A REVIEW OF THE ANNEXES TO THE EU-USA PNR AGREEMENT AND RELATED PRESS RELEASE

A DATA PROTECTION ANALYSIS
FROM AMBERHAWK TRAINING LIMITED
DR. C. N. M. POUNDER, DECEMBER 2011

ANNEX I: AGREEMENT BETWEEN THE UNITED STATES OF AMERICA AND THE EUROPEAN UNION ON THE USE AND TRANSFER OF PASSENGER NAME RECORDS TO THE UNITED STATES DEPARTMENT OF HOMELAND SECURITY

THE UNITED STATES OF AMERICA

and

THE EUROPEAN UNION,

Hereinafter referred to as "the Parties,"

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

SEEKING to enhance and encourage cooperation between the Parties in the spirit of transatlantic partnership;

RECOGNIZING the right and responsibility of states to ensure the security of their citizens and protect their borders and mindful of the responsibility of all nations to protect the life and safety of the public including those using international transportation systems;

CONVINCED that information sharing is an essential component in the fight against terrorism and serious transnational crime and that in this context, the processing and use of Passenger Name Records (PNR) is a necessary tool that gives information that cannot be obtained by other means;

DETERMINED to prevent and combat terrorist offenses and transnational crime, while respecting fundamental rights and freedoms and recognizing the importance of privacy and the protection of personal data and information;

HAVING REGARD for international instruments, U.S. statutes and regulations requiring each air carrier operating passenger flights in foreign air transportation to or from the United States to make PNR available to the Department of Homeland Security (DHS) to the extent they are collected and contained in the air carrier's automated reservation/departure control systems, and comparable requirements that are or may be implemented in the EU;

NOTING that DHS processes and uses PNR for the purpose of preventing, detecting, investigating and prosecuting terrorist offenses and transnational crime in compliance with safeguards on privacy and the protection of personal data and information, as set out in this Agreement;

STRESSING the importance of sharing PNR and relevant and appropriate analytical information obtained from PNR by the United States with competent police and judicial authorities of Member States, and Europol or Eurojust as a means to foster international police and judicial cooperation;

ACKNOWLEDGING both Parties' longstanding traditions of respect for individual privacy, as reflected in their laws and founding documents;

Comment [U1]: The Agreement starts by saying that its prime purpose is to combat terrorism and serious transnational crime.

However, the term "serious transnational crime" is not found in the Agreement, other than in this preamble, it is not a defined term nor is it used by any Article.

The Agreement also covers matters that are **NOT** criminal and **NOT** terrorist related – see Article 4(2) and 4(3). These other matters are not described in the Preamble.

Comment [U2]: It would have been reassuring if the phrase "**proportionate** information sharing" was used here; it would signal that any information sharing would be a justifiable interference in terms of Article 8(2) of the European Convention of Human Rights

The use of the word "proportionate" would mean that the balance between the needs of the law enforcement authorities and the privacy protection was an integral component in any decision to share PNR data

Comment [U3]: Note the text has dropped the word "serious"; now it is mere "transnational crime" (not "serious transnational crime" as in the "DESIRING STATEMENT" above – see U1)

Comment [U4]: As we shall see, the protection specified in Articles 5-13 relates only to **PNR data** and not the other personal data that might be associated with PNR data. This severely limits the scope of the protection to the anodyne personal data identified in Annex 1.

Comment [U5]: As we shall see these safeguards are weak; there is no identifiable role for any data protection authority expressly written into the Agreement.

Comment [U6]: It would have been reassuring to see the word "proportionate" to describe the information sharing – see U2 above (e.g. "STRESSING the importance of proportionate sharing...")

MINDFUL of the EU's commitments pursuant to Article 6 of the Treaty on European Union on respect for fundamental rights, the right to privacy with regard to the processing of personal data as stipulated in Article 16 of the Treaty on the Functioning of the European Union, the principles of proportionality and necessity concerning the right to private and family life, the respect for privacy, and the protection of personal data under Article 8 of the European Convention on the Protection of Human Rights and Fundamental Freedoms, Council of Europe Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data and its additional Protocol 181, and Articles 7 and 8 of the Charter of Fundamental Rights of the European Union;

MINDFUL that DHS currently employs robust processes to protect personal privacy and ensure data integrity, including physical security, access controls, data separation and encryption, audit capabilities and effective accountability measures;

RECOGNIZING the importance of ensuring data quality, accuracy, integrity, and security, and instituting appropriate accountability to ensure these principles are observed;

NOTING in particular the principle of transparency and the various means by which the United States ensures that passengers whose PNR is collected by DHS are made aware of the need for and use of their PNR;

FURTHER RECOGNIZING that the collection and analysis of PNR is necessary for DHS to carry out its border security mission, while ensuring that collection and use of PNR remains relevant and necessary for the purposes for which it is collected;

RECOGNIZING that, in consideration of this Agreement and its implementation, DHS shall be deemed to ensure an adequate level of data protection for the processing and use of PNR transferred to DHS;

MINDFUL that the United States and the European Union are committed to ensuring a high level of protection of personal information while fighting crime and terrorism, and are determined to reach, without delay, an agreement to protect personal information exchanged in the context of fighting crime and terrorism in a comprehensive manner that will advance our mutual goals;

ACKNOWLEDGING the successful Joint Reviews in 2005 and 2010 of the 2004 and 2007 Agreements between the Parties on the transfer of PNR;

NOTING the interest of the parties, as well as EU Member States, in exchanging information regarding the method of transmission of PNR as well as the onward transfer of PNR as set forth in the relevant articles of this Agreement, and further noting the EU's interest in having this addressed in the context of the consultation and review mechanism set forth in this Agreement;

AFFIRMING that this Agreement does not constitute a precedent for any future arrangements between the Parties, or between either of the Parties and any other party, regarding the processing, use, or transfer of PNR or any other form of data, or regarding data protection;

Comment [U7]: Note the text does not link these privacy commitments to the actual information sharing. (e.g. it could have said that "MINDFUL that any information sharing has **to conform** with the EU's commitments pursuant to .....). or "MINDFUL that any information sharing has to **be proportionate and conform**..."

In any event, "MINDFUL" is not a very strong proposition. For instance having some "privacy obligation in your mind" is not the same as having to "conform with" or "apply" these privacy obligations.

For example, one may have all sorts of thoughts about an attractive individual "in your mind"; it does not mean that what is in your mind comes to pass!

Comment [U8]: As we shall see, one of the themes of my analysis is that the text of the Agreement has been drafted to exclude a role for any of Europe's data protection authorities.

As DHS processes are "robust", there appears to be little harm in allowing data protection authorities an independent role For example, the fact that an authority could independently verify that DHS procedures are "robust" would help public acceptability of this Agreement.

Comment [U9]: This exposes a conflict of interest because the EU has two responsibilities: (a) it negotiates the terms of the Agreement to facilitate the transfer of PNR data, and (b) it also decides whether the privacy protection in the USA is adequate.

As the EU has a vested interest in getting PNR data from the USA to support Europe's law enforcement bodies, the suspicion is that it has compromised on data protection standards to get these data.

The role of the data protection authority should be to act as an independent counter-balance that ensures that any compromise on the personal data needs of law enforcement does not unfairly prejudice individual privacy. **There is no independent counter-balance in this Agreement.**

As we shall see, the level of data protection falls well below normal European standards but the EU has deemed this level to be adequate in circumstances.

Comment [U10]: The review mechanism, as we shall see, does not mention a role for **any data protection authority** (although the Commission could choose to include such authorities, as part of the review team, there is no obligation for the Commission to do so). A point made by the EDPS.

Note also that the concept of "onward transfer" used in this paragraph is not qualified in terms of "proportionate onward transfer" – see U2 above

RECOGNIZING the related principles of proportionality as well as relevance and necessity that guide this Agreement and its implementation by the European Union and the United States; and

HAVING REGARD to the possibility of the Parties to further discuss the transfer of PNR data in the maritime mode;

HEREBY AGREE:

CHAPTER I: GENERAL PROVISIONS

Article 1: Purpose

1. The purpose of this Agreement is to ensure security and to protect the life and safety of the public.

2. For this purpose, this Agreement sets forth the responsibilities of the Parties with respect to the conditions under which PNR may be transferred, processed and used, and protected.

Article 2: Scope

1. PNR, as set forth in the Guidelines of the International Civil Aviation Organization, shall mean the record created by air carriers or their authorized agents for each journey booked by or on behalf of any passenger and contained in carriers' reservation systems, departure control systems, or equivalent systems providing similar functionality (collectively referred to in this Agreement as reservation systems). Specifically, as used in this Agreement, PNR consists of the data types set forth in the annex to this Agreement.

2. This Agreement shall apply to carriers operating passenger flights between the European Union and the United States.

3. This Agreement shall also apply to carriers incorporated or storing data in the European Union and operating passenger flights to or from the United States.

Article 3: Provision of PNR

The Parties agree that carriers shall provide PNR contained in their reservation systems to DHS as required by and in accordance with DHS standards and consistent with this Agreement. Should PNR transferred by carriers include data beyond those listed in the annex to this Agreement, DHS shall delete such data upon receipt.

Article 4: Use of PNR

1. The United States collects, uses and processes PNR for the purposes of preventing, detecting, investigating, and prosecuting:

(a) Terrorist offenses and related crimes, including

i. Conduct that –

1. involves a violent act or an act dangerous to human life, property, or infrastructure; and

Comment [U11]: The Article states that the proportionality related principles only "**guide**" this Agreement; they are not really a central component to it.

This reinforces the comments concerning "MINDFUL" (see U7) that there is not a strong linkage between proportionality, privacy protection and the Articles that allow for information sharing for law enforcement needs.

Comment [U12]: A promise to extending the Agreement to shipping; bit of a puzzle – How many people go to the USA by boat? Perhaps this is to close an obvious loophole.

Comment [U13]: Article 2(1) defines **PNR data** to be the items listed in Annex 1

So when the Agreement uses the term **PNR data**, it is referring to the Annex 1 detail; it does not include **any other personal details** that the DHS might collect (e.g. on a suspect who is travelling to the USA).

This limited definition thus restricts the individual "rights" in the Agreement; they **apply just to the PNR data**.

Comment [U14]: As terrorism offences are in Article 4(1)(a); it follows that the rest of the Article (e.g. Article 4(2)) does not relate to terrorism offences.

We use this fact later.

2. appears to be intended to –

a. intimidate or coerce a civilian population;

b. influence the policy of a government by intimidation or coercion; or

c. affect the conduct of a government by mass destruction, assassination, kidnapping, or hostage-taking.

ii. Activities constituting an offense within the scope of and as defined in applicable international conventions and protocols relating to terrorism;

iii. Providing or collecting funds, by any means, directly or indirectly, with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the acts described in subparagraphs (i) or (ii);

iv. Attempting to commit any of the acts described in subparagraphs (i), (ii), or (iii);

v. Participating as an accomplice in the commission of any of the acts described in subparagraphs (i), (ii), or (iii);

vi. Organizing or directing others to commit any of the acts described in subparagraphs (i), (ii), or (iii);

vii. Contributing in any other way to the commission of any of the acts described in subparagraphs (i), (ii), or (iii);

viii. Threatening to commit an act described in subparagraph (i) under circumstances which indicate that the threat is credible;

(b) Other crimes that are punishable by a sentence of imprisonment of three years or more and that are transnational in nature.

A crime is considered as transnational in nature in particular if:

i. It is committed in more than one country;

ii. It is committed in one country but a substantial part of its preparation, planning, direction or control takes place in another country;

iii. It is committed in one country but involves an organized criminal group that engages in criminal activities in more than one country;

iv. It is committed in one country but has substantial effects in another country; or

v. It is committed in one country and the offender is in or intends to travel to another country.

2. PNR may be used and processed on a case-by-case basis where necessary in view of a serious threat and for the protection of vital interests of any individual or if ordered by a court.

Comment [U15]: The use of the word "Other crimes" means crimes "other than the terrorist related crimes". This provision is therefore **NOT INTENDED** to relate to crimes associated with terrorism.

Comment [U16]: A crime that could attract a maximum three year sentence anywhere in the USA or in Europe could cover a large number of minor crimes.

This repeats the concerns over the general internal EU PNR provisions currently being considered; there is widespread concern that the 3 year sentence provision is too wide. (e.g. examples such as non payment of a restaurant bill; see Hawktalk blog of 08/02/2011)

Notice that comment U1 note that the Agreement STRESSES "combating terrorism and serious transnational crime". However, the word "serious" is dropped in this definition of "transnational crime".

Comment [U17]: Use of the term "serious transnational crime" instead of "transnational crime" would have offered more reassurance to the public that the Agreement remained focused on its primary objectives (see U1).

Comment [U18]: The use of "in particular" here means that there could be other forms of "transnational crime" not described in sub-paragraphs (i),(ii),(iii),iv) and (v). I have no idea these other forms could be; the Commission should explain.

Comment [U19]: This is a curious definition of a crime that is supposed to be "transnational". It covers a passenger who is allegedly involved in a crime in one country and then goes on holiday to the USA (see U16 about the restaurant bill).

Comment [U20]: Vital interests are life threatening situations; clearly includes passengers with an infectious disease. This purpose/functionality is not mentioned in the Preamble which describes the purpose of the Agreement (see U1)

Ordered by the court could potentially involve lots of things (e.g. failure to pay maintenance). This purpose/functionality is also not mentioned in Preamble – see U1

3. PNR may be used and processed by DHS to identify persons who would be subject to closer questioning or examination upon arrival to or departure from the United States or who may require further examination.

4. Paragraphs 1, 2, and 3 of this Article shall be without prejudice to domestic law enforcement, judicial powers, or proceedings, where other violations of law or indications thereof are detected in the course of the use and processing of PNR.

CHAPTER II: SAFEGUARDS APPLICABLE TO THE USE OF PNR

Article 5:Data Security

1. DHS shall ensure that appropriate technical measures and organizational arrangements are implemented to protect personal data and personal information contained in PNR against accidental, unlawful or unauthorized destruction, loss, disclosure, alteration, access, processing or use.

2. DHS shall make appropriate use of technology to ensure data protection, security, confidentiality and integrity. In particular, DHS shall ensure that:

(a) encryption, authorization and documentation procedures recognized by competent authorities are applied. In particular, access to PNR shall be secured and limited to specifically authorized officials;

(b) PNR shall be held in a secure physical environment and protected with physical intrusion controls; and

(c) mechanism exists to ensure that PNR queries are conducted consistent with Article 4.

3. In the event of a privacy incident (including unauthorized access or disclosure), DHS shall take reasonable measures to notify affected individuals as appropriate, to mitigate the risk of harm of unauthorized disclosures of personal data and information, and to institute remedial measures as may be technically practicable.

4. Within the scope of this Agreement, DHS shall inform without undue delay the relevant European authorities about cases of significant privacy incidents involving PNR of EU citizens or residents resulting from accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, or any unlawful forms of processing or use.

5. The United States confirms that effective administrative, civil, and criminal enforcement measures are available under U.S. law for privacy incidents. DHS may take disciplinary action against persons responsible for any such privacy incident, as appropriate, to include denial of system access, formal reprimands, suspension, demotion, or removal from duty.

6. All access to PNR, as well as its processing and use, shall be logged or documented by DHS. Logs or documentation shall be used only for oversight, auditing, and system maintenance purposes or as otherwise required by law.

Comment [U21]: Note that this use of PNR data with this provision, by implication, **does not** relate to terrorism (that is in Article 4(1)(a)), **nor** transnational crime (that is in Article 4(1)(b)), **nor** vital interests, **nor** by order of a court (that is in Article 4(2)).

What are these circumstances? I have no idea. **There is a need for some kind of explanation as to what is intended**. These circumstances are also not mentioned in Preamble – see U1

Comment [U22]: Note that direct notification of the privacy incident to the relevant data protection authority is not mentioned. The words "as appropriate" apply to the DHS so it can decide whether contact with affected individuals is needed.

Normally, one would expect the data protection authority to be involved in the decision whether contact with data subjects was appropriate following a report to it concerning an incident.

From the US perspective, I can understand the issue of having a data protection authority giving directions the DHS. However, this objection disappears if the DHS had an obligation to consult a data protection authority for advice on best practice (as any advice can be set aside).

Procedures at the DHS are "robust" – see comments at U8 - so in theory, I cannot see the harm if a data protection authority were to give advice or be notified about a data loss or a serious privacy incident.

Comment [U23]: The provision does not stipulate that a data protection authority or the European Data Protection Supervisor is a "relevant authority.

A data protection authority could be "relevant authority" of course so the provision is suitably vague – vague enough to **exclude** them.

In my view, the data protection authorities should be alerted to serious privacy incidents and data losses. - see U22 - as this would enhance public confidence in the Agreement.

Comment [U24]: It would have been a simple matter to allow a data protection authority or the European Data Protection Supervisor to have access to these logs, or to require statistics from these logs to be collected or produced.

Such an involvement ensures that the audit trail/logs etc collect the neccessary detail and allows for **independent analysis**. This independence can reassure the public about the use of PNR data.

The suspicion has to be that the EU and the DHS have drafted these provisions so that Europe's data protection authorities are NOT in the loop

Article 6: Sensitive Data

1. To the extent that PNR of a passenger as collected includes sensitive data (i.e., personal data and information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or data concerning the health or sex life of the individual), DHS shall employ automated systems to filter and mask out sensitive data from PNR. In addition, DHS shall not further process or use such data, except in accordance with paragraphs 3 and 4 of this Article.

2. DHS shall provide to the European Commission within 90 days of the entry into force of this Agreement a list of codes and terms identifying sensitive data that shall be filtered out.

3. Access to, as well as processing and use of, sensitive data shall be permitted in exceptional circumstances where the life of an individual could be imperiled or seriously impaired. Such data may be exclusively accessed using restrictive processes on a case-by-case basis with the approval of a DHS senior manager.

4. Sensitive data shall be permanently deleted not later than 30 days from the last receipt of PNR containing such data by DHS. However, sensitive data may be retained for the time specified in U.S. law for the purpose of a specific investigation, prosecution or enforcement action.

Article 7: Automated Individual Decisions

The United States shall not make decisions that produce significant adverse actions affecting the legal interests of individuals based solely on automated processing and use of PNR.

Article 8 :Retention of Data

1. DHS retains PNR in an active database for up to five years. After the initial six months of this period, PNR shall be depersonalized and masked in accordance with paragraph 2 of this Article. Access to this active database shall, unless otherwise permitted by this Agreement, be restricted to a limited number of specifically authorized officials.

2. To achieve depersonalization, personally identifiable information contained in the following PNR data types shall be masked out:

(a) name(s);

(b) other names on PNR;

(c) all available contact information (including originator information);

(d) General Remarks, including other supplementary information (OSI), special service information (SSI), and special service request (SSR); and

(e) any collected APIS information.

Comment [U25]: This provision excludes criminal convictions and criminal intelligence from the list of Sensitive Data.

Its omission in this Article thus implies that PNR data could include criminal intelligence and criminal record data.

Yet these criminal related data items are not listed as PNR data items in Annex 1 (unless they appear in a free text field); so these data should not appear in PNR data.

I am puzzled here as to what is going on, unless of course the objective is to transmit criminal record data or criminal intelligence as part of the free text fields associated with PNR data.

The EDPS wants ALL sensitive data excluded; so presumably he thinks that this provision includes Sensitive Data

Comment [U26]: A simple enhancement to the privacy protection on offer would arise if there were to be consultation with a data protection authority or the European Data Protection Supervisor about the nature of the filtering process.

Comment [U27]: I am not sure whether this provision is of any value at all as it relates **solely** to PNR data. Reading the text (and the press release - see U62) this is what it says!

This means, for instance, if there were to be automated decisions made in conjunction with a DHS watch list or other personal data used **in conjunction with** PNR data, then this safeguard does not apply.

In this instance, the automated decision would **not be based solely** on the automated processing of PNR data; it would be based on PNR data **PLUS** something else.

Comment [U28]: I am sure that many commentators will focus on a retention of personal data for 5-15 years or more. The EDPS thinks retention should be six months maximum.

All I would say is that would be helpful to know the evidence base for retention periods specified in this Article.

Depersonalisation only acts as a limited security protection as the identifying personal data (i.e. demasking) can be reconstituted easily.

However, this provision is qualified by Articles 8(6), 20 and 26(1). (see comments below at U31, U49 and U53).

THIS QUALIFICATION IS IMPORTANT as the retention period could be extend beyond the periods identified in this Article. **Any politician who says otherwise has not read these provisions.**

3. After this active period, PNR shall be transferred to a dormant database for a period of up to ten years. This dormant database shall be subject to additional controls, including a more restricted number of authorized personnel, as well as a higher level of supervisory approval required before access. In this dormant database, PNR shall not be repersonalized except in connection with law enforcement operations and then only in connection with an identifiable case, threat or risk. As regards the purposes as set out in Article 4, paragraph (1)(b), PNR in this dormant database may only be repersonalized for a period of up to five years.

4. Following the dormant period, data retained must be rendered fully anonymized by deleting all data types which could serve to identify the passenger to whom PNR relate without the possibility of repersonalization.

5. Data that are related to a specific case or investigation may be retained in an active PNR database until the case or investigation is archived. This paragraph is without prejudice to data retention requirements for individual investigation or prosecution files.

6. The Parties agree that, within the framework of the evaluation as provided for in Article 23, paragraph 1, the necessity of a 10-year dormant period of retention will be considered.

Article 9: Non-discrimination

The United States shall ensure that the safeguards applicable to processing and use of PNR under this Agreement apply to all passengers on an equal basis without unlawful discrimination.

Article 10: Transparency

1. DHS shall provide information to the traveling public regarding its use and processing of PNR through:

(a) publications in the Federal Register;

(b) publications on its website;

(c) notices that may be incorporated by the carriers into contracts of carriage;

(d) statutorily required reporting to Congress; and

(e) other appropriate measures as may be developed.

2. DHS shall publish and provide to the EU for possible publication its procedures and modalities regarding access, correction or rectification, and redress procedures.

Comment [U29]: Even if one accepted the retention period as reasonable, any data protection analysis would conclude that identifiable data relating to Articles 4(2) and 4(3) should be deleted after 5 years. After all these are provisions which **do not involve crime or terrorism** by definition, and this provision (Article 9(6)) is limited to retention needs of law enforcement**.**

It would have been clearer if this provision expressly mentioned what happened to PNR data collected pursuant to Articles 4(2) and 4(3) .

As it is, there is doubt as to what happens in practice, I suspect details about non payment of a bill in connection with a court order (as this is arguably law enforcement) could easily be kept for 10 years.

This is a poorly drafted provision that could allow this Agreement to undergo "function creep" and be used, in future, to trace debtors (by order of a court in the USA).

Comment [U30]: As this provision is not expressly linked to Articles 4(1)(a) or 4(1)(b) (i.e. terrorism and transnational crime), it allows for retention periods in excess of 10 years above for any investigation across the whole spectrum of Article 4 (some of which do not deal with terrorism or crime).

Comment [U31]: This should be read as saying that 10 years might well be increased, as the USA, as is well known, wants a much longer retention period. If this Agreement is renewed, the retention period could be extended.

This provision allows the politicians to claim there is a 10 year retention period in the Agreement knowing that in practice, this retention period could be extended (e.g. for a further 10 years) in about 7 years time (see comments about Article 20, as they are important.

This provision and Article 20 **undermines** any claim that the retention period is a fixed certainty. This is not the case.

Comment [U32]: This transparency provision covers the fair processing notice. Note that the obvious place to provide this notice is on the actual ticket and not buried in the contract. I do not know why this simple suggestion is omitted.

Comment [U33]: The right of access and correction of personal data are central tenets of data protection. I cannot see any reason why there is no role for any data protection authority or the European Data Protection Supervisor in designing, suggesting or approving these procedures.

As EU and/or DHS can decide what these procedures are and what is published without any independent advice, the risk is that procedures are not audited sufficiently and might not deal with all the relevant data protection issues.

3. The Parties shall work with the aviation industry to encourage greater visibility to passengers at the time of booking on the purpose of the collection, processing and use of PNR by DHS, and on how to request access, correction and redress.

Article 11: Access for Individuals

1. In accordance with the provisions of the Freedom of Information Act, any individual, regardless of nationality, country of origin, or place of residence is entitled to request his or her PNR from DHS. DHS shall timely provide such PNR subject to the provisions of paragraphs 2 and 3 of this Article.

2. Disclosure of information contained in PNR may be subject to reasonable legal limitations, applicable under U.S. law, including any such limitations as may be necessary to safeguard privacy-protected, national security, and law enforcement sensitive information.

3. Any refusal or restriction of access shall be set forth in writing and provided to the requesting individual on a timely basis. Such notification shall include the legal basis on which information was withheld and shall inform the individual of the options available under U.S. law for seeking redress.

4. DHS shall not disclose PNR to the public, except to the individual whose PNR has been processed and used or his or her representative, or as required by U.S. law.

Article 12: Correction or Rectification for Individuals

1. Any individual regardless of nationality, country of origin, or place of residence may seek the correction or rectification, including the possibility of erasure or blocking, of his or her PNR by DHS pursuant to the processes described in this Agreement.

2. DHS shall inform, without undue delay, the requesting individual in writing of its decision whether to correct or rectify the PNR at issue.

3. Any refusal or restriction of correction or rectification shall be set forth in writing and provided to the requesting individual on a timely basis. Such notification shall include the legal basis of such refusal or restriction and shall inform the individual of the options available under U.S. law for seeking redress.

Comment [U34]: Note that this "greater visibility" provision does not mention visibility to any data protection authority or to the European Data Protection Supervisor.

Comment [U35]: This is a weak provision **applying just to PNR data** (i.e. access to personal data in Annex 1). It is a very minor right as one assumes the data subject knows which flight he caught and how he paid for it etc, and where he lives. Perhaps if he is interested in what seat he sat in – the right becomes useful – who knows? But this shows the level that this right is operating.

What the data subject should have is, **subject to an exemption to protect the law enforcement purpose**, access to **ALL** the personal data and not just the PNR data. If there is a problem, the problem will not rest with the PNR data; it will lie with the associated personal data that investigators collect, use and interpret.

The Agreement ignores an obvious compromise: for a data protection authority or European Data Protection Supervisor to look at the personal data on behalf of a data subject (i.e. to act as honest broker to sort out any problem).

Comment [U36]: This exemption from access is so unlike the UK DP Act which provides for an exemption from the right of access if there is "prejudice" to a crime related purpose.

This exemption thus envisages exclusions for the right of access to PNR data even where there is no prejudice to an investigation.

Comment [U37]: This is likely to mean "go to court". Like U35, the Agreement overlooks the compromise whereby a data protection authority can act "as honest broker" if there are problems– see also U39

Comment [U38]: The right **only applies to PNR data. (**e.g. data subject can correct the data which relate to which seat he sat in). It is limited and inconsequential.

What the data subject usually gets from a data protection regime is, **subject to an applicable exemption**, a right of correction that applies to **ALL** relevant personal data collected and **not just the PNR data**.

As with U35/U39 – it overlooks a role for a data protection authority or European Data Protection Supervisor to look at the other personal data on behalf of a data subject and make an independent judgment on whether these data should be corrected

Comment [U39]: Another provision which means "go to Court". Note that if a data protection authority or the European Data Protection Supervisor could suggest redress, this would avoid the difficulty of a data subject taking a court case in a unfamiliar jurisdiction.

In practice, Article 12(3) has been drafted to provide a safeguard that no-one can use.

Article 13: Redress for Individuals

1. Any individual regardless of nationality, country of origin, or place of residence whose personal data and personal information has been processed and used in a manner inconsistent with this Agreement may seek effective administrative and judicial redress in accordance with U.S. law.

2. Any individual is entitled to seek to administratively challenge DHS decisions related to the use and processing of PNR.

3. Under the provisions of the Administrative Procedure Act and other applicable law, any individual is entitled to petition for judicial review in U.S. federal court of any final agency action by DHS. Further, any individual is entitled to petition for judicial review in accordance with applicable law and relevant provisions of:

(a) the Freedom of Information Act;

(b) the Computer Fraud and Abuse Act;

(c) the Electronic Communications Privacy Act; and

(d) other applicable provisions of U.S. law.

4. In particular, DHS provides all individuals an administrative means (currently the DHS Traveler Redress Inquiry Program (DHS TRIP)) to resolve travel-related inquiries including 35/38/those related to the use of PNR. DHS TRIP provides a redress process for individuals who believe they have been delayed or prohibited from boarding a commercial aircraft because they were wrongly identified as a threat. Pursuant to the Administrative Procedure Act and Title 49, United States Code, Section 46110, any such aggrieved individual is entitled to petition for judicial review in U.S. federal court from any final agency action by DHS relating to such concerns.

Comment [U40]: The challenge only relates to **the PNR data**; the challenge provision does not cover information that is **not PNR data**.

Perhaps the data subject wants to challenge which seat he sat on – that's about how useful this is.

Notice there if there were to be an obligation to consult a data protection authority or seek the views of a data protection authority, then this does not mean that advice is followed.

In that sense, the above suggestion for the involvement of a data protection regulator is very minimal and modest indeed.

This sense applies to comments at U35/U38/U39 about the role of a data protection authority as "honest broker or go-between

Article 14: Oversight

1. Compliance with the privacy safeguards in this Agreement shall be subject to independent review and oversight by Department Privacy Officers, such as the DHS Chief Privacy Officer, who:

(a) have a proven record of autonomy;

(b) exercise effective powers of oversight, investigation, intervention, and review; and

(c) have the power to refer violations of law related to this Agreement for prosecution or disciplinary action, when appropriate.

They shall, in particular, ensure that complaints relating to non-compliance with this Agreement are received, investigated, responded to, and appropriately redressed. These complaints may be brought by any individual, regardless of nationality, country of origin, or place of residence.

Comment [U41]: Yet again, another oversight provision where there is no role for a data protection authority or the European Data Protection Supervisor (EDPS) to recommend a course of action.

There is not even the weak provision that requires the DHS to consider "guidance" from a data protection authority or EDPS (see U40 above).

Just ask a simple question: "Who should have oversight of an issue that involves data protection?".

The answer this Agreement arrives at is that any oversight is undertaken by the very bodies that are responsible for the interference with private and family life in the first place.

2. In addition, application of this Agreement by the United States shall be subject to independent review and oversight by one or more of the following entities:

(a) the DHS Office of Inspector General;

(b) the Government Accountability Office as established by Congress; and

(c) the U.S. Congress.

Such oversight may be manifested in the findings and recommendations of public reports, public hearings, and analyses.

Comment [U42]: Note that there is no regular reporting mechanism to the public here. This "may" happen – and of course it may not.

The DHS could easily be required to provide a confidential memorandum to the European Data Protection Supervisor for instance. The EDPS could be allowed to ask about the statistics about the scheme or to require such statistics to be maintained.

Because of the lack of independence, any analysis provided by the DHS runs the risk of being flawed, skewed, self-serving and lacking credibility. At worst, it's like asking Count Dracula (yes him again) to report on the effectiveness of the distribution of blood from a blood bank, where the Count controls access to the blood bank.

CHAPTER III: MODALITIES OF TRANSFERS

Article 15: Method of PNR Transmission

1. For the purposes of this Agreement, carriers shall be required to transfer PNR to DHS using the "push" method, in furtherance of the need for accuracy, timeliness and completeness of PNR.

2. Carriers shall be required to transfer PNR to DHS by secure electronic means in compliance with the technical requirements of DHS.

3. Carriers shall be required to transfer PNR to DHS in accordance with paragraphs 1 and 2 of this Article, initially at 96 hours before the scheduled flight departure and additionally either in real time or for a fixed number of routine and scheduled transfers as specified by DHS.

4. In any case, the Parties agree that all carriers shall be required to acquire the technical ability to use the "push" method not later than 24 months following entry into force of this Agreement.

5. DHS may, where necessary, on a case-by-case basis, require a carrier to provide PNR between or after the regular transfers described in paragraph 3. Wherever carriers are unable, for technical reasons, to respond timely to requests under this Article in accordance with DHS standards, or, in exceptional circumstances in order to respond to a specific, urgent, and serious threat, DHS may require carriers to otherwise provide access.

Article 16: Domestic Sharing

1. DHS may share PNR only pursuant to a careful assessment of the following safeguards:

(a) Exclusively as consistent with Article 4;

Comment [U43]: There is no obligation to have any domestic sharing "proportionate". For example, a heading that simply stated "Proprotionate Domestic Data Sharing" would reassure.

Inclusion of this "p" word would formalise a balance between privacy and law enforcement as part of the sharing process; its absence, I am afraid, speaks volumes as to the level of privacy protection on offer.

Notice that no independently designed statistics will be kept to demonstrate that domestic sharing is justified. There is no obligations to keep statistics on what is shared, when it was shared, with whom, by whom and with what outcome etc. See also U46

The point is simply expressed: the design of the audit trail should have an independent element; the design should not be left to the parties doing the data sharing and the interfering with private and family life.

In the UK for instance there is a Code of Practice on data sharing; that Code contains the detail the UK's data protection authority wants to be retained to assess whether the data sharing was in accordance with the UK Act. Something similar should occur in this Agreement.

Comment [U44]: Remember this is the whole of Article 4 and therefore includes circumstances that **do not** relate to crime or terrorism.

(b) Only with domestic government authorities when acting in furtherance of the uses outlined in Article 4;

(c) Receiving authorities shall afford to PNR equivalent or comparable safeguards as set out in this Agreement; and

(d) PNR shall be shared only in support of those cases under examination or investigation and pursuant to written understandings and U.S. law on the exchange of information between domestic government authorities.

2. When transferring analytical information obtained from PNR under this Agreement, the safeguards set forth in paragraph 1 of this Article shall be respected.

Article 17: Onward Transfer

1. The United States may transfer PNR to competent government authorities of third countries only under terms consistent with this Agreement and only upon ascertaining that the recipient's intended use is consistent with these terms.

2. Apart from emergency circumstances, any such transfer of data shall occur pursuant to express understandings that incorporate data privacy protections comparable to those applied to PNR by DHS as set out in this Agreement.

3. PNR shall be shared only in support of those cases under examination or investigation.

4. Where DHS is aware that PNR of a citizen or a resident of an EU Member State is transferred, the competent authorities of the concerned Member State shall be informed of the matter at the earliest appropriate opportunity.

5. When transferring analytical information obtained from PNR under this Agreement, the safeguards set forth in paragraphs 1-4 of this Article shall be respected.

Article 18: Police, Law Enforcement and Judicial Cooperation

1. Consistent with existing law enforcement or other information-sharing agreements or arrangements between the United States and any Member State of the EU or Europol and Eurojust, DHS shall provide to competent police, other specialized law enforcement or judicial authorities of the Member States and Europol and Eurojust within the remit of their respective mandates, as soon as practicable, relevant, and appropriate, analytical information obtained from PNR in those cases under examination or investigation to prevent, detect, investigate, or prosecute within the European Union transnational crime as described in Article 4, paragraph 1(b) or conduct or activities related to terrorist offenses.

2. A police or judicial authority of a Member State of the EU, or Europol or Eurojust, may request, within its mandate, access to PNR or relevant analytical information obtained from PNR that are necessary in a specific case to prevent, detect, investigate, or prosecute within the European Union a terrorist offense or transnational crime as described in Article 4,

Comment [U45]: This is a terribly loose provision. As with U43, it would have been nice to have Article 17 entitled "Proportionate Onward Transfer".

Comment [U46]: No obligation to make sure that Third countries do not onward disclose.

No penalty if the Third Country uses the data for something else.

No obligation to ensure that the onward transfer is proportionate.

No need to keep records of the transfer (see comments re the UK Code of Practice on data sharing at U43).

No role for any data protection authority See ANNEX II which sets out a mechanism for review of thisArticle; a review that does not involve any data protection authority. (Perish that thought immediately!).

Comment [U47]: Note that the Agreement does not even say that onward transfer is limited to "terrorism" or "serious transnational crime" so it can be very broad.

This has been picked up by the EDPS.

Comment [U48]: Note that it does not say a data protection authority is a competent authority.

Another example of drafting that keeps data protection authorities out of the loop.

paragraph 1(b). DHS shall, subject to the agreements and arrangements noted in paragraph 1 of this Article, provide such information.

3. Pursuant to paragraphs 1 and 2 of this Article, DHS shall share PNR only following a careful assessment of the following safeguards:

(a) Exclusively as consistent with Article 4;

(b) Only when acting in furtherance of the uses outlined in Article 4; and

(c) Receiving authorities shall afford to PNR equivalent or comparable safeguards as set out in this Agreement.

4. When transferring analytical information obtained from PNR under this Agreement, the safeguards set forth in paragraphs 1-3 of this Article shall be respected.

CHAPTER IV: IMPLEMENTING AND FINAL PROVISIONS

Article 19: Adequacy

In consideration of this Agreement and its implementation, DHS shall be deemed to provide, within the meaning of relevant EU data protection law, an adequate level of protection for PNR processing and use. In this respect, carriers which have provided PNR to DHS in compliance with this Agreement shall be deemed to have complied with applicable legal requirements in the EU related to the transfer of such data from the EU to the United States.

Article 20: Reciprocity

1. The Parties shall actively promote the cooperation of carriers within their respective jurisdictions with any PNR system operating or as may be adopted in the other's jurisdiction, consistent with this Agreement.

2. Given that the establishment of an EU PNR system could have a material effect on the Parties' obligations under this Agreement, if and when an EU PNR system is adopted, the Parties shall consult to determine whether the present Agreement would need to be adjusted accordingly to ensure full reciprocity. Such consultations shall in particular examine whether any future EU PNR system would apply less stringent data protection standards than those provided for in the present Agreement, and whether, therefore, it should be amended.

Comment [U49]: I have highlighted this part of the Agreement because I find it an astonishing statement of intent.

It suggests that even the weak data protection standards in this Agreement are too high for the USA (and possibly the law enforcement agenices of some EU countries).

Look at this provision WITH Articles 8(6) and 20 about reviewing (i.e. lengthening) data retention periods. **It is now clear that any politician cannot give a guarantee that the retention period is fixed** (see U31/U53).

Apart from, extending the retention period associated with PNR data, the most likely provisions that could be "under review" would be onward transfer, rights of access to personal data and correction, and data sharing.

All provisions could also be changed by this review.

Article 21: Implementation and Non-Derogation

1. This Agreement shall not create or confer, under U.S. law, any right or benefit on any person or entity, private or public. Each Party shall ensure that the provisions of this Agreement are properly implemented.

2. Nothing in this Agreement shall derogate from existing obligations of the United States and Member States, including under the Agreement on Mutual Legal Assistance between the European Union and the United States of 25 June 2003 and the related bilateral mutual legal assistance instruments between the United States and Member States.

Article 22: Notification of Changes in Domestic Law

The Parties shall advise each other regarding the enactment of any legislation that materially affects the implementation of this Agreement.

Article 23: Review and Evaluation

1. The Parties shall jointly review the implementation of this Agreement one year after its entry into force and regularly thereafter as jointly agreed. Further, the Parties shall jointly evaluate this Agreement four years after its entry into force.

2. The Parties shall jointly determine in advance the modalities and terms of the joint review and shall communicate to each other the composition of their respective teams. For the purpose of the joint review, the European Union shall be represented by the European Commission, and the United States shall be represented by DHS. The teams may include appropriate experts on data protection and law enforcement. Subject to applicable laws, participants in the joint review shall be required to have appropriate security clearances and to respect the confidentiality of the discussions. For the purpose of the joint review, DHS shall ensure appropriate access to relevant documentation, systems, and personnel.

3. Following the joint review, the European Commission shall present a report to the European Parliament and the Council of the European Union. The United States shall be given an opportunity to provide written comments which shall be attached to the report.

Article 24: Resolution of Disputes and Suspension of Agreement

1. Any dispute arising from the implementation of this Agreement, and any matters related thereto, shall give rise to consultations between the Parties, with a view to reaching a mutually agreeable resolution, including providing an opportunity for either Party to cure within a reasonable time.

2. In the event that consultations do not result in a resolution of the dispute, either Party may suspend the application of this Agreement by written notification through diplomatic channels, with any such suspension to take effect 90 days from the date of such notification, unless the Parties otherwise agree to a different effective date.

3. Notwithstanding any suspension of this Agreement, all PNR obtained by DHS pursuant to this Agreement prior to its suspension shall continue to be processed and used in accordance with the safeguards of this Agreement.

Article 25: Termination

1. Either Party may terminate this Agreement at any time by written notification through diplomatic channels.

2. Termination shall take effect 120 days from the date of such notification, unless the Parties otherwise agree to a different effective date.

Comment [U50]:

This allows for a review and evaluation of an Agreement that involves the processing of personal data but does not include any European data protection authority or the European Data Protection Supervisor. (see comments re the UK Code of Practice on data sharing at U43). Unacceptably poor in my humble estimation.

Instead the EU and DHS could get in a huddle and decide what report to the European Parliament says in order to put the Agreement in the best light).

There is no provision to provide any independent statistic that shows the use of PNR data is valid and effective. Indeed, there is no provision that requires statistics to be kept.

There is no provision which allows the a data protection authority or the European Data Protection Supervisor to audit, or to ask that certain statistics based on the logs are provided.

The lack of any semblance of independent review or meaningful review undermines this provision.

Comment [U51]:

As before, this review does not go through any independent body, other than the organisations that have a vested interest in showing the the exchange of PNR data is the best thing since sliced bread.

Any joint review runs the risk that it will be unable to command any public confidence.

Back to Count Dracula comment I suspect – see U42, and the Code of Practice comments at U43

Comment [U52]:

Another resolution of disputes procedure that involves personal data but excludes the European Data Protection Supervisor or any data protection authority.

3. Prior to any termination of this Agreement, the Parties shall consult each other in a manner which allows sufficient time for reaching a mutually agreeable resolution.

4. Notwithstanding any termination of this Agreement, all PNR obtained by DHS pursuant to this Agreement prior to its termination shall continue to be processed and used in accordance with the safeguards of this Agreement.

Article 26: Duration

1. Subject to Article 25, this Agreement shall remain in force for a period of seven years from the date of its entry into force.

2. Upon the expiry of the period set forth in paragraph 1 of this Article, as well as any subsequent period of renewal under this paragraph, the Agreement shall be renewed for a subsequent period of seven years unless one of the Parties notifies the other in writing through diplomatic channels, at least twelve months in advance, of its intention not to renew the Agreement.

3. Notwithstanding the expiration of this Agreement, all PNR obtained by DHS under the terms of this Agreement shall continue to be processed and used in accordance with the safeguards of this Agreement. Similarly, all PNR obtained by DHS under the terms of the Agreement Between the United States of America and the European Union on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security (DHS), signed at Brussels and Washington July 23 and 26, 2007, shall continue to be processed and used in accordance with the safeguards of that Agreement.

Article 27: Final provisions

1. 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.

2. This Agreement, as of the date of its entry into force, shall supersede the July 23 and 26, 2007 Agreement.

3. This Agreement will only apply to the territory of Denmark, the United Kingdom or Ireland, if the European Commission notifies the United States in writing that Denmark, the United Kingdom or Ireland has chosen to be bound by this Agreement.

4. If the European Commission notifies the United States before the entry into force of this Agreement that it will apply to the territory of Denmark, the United Kingdom or Ireland, this Agreement shall apply to the territory of such State on the same day as for the other EU Member States bound by this Agreement.

5. If the European Commission notifies the United States after entry into force of this Agreement that it applies to the territory of Denmark, the United Kingdom or Ireland, this Agreement shall apply to the territory of such State on the first day following receipt of the notification by the United States.

Comment [U53]:

After 7 years, we can expect Article 20(2) to be debated; this is the important provision here (see U49)

Article 20 calls for consultations that "shall in particular examine whether any future EU PNR system would apply less stringent data protection standards than those provided for in the present Agreement".

Another Article that foreshadows even weaker data protection controls. This provision should be considered in the context of comments made in relation to Articles 8(6) and 20(2) – U31 and U49

Done at…this…day of…2011, in two originals.

Pursuant to EU law, this Agreement shall also be drawn up by the EU in the Bulgarian, Czech, Danish, Dutch, Estonian, Finnish, French, German, Greek, Hungarian, Italian, Latvian, Lithuanian, Maltese, Polish, Portuguese, Romanian, Slovak, Slovenian, Spanish and Swedish languages.

ANNEX I: PNR Data Types

1. PNR record locator code

2. Date of reservation/issue of ticket

3. Date(s) of intended travel

4. Name(s)

5. Available frequent flier and benefit information (i.e., free tickets, upgrades, etc.)

6. Other names on PNR, including number of travelers on PNR

7. All available contact information (including originator information)

8. All available payment/billing information (not including other transaction details linked to a credit card or account and not connected to the travel transaction)

9. Travel itinerary for specific PNR

10. Travel agency/travel agent

11. Code share information

12. Split/divided information

13. Travel status of passenger (including confirmations and check-in status)

14. Ticketing information, including ticket number, one way tickets and Automated Ticket Fare Quote

15. All baggage information

16. Seat information, including seat number

17. General remarks including OSI, SSI and SSR information

18. Any collected Advance Passenger Information System (APIS) information

19. All historical changes to the PNR listed in numbers 1 to 18

Comment [U54]: In Article 6 I make the comment that criminal related personal data is excluded from the list of "sensitive data" although usually such criminal data is treated as special personal data by most data protection regimes in Europe.

I speculated that this may be because the authorities might want to attach such criminal data and intelligence as part of the PNR data (see U25).

The EDPS has called for a shorter list containing no "sensitive data".

I also made the comment that the rights identified in Articles 6-13 are of little value **if they relate to just PNR data (which I think is correct from my reading of the text and the press release)**.

This Annex is the list of personal data that comprise PNR data and subject to the right of access and correction. That is why I say the rights are really of very little value

Although there will be circumstances where the rights could be useful for data subjects, I contend that for the vast majority of data subjects this list of items will be of little (probably no) interest at all.

Most of the data protection issues will reside in the other personal data (e.g. name of flyer shared with a known criminal etc and the authorities think the criminal is flying to the USA). It is the other personal data that needs correcting, updating etc.

Of course, the DHS will no doubt correct its records, but any damage to the data subject arises from the other information and not the PNR data.

Data subject rights are a central tenet of any data protection regime; there is no role for any data protection authority in connection with these rights.

ANNEX II

Declaration by the EU on the Agreement on the use and transfer of Passenger Name Records to the United States Department of Homeland Security ("the Agreement"), in respect of its obligations under Articles 17; and 23 of the Agreement.

1. In the context of the joint review and evaluation mechanism set out in Article 23 of the Agreement, and without prejudice to other matters that may be raised through this mechanism, the European Union will seek information from the US on the exchange of information where appropriate, regarding the transfers of European Union citizens' and residents' PNR data to the authorities of third countries as laid down in Article 17 of the Agreement;

2. In the context of the consultation and review mechanism set out in Article 23 of the Agreement, the EU will request from the US all appropriate information on the implementation of the conditions governing those transfers in accordance with the provisions of Article 17.

3. The EU, in the context of the consultation and review mechanism set out in Article 23 of the Agreement, will pay particular attention to the respect of all the safeguards for the implementation of the provisions of Article 17(2), so as to be satisfied that third countries receiving such data have agreed to afford to the data the privacy protections comparable to those provided to PNR by DHS under the Agreement.

Comment [U55]:

As we shall see this Annex does not apply to any use or internal USA disclosure made by the DHS; **it only applies to onwards transfers by the USA**

As this excludes Article 16 on Domestic sharing, it sends the message that the EU is not bothered as to what the USA does internally with PNR data.

The Article also excludes any data protection authority in the Review, but by now this is not a surprise.

Annotated Press Release issued by the Commission

(on http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/1368)

New EU-US agreement on PNR improves data protection and fights crime and terrorism

Brussels, 17 November 2011 – Today, the European Union and the United States have initialled a new agreement on the transfer of air passengers' data for flights from the EU to the US. If adopted by the European Parliament and EU Member States in the Council of Ministers, the new agreement on Passenger Name Records (PNR) will replace the current agreement from 2007, improving data protection whilst providing an efficient tool to fight serious transnational crime and terrorism.

The new PNR agreement brings more clarity and legal certainty to both citizens and air carriers. It ensures better information sharing by US authorities with law enforcement and judicial authorities from the EU, it sets clear limits on what purposes PNR data may be used for, and it contains a series of new and stronger data protection guarantees.

"*Protection of personal data has been my priority since the beginning of the negotiations in December 2010, and I am satisfied with the result, since it represents a big improvement over the existing Agreement from 2007. The new agreement contains robust safeguards for European citizens' privacy, without undermining the effectiveness of the agreement in terms of EU and US security,*" said Cecilia Malmström, EU Commissioner for Home Affairs.

The agreement is a legally binding text with **stronger rules on police and law enforcement cooperation**. The US authorities (Department of Homeland Security, DHS) will be obliged to share PNR and analytical information obtained from this data with law enforcement and judicial authorities of the EU in order to prevent, detect, investigate, or prosecute serious transnational crime or terrorist offences. This will be of direct benefit for the EU.

The agreement also gives a detailed description of the purposes for which PNR data may be used by US authorities. These are notably: the **prevention, detection, investigation and prosecution of terrorism and of transnational crimes** punishable by 3 years of imprisonment or more. Minor crimes are thus excluded. PNR will be used to tackle serious crimes, such as drug trafficking, trafficking in human beings and terrorism.

The agreement sets out privacy-friendly rules on **how and for how long PNR data may be stored.** Data will be de-personalised 6 months after it is received by the US authorities. After 5 years the de-personalised data will be moved to a 'dormant database' with stricter requirements for access by US officials. The total duration of data storage is limited to 10 years for serious transnational crimes. Only for terrorism will the data be accessible for 15 years.

The agreement establishes the rule that PNR data must be sent from air carriers' databases to the US authorities (through a **'push' system**). The DHS will thus not collect data directly from air carrier's reservation systems (through 'pull') except in exceptional circumstances, such as where carriers are not able to send the data for technical reasons.

Comment [U56]: I have decided to annotate the press release because it does not, in my view, even pass the standard of being "economical with the truth".

This Press Release turns "misleading by omission" into an art form..

Comment [U57]: This statement is misleading as the Agreement does not use the term "serious transnational crime" in its effective Articles. If the Agreement was limited to "serious transnational crime" and terrorism it would be less controversial. The Agreement also deals with issues that do not involve crime or terrorism. – See U1

Comment [U58]: The Press Release omits to say that:

- the "strong guarantees" of data protection are not supervised by any data protection authority, and that these authorities do not have an expressly defined role in upholding these "strong guarantees".
- the Agreement does not mention any a role for European Data Protection Authorities even when dealing with data protection issues (e.g. a serious data loss).
- the Agreement does not provide for proportionate data sharing as an obligation; it only expresses it at the level of an aspiration.

Comment [U59]: The Press release places an emphasis on serious transnational crime again. This is a term **not** found in the Agreement.

Comment [U60]: The Press release fails to mention the non-crime, non-terrorist related purposes in Article 4(2) and Article 4(3)

Comment [U61]: The Press release fails to stated that the Agreement only lasts 7 years. At the end of the 7 years, there is consultation on "whether any future EU PNR system would apply less stringent data protection standards than those provided for in the present Agreement". (i.e. consultation on lowering standards)

In other words, the Press release does not state that after 7 years there could be negotiated an extension of the 10 year retention of PNR data – see U31/U49 relating to Articles 8(6) and 20.

The agreement has comprehensive safeguards for passengers' **right to data protection**. Passengers can obtain access to correct and delete their PNR data at the DHS. Passengers also have the right to administrative and judicial redress as provided under US law. Further, the DHS and air carriers will have to provide full information to passengers on the use of PNR and the ways to exercise their rights.

In addition, the agreement prohibits adverse decisions from being taken by the US authorities only on the basis of **automated processing of data**, a human being must always be involved, to address concerns about PNR data being used for illegal profiling. It also lays down very strict conditions for the use of **sensitive data** which might reveal, for example, the religion or sexual orientation of passengers.

Finally, the agreement includes detailed provisions on **data security** to prevent loss of data or breaches of privacy. All processing of PNR data will be logged for the purposes of **oversight and auditing** and there will be oversight of the DHS by independent bodies, including the US Congress.

Background

In 2007, the European Union signed an agreement with the United States on the transfer and processing of Passenger Name Record (PNR) data, based on a set of commitments by the DHS. The 2007 agreement became provisionally applicable.

On 5 May 2010, the European Parliament adopted a resolution where it requested a renegotiation of the agreement. On 2 December 2010, the Council authorised the Commission to negotiate a new agreement with the US for the transfer of PNR data and discussions started immediately.

The purpose of the new agreement is to ensure the availability of PNR data to DHS, in order for it to be used in the fight against serious transnational crime and terrorism. PNR data of all flights between the EU and the US will be transferred by the air carriers to the US DHS. As in the 2007 agreement, the new agreement allows for 19 "data elements" to be transferred, such as passengers' names, travel itineraries and where they bought their tickets.

The new agreement takes into consideration and is consistent with the general criteria laid down in the Communication from the Commission on the Global Approach to the transfer of Passenger Name Record (PNR) data to third countries and the negotiating directives given by the Council

Note by CP: the comments in the margin explain why I think this Press Release turns "misleading by omission" into an art form.

Comment [U62]: Although the "rights" or safeguards only applies **to PNR data,** the press release fails to state that these are very limited (See Annex1 & U27-U39).

The access right is **just to PNR personal data** in Annex 1. This is a very minor right as one assumes the data subject knows which flight he caught and how he paid for it etc, and where he lives. Perhaps he is interested in what seat he sat in- then the right is useful!

In any event, the Press release fails to state that there is no role for the data protection authorities in upholding these rights.

Comment [U63]: The press release gives a misleading impression that it applies to all data; this is incorrect. The actual Article is limited to just to the **PNR data**.

Comment [U64]: The Press release fails to state that the audit and logging requirements are not independently determined or assessed. The DHS decides on its own audit and logging requirements and reports on them. No role for a data protection authority in the audit and logging.

Comment [U65]: The Press release fails to state that the Agreement does not even provide for serious data losses and privacy violations to be reported to the data protection authorities.

Comment [U66]: The Agreement does not use "serious trans national crime" as part of the text of the Agreement. The Agreement is not limited to terrorism and serious transnational crime.

ADVERT

COURSES FOR PRIVACY PRACTITIONERS OR DATA PROTECTION OFFICERS

Amberhawk provides a wide range of public training suitable for data protection officers in the UK. These include courses leading to the ISEB qualification in data protection which can be held on-site. ***We are the only course provider that delivers the data protection ISEB syllabus in public courses to ISEB's recommended length of time; all other provides reduce a 40 hour syllabus to 30 hours or less.***

With respect to on-site training, Amberhawk can provide sector specific training (e.g. on rights of access, CCTV, human resources, data sharing, direct marketing) or targeted at specific staff members (e.g. managers) or on specilisat aspects (e.g. social work functions, anti-fraud functions).

We have day long public courses in Data Protection Audit, Privacy Impact Assessments and RIPA as well as our popular, twice yearly, UPDATE session in London.

We will be soon delivering courses to ISEB's syllabus on Information Security Management (useful to those involved in implementing ISO27002 and HMG Security Framework). From April 2012 we suspect.

COURSES IN FREEDOM OF INFORMATION

Amberhawk provides a wide range of public training suitable for those dealing with Freedom of Information and the Environmental Information Regulations. These include courses leading to the ISEB qualification. ***We are the only course provider that delivers the FOI ISEB syllabus in public courses to ISEB's recommended length of time; all other provides reduce a 40 hour syllabus to 30 hours or less.***

With respect to on-site training, Amberhawk can provide sector specific training aimed at those helping a public authority meet its obligations. Courses can include Re-use Regulations by Public Sector Bodies.

If you ever get to read this line and want to attend our Leeds FOI course on 2nd February 2012, you have just earned a bonus; ***we will give you over £700 off, and charge you £1500+VAT.***