines' collective behalf. Most prominent of these in Europe is Amadeus which most European airlines use. This contains records relating to the fights of participating airlines and can be accessed and updated by the airlines and third parties such as travel agents who can create and amend records when dealing with a passenger's reservation.

The PNR contains a variety of information about passengers ranging from flight details, method of payment, dietary preferences and free text information containing general remarks. In addition to the PNR airlines create what is know as APIS data when a passenger checks in. This is held on the airline's own departure control systems(DCS).

In the aftermath of 9/11 US authorities realised the potential security benefits of having prior notice of passengers arriving in their territory to enable them to check against watch lists and undertake passenger profiling. The data held as PNR was seen as particularly valuable. The US Government passed a legal statute (Title 49 United States Code section 44909 © (3) and Title 19 Code of Federal Regulations section 122.49b). This required each air carrier operating passenger flights to or from the US to provide US Customs and Border Protection (CBP) with electronic access to PNR data to the extent that it is collected and contained in the carrier's automated reservation and departure control systems. Airlines failing to comply with the US requirements faced sanctions ranging from delays in offloading passengers, through to substantial fines and ultimately denial of landing rights.

[2] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp103_en.pdf

2. Data Protection Issues

PNR details of airline passengers are personal data within the meaning of the EU Data Protection Directive 95/46/EC and the UK Data Protection Act 1998. At the heart of data protection legislation are standards that must be followed by those who process personal information about individuals. These provide safeguards to ensure that individuals' personal details are handled correctly and in appropriate ways. The principles, in essence, require that personal information is:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept for longer than necessary.
- Processed in line with individuals' rights.
- Kept secure.
- Not transferred to countries without adequate protection.

One of the requirements of both pieces of legislation is that personal data processed by data controllers in the EU are not transferred outside the European Economic Area (EEA) unless there is an adequate level of protection (Principle 8 -DPA 1998- Art 25&26 EU DP Directive). There are exceptions to this rule known as derogations (Schedule 4 -DPA 1998). These include circumstances such as where an individual has consented to the transfer, where the transfer is necessary for the performance of a contract with an individual or where the European Commission has made a finding that an adequate level of protection exists in the third country. The requirement by the US authorities to have direct access to European carriers" PNR records meant that personal data would be transferred outside the EEA to the US. The US, although having some laws, such as the Federal Privacy Act. which include elements familiar in data protection legislation, has no general DP law similar to the laws in place in European Union member states and now in place in many other countries around the world. The European Commission had made no adequacy finding in respect of the US. Any transfers by airlines of personal data held in the EU were therefore potentially in breach of the EU legislation prohibiting transfers outside the EEA unless there were other grounds for concluding that adequate protection existed or unless another derogation applied.

The extent of the personal data required by the US included potentially sensitive data such as dietary preferences which could reveal religious beliefs. The lack of any established safeguards for the receipt and recording of such PNR data in particular called into question whether there was an adequate level of protection in the arrangements. If airlines were therefore prohibited from transferring the required PNR details this could have led to sanctions being imposed by the US authorities including denial of landing rights.

3. Proposed Data Protection Solution

The national EU data protection supervisory authorities (the Information Commissioner and his counterparts in the rest of the EU) meet regularly together as a working party established under Article 29 of the EU Data Protection Directive. This is known as the Article 29 Working Party. The Working Party realised that there was a serious problem that needed resolving in a way that addressed legitimate US concerns about homeland security whilst at the same time respecting the privacy and data protection rights of passengers. It called upon the European Commission to look to adopting an EU wide solution (WP66). The European Commission then took an initiative based upon its powers to make an adequacy finding under the EU Directive. Once such a finding was in place airlines would then be able to transfer data to the US. The aim of the Commission was to broker an agreement with the US Government that put in place data protection safeguards in the US authorities' handling of personal data. These safeguards would then provide the basis for the Commission make a finding of adequacy.

One of the roles of the Working Party is to provide opinions. This includes a requirement to give its view to the European Commission on any proposed adequacy findings (WP78 &87). The Working Party therefore became engaged in the process of determining whether the arrangements put in place by the US for PNR data represented an adequate level of protection. Ultimately findings of adequacy are made by the European Commission. They do not have to follow the opinion of the Working Party.

Once negotiations between the US and the European Commission commenced US action against airlines for failure to implement the US PNR requirements was temporarily suspended. During the negotiations, the European Commission provided regular updates to meetings of the Article 29 Working Party. The Working Party developed a number of opinions based upon the different proposals being put forward. In doing so they

were aware that in the absence of an agreement individual national data protection authorities would have the power to take action against any airlines that transferred personal data outside the EEA. However once an adequacy finding had been made by the European Commission such transfers could take place without the risk of such enforcement action. The Article 29 Working Party was committed to the process of securing an adequacy finding but wanted this done on terms that reflected what it saw as proper safeguards as set out in its various opinions.

The process adopted by the European Commission resulted in an international agreement between the US and the European Union. This was underpinned by a binding undertaking made by US Department of Homeland Security Bureau of Customs and Border Protection. The undertaking involved US commitment to put in place restrictions and safeguards that would ensure an adequate level of protection.

The undertaking provides restrictions on:

— the purposes for which PNR data can be used in the US (essentially terrorism, serious crimes of a transnational nature and flights from warrants).
— the number of PNR items to be accessed.
— accessing sensitive data.
— use of a pull system of access to PNR data.
— retention periods.
— access by third parties.

The undertaking also provided for security measures, redress for individuals, supervision by DHS Chief Privacy Officer and a joint review mechanism on an annual basis.

The Commission, having noted the Working Party's opinion proceeded to make its finding that an adequate level of protection had been secured in the undertaking. The Article 29 Working Party's position (WP 95) was that whilst substantial progress had been made on securing safeguards a number of significant areas still needed addressing. The European Parliament was consulted by the Commission as part of the process and expressed reservations over the proposed arrangements. This resulted in the matter being referred by the Parliament to the European Court of Justice.

4. The Information Commissioner's Position

The Information Commissioner was supportive of the efforts to secure safeguards in the US and to use these as the basis for an adequacy finding. However he took the view that it was at least arguable that a derogation from the need for an adequate level could apply on the basis that transfers of personal data were necessary for the airlines to perform their contacts with passengers (Schedule 4 (3) -DPA 1998). The argument behind this was that in practice an airline would not be able to fly a passenger to the US if it did not provide PNR data because the airline would suffer severe sanctions which might include denial of landing rights. Nevertheless he was convinced that an adequacy finding would prove a more effective long-term solution.In particular airlines. would have greater legal certainty and the US would have in place data protection safeguards which might not otherwise exist. Whilst the Information Commissioner shared the continued concerns expressed by the Article 29 Working Party, he took the view that the results of the negotiations with the US authorities did represent a substantial improvement on what might have otherwise been the situation.

5. Implementation and Subsequent Action

Since the implementation of the agreement, undertaking and adequacy finding further efforts have been made to ensure a proper level of data protection is delivered in the practical operation of the arrangements. In particular the Article 29 Working Party's sub group dealing with PNR issues has liaised with the Association of European Airlines (AEA) over how the arrangements work in practice as well as to expedite the technical arrangements necessary to move from a "pull" system to a "push" system. The Working Party has also developed advice to airlines on how best to inform passengers that their PNR details are passed on to the US authorities (WP 97).

One of the important data protection safeguards included in the undertaking provided by the US was an annual joint review with the European Commission. One joint review has taken place examining the practical arrangements put in place by the US to comply with the undertaking. The EU side of the review team included three members from national data protection authorities. The United Kingdom was represented. A version of the Commission Staff Working Paper summarising the outcome of the joint review has been published.

6. European Court of Justice Ruling

The reference of the international agreement and the Commission's adequacy finding by the European Parliament to the European Court of Justice resulted in a judgment issued on the 30th May 2006. The ECJ ruled that the agreement and the adequacy finding should be annulled. The annulment was founded on the Commission not using the correct legal basis for these instruments rather than any consideration of whether the measures themselves represented an adequate level of protection. The Court stayed the effect of the judgment until 30 September 2006 to give the Commission time to identify and implement a more appropriate legal basis. A failure to put arrangements in place would have once more called into question whether transfers of personal data to the US authorities complied with EU and national data protection law.

7. Current Agreement Between the US and EU

As the ECJ judgment was stayed the existing finding of adequacy remained in place for the short term. The Article 29 Working Party adopted opinions (WP122 & WP124) which supported the efforts by the Commission and Council to conclude a new agreement before the 1st October 2006. The Working Party was keen to ensure that any agreement at least preserved the data protection safeguards in the existing arrangements. They also hoped that it would take into account the previously expressed concerns. In the event a new agreement was concluded carrying forward the undertaking of DHS CBP and effectively preserving the status quo until negotiations could take place on a new long term agreement. This was on the basis of a Council Decision (2006/729/CFSP/JHA). The terms of the agreement have been clarified by an exchange of letters between the DHS and the Council Presidency/ Commission (2006/C 259/01 &02)

8. Future Arrangements

The Information Commissioner and his colleagues on the Article 29 Working Party remain committed to ensuring that any new agreement incorporates appropriate data protection safeguards and does not result in any lessening of the protection established in the current arrangements. Key safeguards sought in any new agreement include:

- Limitation of the amount of data transferred to that strictly necessary.
- Limitations on the purposes for which the data can be used including restrictions on who it may be disclosed to.
- An effective mechanism for supervising compliance with the agreement.
- Mandatory use of a "push" system removing the need for US authorities to interrogate EU airline systems.

Memorandum by Professor Paul de Hert, Tilburg Institute for Law, Technology and Society, The Netherlands, and Vrije Universiteit, Brussels, Belgium and Gloria González Fuster, Researcher, Institute for European Studies, Vrije Universiteit, Brussels, Belgium

1. One of the major challenges for the current EU data protection regime is to ensure legal certainty. A series of interinstitutional conflicts and tensions have conveyed the image of a legislator that cannot be trusted, as not able or not willing to recognise the exact scope of the provisions it aims to establish. This issue concerns especially what Advocate General Léger has called in its Conclusions the "new set of issues" related to the *"use of commercial data for law enforcement purposes",*[3] which refers both to the PNR case and the Data Protection Case.

2. From a legal point of view, however, the European Court of Justice (ECJ) has been clear in its judgement: the only factor to take into account in order to determine the scope of data processing is the nature of the processing itself, as opposed to the origin of the data. In this sense, the view manifested by the European Data Protection Supervisor according to which the judgement creates loopholes in EU legislation could be discussed. Indeed, all processing needs either to be included in the exemptions to Directive 95/46/EC, either to fall under the scope of the Directive.

3. Despite the fact that such legal *loopholes* may not exist as such, it is undeniable that the *"use of commercial data for law enforcement purposes"* could require special protection provisions, different from those currently offered under the EU third pillar. Indeed, the collection of data for law enforcement purposes as commercial data could seriously mislead the data subject and damage therefore its individual rights.

[3] See point 160 of Conclusions de l'Avocat Général M Philippe Léger, 22 November 2005 (p I—42).

4. The will to enhance protection in those cases is precisely one of the reasons that have lead some EU institutional actors to privilege wide interpretations of the data processing falling under the EU first pillar. The first pillar offers, indeed, more consistent data protection, as well as other institutional specificities such a reinforced participation of the European Parliament and a less limited ECJ role.

5. However, forced or creative interpretations of the scope of the Data Protection Directive contribute dangerously to the general lack of legal certainty already mentioned. In this sense, they do not serve the cause of effective EU data protection.

6. Currently, one of the major differences between EU data protection in the first and in the third pillar is that in the latter there is no formal requirement to declare that a third country ensures "adequate" data protection to allow the transfer of data to said country. The second version of the PNR agreement signed between the EU and the US, approved in the framework of the third pillar, is nevertheless based on a Council Decision stating that "adequate" protection will be provided by US authorities.

7. The fact that such "adequate" protection might indeed be provided is actually very strongly discussed, as well as probably impossible to prove. To the general difficulties already encountered by the EU to review such "adequacy" for US processing falling under the first pillar, need to be added the specific review limitations related to security matters (such as, for instance, the possible use of the confidentiality principle to block checks coming from external authorities).

8. If declaring that the US authorities offer "adequate" data protection is not legally required (6), allegedly not accurate and in any case subject to debate (7), the interest for the Council to provide such a statement is doubtful.

9. A very important lesson to be learned from the management of the PNR issue in the EU until now is the lack of efficiency of the European data protection Supervisory authorities in monitoring compliance with data protection law. By not taking any actions against airline companies not complying with data protection law, the data protection Supervisory authorities have shown what could be interpreted as a lack of courage. It is uncertain whether one needs to be disappointed by this. Rather it teaches us that the excellent work of the European data protection Supervisory authorities as privacy watch-dogs, may more often than one would expect, be in need of complementary political control and decision-making. To put it differently: data protection is one system of protection and action, but it would be a mistake to think that is a sufficient system on its own.

10. The credibility of the current EU data protection system has also been undermined by the so-called "SWIFT case", which also showed that serious violations of data protection law manage to escape from the supervision of the data protection authorities and finally need to be addressed at a different, political level. This can be linked to the general limitations of data protection law as legislation dominated by its procedural dimension, where priority is given to regulate inconvenient data transfers instead of avoiding them.

11. Another actor with a capital role to play in the EU data protection regime is the judiciary, at least in theory. It bears the responsibility to proceed to the ultimate check of compliance of transfers with data protection principles from the human rights perspective. In this sense, Advocate Léger's Opinion in the PNR case was dramatically unsatisfactory. It limited itself to a formal compliance check, instead of offering a strict review of the different alternatives encountered and their different impact on privacy and individual rights. In the era of continuous technology developments, the only way to judge proportionality and necessity of measures is via balancing the impact of choices.

12. Another problem to be found in Advocate Léger's Opinion in the PNR case is his non-acceptance of the capacity of the US to unilaterally modify the content of the PNR agreement. Indeed, Advocate Léger did not recognise such capacity and used the argument to dismantle part of the European Parliament's argumentation. His interpretation on the question *whether the provisions of the agreement are to be binding on the parties, or whether the US authorities are to be able to give a unilateral explanation of how they intend to interpret them* could nevertheless be different had he expressed his Opinion after the publication of the Letter to the Council Presidency and the Commission from the Department of Homeland Security (DHS) of the USA, Concerning the Interpretation of Certain Provisions of the Undertakings Issued by DHS on 11 May 2004 in Connection with the Transfer by Air Carriers of Passenger Name Record (PNR) Data. The Letter seems to significantly change the factual background on which his Opinion is based and could serve to sustain that the parties are indeed allowed to substantially review how they intend to implement the agreement.

13. Regarding the second and current version of the PNR agreement, a major aspect to be pointed out is the final provision according to which "This Agreement does not create or confer any right or benefit on any other person or entity, private or public". This explicit denial of the data subject's rights reinforces the idea that insisting on declaring that the protection provided by the US might be "adequate" is not fully convincing.

14. Concerning the question *whether the EU has any realistic prospect of securing agreement on any provisions which the United States are reluctant to agree,* it must be admitted that, if the second version of the agreement has not secured better protection than the first version, it is probably not realistic to expect any improvement in future agreements unless new approaches are adopted.

15. Concerning the question *whether the existing agreement with Canada can (with a change of legal base) be used as a model,* it needs to be noted that dissimilarities between the US and Canada regarding data protection can be considered sufficient to require totally different approaches. The most notable dissimilarity is that Canada recognises the principle of the need of independent supervision, whereas the US does not.

16. Taking into account the specificity of the use of commercial data for law enforcement purposes (3), the weakness of data protection in the third pillar (4), the apparent inopportunity of affirming the "adequacy" of the protection ensured by the US authorities (8), the limitations of the protection based almost exclusively on the supervision by data protection authorities (10) and the unclear response to be expected from the judiciary (11), it has to be recognised that there is an imperious need for the EU to establish new checks and balances in this field.

17. New checks and balances should not be expected to come from the US side, neither should the responsibility for those checks and balances be placed by the EU exclusively on the hands of the US authorities, mainly because of the lack of accountability in case of non compliance. In this sense, the regulation of the duty to inform data subjects travelling from the EU on the data processed is a good example of what should be avoided in future agreements, as the duty is exclusively regulated by the Undertakings of the Department of Homeland Security Bureau of CBP, which can be unilaterally "interpreted" by the US, and simply falls under CBP responsibility.

18. For the sake of efficiency and accountability, checks and balances need to be implemented in the EU, under EU responsibility. The fact that the processing of the PNR is to take place in the US does not mean that the EU should simply rely on the protection as promised by the US, without contributing to an effective protection inasmuch as possible.

19. In the collection of data for law enforcement purposes as commercial data, information to the data subject is essential. Information on the further processing of the data must be given for two reasons: on the one hand, to ensure the possibility of the data subject to make effective use of its rights (notably, of rectification), and, on the other hand, to raise awareness of the current reality of data transfers to the general public. Both purposes are to be interpreted as part of the progressive empowerment of the data subject, which should be in fact the main objective to be fulfilled by the provision of information under EU law.

20. The information given to the data subject should cover the exact data transferred, the moment when the transfer is expected to take place, the use foreseen after the transfer, and the exact rights the data subject has concerning the data once they have been transferred, as well as information on how to introduce requests to US authorities to use the rights recognised by the US and, suitably, contact information to EU Supervisory authorities able to offer assistance. The information should be provided at the moment of the collection, and therefore the obligation to inform should be placed on those responsible for the collection. Eventual complaints regarding costs of this measure should be forwarded to the US authorities responsible of implementing the data transfer system.

21. The monitoring of this obligation could be taken care of by data protection authorities. Due to the European dimension of the issue, the monitoring should ideally be developed at EU level, or at least there should be mechanisms to coordinate actions. A EU level coordination of the monitoring could also contribute to the collection of information on eventual problems encountered by travellers, which could be used in future negotiations with the US. The possibility of offering assistance could be particularly useful in this sense, and would additionally contribute to increasing the quality of the data provided to the US authorities. *The weight to be given in the negotiations to the view of the European data protection authorities* could in the future substantially depend on the effective role they play in providing assistance to the data subjects to make sure the data transferred to the US and processed by US authorities is accurate.

22. Better informed travellers represent not only data subjects effectively able to take benefit from the rights they have been recognised. Information is also instrumental to raise public awareness of the measures being implemented. Information is in this sense a key to the promotion of real public debate on data protection and data transfers, and therefore also an essential tool to enhance the role of parliaments.

23. On a mid term perspective, other enhanced mechanism of protection should probably be established to reduce conflictive situations in the field of global data transfers. New paths to explore could include digital watermarking, an already widespread practice in the field of digital rights management allowing the marking of digital content. In fact, all the techniques used for Digital Restriction Management should be careful examined, as they can allow the secure transfer data that will be impossible to manipulate by non authorized

parties, easy to track by the pertinent authorities and, more importantly, inaccessible after a certain number of processing activities. This could be particularly useful in the search to a solution to the question on how information given can be restricted to the use for which it is given.

24. The future PNR agreement needs imperatively to be approved only for a limited temporal application. Furthermore, it should include provisions on the elements to be taken into account for its own revision, notably:

(i) the analysis of the eventual persistent need for the transfer of data;

(ii) the examination of the practical utility of the transfers, inasmuch as demonstrated by practice;

(iii) the eventual concerns expressed by travellers, as monitored by data protection authorities;

(iv) technology developments that could improve the protection of data and/or enhance the enjoyment of individual rights related to the data transferred.

25. In conclusion, *regarding the position to be adopted by the Commission in the coming negotiations with the US,* the major concern must be to conclude a temporary agreement subject to revision, whose main objective should be to effectively increase the level of protection of the individual rights with provisions to be implemented at EU level, and therefore accountable in the EU. Information to travellers is to be seen as a key element to empower the data subjects, to which data protection authorities should provide all the possible assistance.

26. *The part to be played by the European Parliament and national parliaments* could be precisely to stand for this empowerment of the data subject, as a way to protect individual rights and promote public debate in the delicate field of the use of commercial data for law enforcement purposes.

This evidence was submitted on an individual (non corporate) basis and concluded 28 February 2007, in Brussels.

ISBN 978-0-10-401073-0

9 780104 010730

Printed in the United Kingdom by The Stationery Office Limited
6/2007 363562 19585