Statewatch Analysis

Making Fundamental Rights Flexible

The European Commission's Approach to Negotiating Agreements on the Transfer of Passenger Name Record (PNR) Data to the USA and Australia

Chris Jones

Passenger Name Record (PNR) data consists of various different pieces of information collected by airlines when an individual books a plane ticket. A list of nineteen different pieces of information to be passed onto law enforcement authorities has become standard, including names, frequent flyer information, all available contact information (address, phone number, and email), baggage information, as well as general remarks, which permits the provision of less standardised information.[1]

Following the terrorist attacks of 11th September 2001, the US government became interested in the potential use of PNR for the prevention, investigation or prosecution of terrorist acts. The provision of this information from airline carriers to the government has been a matter of fierce debate for a number of years, with those for the transfer of PNR data arguing that it is an indispensible tool in the 'fight against terrorism'. Those opposed point the gross invasion of privacy such transfers represent, and argue that there are no meaningful statistics demonstrating PNR is of any benefit. As the US began obliging airline carriers flying into the country to provide PNR data, other governments began to adopting similar policies. This has led to the signing by the European Union of a number of agreements on the transfer of PNR data. Such agreements have to date been signed between the EU and Australia, Canada and the US. Two updated agreements, between the EU and Australia and the EU and the USA, have recently

[1] The full list is: PNR record locator code; Date of reservation/issue of ticket; Date(s) of intended travel; Name(s); Available frequent flier and benefit information (i.e., free tickets, upgrades, etc.); other names on PNR, including number of travellers on PNR; All available contact information (including originator information); All available payment/billing information (not including other transaction details linked to a credit card or account and not connected to the travel transaction); Travel itinerary for specific PNR; Travel agency/travel agent; Code share information; Split/divded information; Travel status of passenger (including confirmations and check-in status); Ticketing information, including ticket number, one way tickets, and Automated Ticket Fare Quote; All baggage information; Seat information, including seat number; General remarks including OSI, SSI and SSR information; Any collected APIS information; All historical changes to the PNR listed in numbers 1 to 18.

emerged. This analysis examines the differing provisions of these two agreements in the context of the European Union's 'global approach' to negotiating agreements on the transfer of PNR data.

The Global Approach

In September 2010, the *Communication from the Commission on the global approach to transfers of Passenger Name Record (PNR) data to third countries* was published. A revision of guidelines and criteria for PNR agreements was deemed necessary due to the increase in the number of countries establishing systems for the receipt and analysis of PNR data. Following the entry into force of the Lisbon Treaty, the consent of the the European Parliament also became a necessity for the conclusion of any such agreements. It is the need for parliamentary approval that required the re-drafting of both the Australian and US agreements.

According to the Global Approach, the revisions "should ensure strong data protection guarantees and full respect of fundamental rights".[2] The development of the Global Approach, according to the Commission, took into account:

"The views on general PNR issues of the major stakeholders, like the Member States, the European Parliament, the European Data Protection Supervisor [EDPS] *and the Article 29 Data Protection Working Party* [A29WP]."[3]

The Global Approach provides a detailed outline of what the basis of PNR agreements with third countries should be. The EU-Australia Agreement and, most significantly, the EU-US Agreement, contradict these principles on numerous points.

Data Protection

The first issue provided with a set of underlying principles is data protection, and purpose limitation is the first area of concern identified. It is noted that PNR data:

"*Should be used only for law enforcement and security purposes to fight terrorism and serious transnational crime.*"[4]

Definitions of terrorism and transnational crime are supposed to be based on "the approach of definitions laid down in relevant EU instruments". It is clear that "the approach of definitions" provides room for manoeuvre on exactly what terrorism and transnational crime are. The agreements fail to provide reference to any EU definitions of the two concepts; the definitions that are used differ between the two documents. The Agreement with Australia defines serious crime as that with a sentence of four years or more, but for the US Agreement that threshold is one year lower at three years or more. Furthermore, the EU-US Agreement contains so

[2] European Commission, 'Communication from the Commission on the global approach to transfers of Passenger Name Record (PNR) data to third countries', 21 September 2010, COM(2010) 492 final, p.3
[3] Ibid., p.4
[4] Ibid., p.8

many derogations that PNR could conceivably be used for the prevention, investigation or prosecution of all manner of offences.

Similar problems with the Agreement stem from the use of sensitive data (i.e. political opinions, trade union membership, medical conditions, etc.), which allows its use in situations where a person's life is "imperilled or may be seriously impaired", as long as it is authorised by a senior manager. The Global Approach states that sensitive data may only be used:

"*Where is an imminent threat to loss of life and provided that the third country provides adequate safeguards.*"[5]

The EU-Australia Agreement does not permit any processing of sensitive data.

Data security is defined by the Global Approach as protecting PNR data:

"*Against misuse and unlawful access by all appropriate technical, security procedures and measures to guard against risks to the security, confidentiality or integrity of the data.*"[6]

The flexibility taken to these principles of the Global Approach is made evident through comparison of the two agreements. More detail is provided in the Annex, but it is clear that the European Commission has neglected the majority of the provisions of the Global Approach in its negotiations with the US. The Agreement with Australia, on the other hand, goes further than its own guidelines and provisions are made which address one of the criticisms made by the EDPS of the Global Approach: that the provisions regarding data security:

"*Could be complemented by an obligation of mutual information in case of security breach: recipients would be responsible for informing their counterparts in case data they received have been subject to unlawful disclosure.*"[7]

Oversight and Accountability

The next issue dealt with by the Global Approach is oversight and accountability. The Office of the Australian Information Commissioner has been granted oversight of the activities of the Australian Customs and Border Protection Service with relation to PNR, as is spelt out clearly in a number of articles. However, the US has no such public official, and the Department of Homeland Security (the primary, but by no means the only recipient of PNR data) is exempt from the US Privacy Act.[8] This means that in the US there is no "independent public authority" with "effective powers of intervention, enforcement, oversight, ensuring compliance with rules and hearing complaints from individuals", leaving the DHS to regulate

[5] Ibid.
[6] Ibid.
[7] European Data Protection Supervisor, 'Opinion of the European Data Protection Supervisor on the Communication from the Commission on the global approach to transfers of Passenger Name Record (PNR) data to third countries', 19 October 2010, p.8
[8] Statewatch News Online, 'US changes the privacy rules to exemption access to personal data', September 2007

itself. That the European Commission has been willing to negotiate an agreement with clear knowledge of this demonstrates its willingness to disregard supposedly fundamental rights.

A number of other issues discussed in the Communication on the Global Approach (transparency and notice; access, rectification and deletion; redress) have been the subject of a thorough analysis by Edward Hasbrouck,[9] and so will not be dealt with in detail here, although they are noted in the comparison below. Suffice to say that the EU-US Draft Agreement sets standards way below those of the Global Approach. The EU-Australia Agreement again fares better, although still leaves much to be desired.

Profiling

It is worth taking note of the provisions of both the Global Approach and the two agreements towards "automated individual decisions", that is, "decisions producing adverse actions or effects on individuals based on automated processing".[10] Examining the text of the two agreements demonstrate significant disparity between them. For example, the Australian authorities permitted to access PNR data "shall not take any decision which significantly affects or produces an adverse legal effect on a passenger solely on the basis of the automated processing of PNR data" (Article 15(1)), and "shall not carry out the automated processing of data on the basis of sensitive data" (15(2)). The EU-US Agreement states that "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 7, emphasis added). This is far less prohibitive, and in fact permits automated processing as long as any resulting adverse action is not significant – a term for which no definition is provided.

Such automated processing would most likely take place either in 'real time' or in a 'pro-active' fashion. The use of PNR data in real time is described by the Commission as:

Use in order to prevent a crime, survey or arrest persons before a crime has been committed or because a crime has been or is being committed. In such cases PNR are necessary for running against predetermined fact-based risk indicators in order to identify the previously "unknown" suspects and for running against various databases of persons and objects sought.

Pro-active (patterns) means:

Use for trend analysis and creation of fact-based travel and general behaviour patterns, which can then be used in real time use. In order to establish travel and behaviour patterns, trend analysts need to be allowed to use the data over a

[9] Edward Hasbrouck, 'European Commission wants to immunize DHS collaborators in travel surveillance and control', May 27 2011
[10] COM(2010) 492 final, p.9

sufficiently long period of time. A commensurate period of retention of the data by law enforcement authorities is necessary in such cases.[11]

Such use of PNR data essentially amounts to profiling. The EDPS has noted that it is easy to confuse notions such as "risk indicators" and "risk assessment" with profiling, and such confusion is:

Strengthened by the alleged objective which is to establish "fact based travel and behavioural patterns". The EDPS questions the link between the original facts, and the patterns deducted from these facts. The process aims at imposing on an individual risk assessment - and possible coercive measures - based on facts which are not related to the individual.[12]

It also raises important questions of by whom the profiles are created, and for what ends – particularly when the use of PNR data in the EU-US Agreement is not limited to the prevention, investigation and prosecution of terrorism or serious transnational crime.

Retention

Following the issue of automated individual decisions, the Global Approach moves on to discuss the retention of data, stating that "the period of retention… should not be longer than necessary for the performance of the defined tasks".[13] It would seem that the tasks the US may wish to undertake using PNR data are particularly extensive, given that they are permitted to hold it for ten years longer than the Australian authorities. The Article 29 Working Party has argued that the period of retention should be uniform for all PNR agreements the EU makes with third countries,[14] while the EDPS has stated that:

"*PNR data should be deleted if the controls made at the occasion of the transmission of data have not triggered any enforcement action.*"[15]

While the Commission has not abrogated any of its stated principles on data retention in the two agreements, this particular set of standards are not particularly stringent in the first place. Regardless of what the Global Approach says, it is clear that the periods of retention in both agreements are disproportionate to the principles of EU data protection and human rights law. The Australian authorities are permitted to retain data for five years; the USA is able to do so for up to 15 years if it is deemed necessary.

---

[11] COM(2010) 492 final, p.4
[12] 'Opinion of the European Data Protection Supervisor on the Communication from the Commission on the global approach to transfers of Passenger Name Record (PNR) data to third countries', p.5
[13] European Commission, 'Proposal for a Council Decision on the signature of the Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service' 19 May 2011, COM(2011) 280 final, p.9
[14] Article 29 Working Party, 'Opinion 7/2010 on European Commission's Communication on the global approach to transfers of Passenger Name Record (PNR) data to third countries', 12 November 2010, p.6
[15] 'Opinion of the European Data Protection Supervisor on the Communication from the Commission on the global approach to transfers of Passenger Name Record (PNR) data to third countries', p.7

The final section of the Global Approach dealing with data protection addresses onward transfers, both to other government authorities and to third countries. The relevant articles differ in length to such a degree that anyone examining the two agreements from a distance would be able to make an informed guess that the EU-US Agreement is far less restrictive than the EU-Australia Agreement. The extent to which this is the case is outlined in detail in the chart below. The Australian government authorities permitted to receive PNR data from the Customs and Border Protection Service are outlined in an annex to the Agreement, and appear to meet the criteria of the Global Approach – that PNR data:

"*Should only be disclosed to other government authorities with powers in the fight against terrorism and serious transnational crime.*"[16]

Presumably these authorities will also be subject to oversight by the Office of the Australian Information Commissioner. Restrictions on the transfer of data to other government authorities in the US are, on the other hand, far less like restrictions than those outlined in the EU-Australia Agreement. They will essentially be available to **any other government department** as long as the DHS deems it necessary. The same is also true of onward transfers by US authorities to the authorities of third countries – where PNR data may end up under the terms of the EU-US Agreement is anyone's guess. The principles of the Global Approach to such transfers are unfortunately reflective of other provisions made in the EU's agreements – that is, onward transfers from one third country to another:

"*Shall be subject to appropriate safeguards… [onward transfers shall be made] only if the latter undertakes to treat the data with the same level of protection set out in the agreement and the transfer is strictly limited to the purposes of the original transfer of the data.*"[17]

The low level of protection and oversight afforded data transferred from the EU to the US therefore means that information contained in any further transfers will be subject to similarly low levels of protection.

Modalities of transmissions

The next section of the Global Approach deals with 'modalities of transmissions' – i.e. the ways in which data should be transferred. With regard to the method of transmission itself, the Global Approach seemed adamant that only the 'push' method should be used, in order to "safeguard the data that is contained in the carriers' databases and to maintain their control thereof".[18] The 'push' method means that:

Air carriers transfer ('push') the required PNR data to the authority requesting them, thus allowing air carriers to retain control of what data is provided. The

[16] COM(2010) 492 final, p.9
[17] Ibid.
[18] Ibid.

'push' method is considered to offer a higher degree of data protection and should be mandatory for all air carriers.[19]

The other option available is the 'pull' method, "under which the competent authorities of the Member State requiring the data can reach into (access) the air carrier's reservation system and extract ('pull') a copy of the required data". It is unfortunate for the principles of the Global Approach that the US has in fact been using a variant on the pull method to obtain information from air carriers' Computer Reservations Systems (CRS).[20] Although this is not explicitly noted in the Draft Agreement, the provisions that allow the DHS to derogate from using the push method seem to make clear that the Commission's negotiators were either unable or unwilling to stand up for the principle of using only the push method. The EDPS noted, specifically with regard to access by US authorities to CRS, that "legal and technical measures should be taken to prevent any bypassing of the 'push' system."[21]

In contrast to the provisions of the EU-US Agreement, two separate articles (20 and 21) of the EU-Australian Agreement make clear that the push method will be the only way for the Australian authorities to obtain PNR data; conditions are also attached to Article 20 where this is first outlined.

Next up is the frequency of transmission, for which the Global Approach states that:

"*There should be a reasonable limit to the number of times the third country requires the data to be transmitted to it, which ensures an adequate benefit to security while minimising the costs of the carriers.*"[22]

It is hard to say what constitutes a reasonable limit, but it is worth pointing out that the US is more stringent in its demands for transfers – it initially requires PNR to be transferred by the air carrier 96 hours before a flight departs. Article 15 (in which frequency of transfer is outlined) also provides the loophole by which US authorities are able to continue using the 'pull' method of PNR data transfer.

Finally, the section on modalities of transmissions states that there should be no obligation placed on air carriers to collect additional data; they should "only be required to transmit what they already collect as part of their business".[23] While this is a welcome addition to the Global Approach, it is not hard to see it being discarded in the future if it deemed necessary for airlines to collect more extensive information from passengers. This has happened before with regard to migration, rather than just movement. In their attempts to deter asylum seekers and other unpopular types of migrant, the European Union and other governmental

[19] European Commission, 'Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime', COM(2011) 32 final, 2 February 2011, p.16
[20] 'European Commission wants to immunize DHS collaborators in travel surveillance and control'
[21] 'Opinion of the European Data Protection Supervisor on the Communication from the Commission on the global approach to transfers of Passenger Name Record (PNR) data to third countries', p.8
[22] COM(2010) 492 final, p.10
[23] Ibid.

authorities across the globe have placed sanctions on those airlines that permit individuals to travel when they do not have the correct documents. Requirements of security are perfectly capable of overriding the need to minimise the costs of business.

Overarching concepts

The concepts referred to by the Commission relate to duration and review; monitoring; dispute resolution; and reciprocity. The theme that has developed so far in the two agreements – the discarding of principles – continues with relation to these issues. As regards monitoring, duration and review, the Global Approach states that:

"*It is essential that the EU is provided with mechanisms for monitoring the correct implementation, for example through periodical joint reviews on the implementation of all aspects of the agreements, including the purpose limitation, the rights of passengers and onward transfers of PNR data, and comprising a proportionality assessment of the retained data on the basis of their value to achieving the purposes for which the data were transferred.*"[24]

Both agreements include articles relating to joint reviews. However, in both cases provisions that would ensure would thorough and binding oversight are lacking. The A29WP noted in their opinion on the Global Approach that "joint reviews should also include representatives of the European data protection authorities". [25] Article 24 of the EU-Australian Agreement contains the non-binding statement that review teams "may include experts on data protection and law enforcement". The EU-US Agreement is non-binding in a similar fashion, and also includes the word "appropriate": "teams may include appropriate experts on data protection and law enforcement". There is thus no certainty that data protection authorities, or even data protection experts, will be included in any reviews that take place of the agreements. Furthermore, the US Agreement does not mention the need for reviews to discuss specific issues of concern, whereas Article 24(2) the Australian Agreement notes the agreement of the parties on the need to discuss:

The mechanism of masking out data according to Article 16(1)(b), any difficulties related to the operational efficiency or cost effectiveness of the mechanism, and experience acquired with similar mechanisms in other mature PNR schemes, including the EU scheme.

It is also notable that this sentence seems to treat the recently-proposed EU PNR scheme as a *fait accompli*.

Were the parties to come into dispute over any issue contained or related to the agreements, the two agreements also provide significantly differing methods of resolution. For example, the EU or Australia may seek consultation for any dispute

[24] Article 29 Working Party, '[Opinion 7/2010 on European Commission's Communication on the global approach to transfers of Passenger Name Record (PNR) data to third countries]', 12 November 2010, p.10
[25] Ibid., p.7

"arising from the interpretation, application or implementation" (Article 23(1)) of the agreement. The EU or US may only seek consultation with the other party for any dispute arising from its implementation (Article 24(1)). There thus seems to be very little room for manoeuvre in the event that the European Union wished to extricate itself from the EU-US arrangement on grounds other than those related to the implementation of the agreement – for example, if the US authorities were interpreting provisions in a manner inconsistent with the drafters' intentions. Once again the terms laid down in the Global Approach have been ignored: it is stated in that document that "[e]ffective dispute resolution mechanisms with respect to interpretation, application and implementation of agreements should be provided".[26]

The lack of specificity provided in the EU-US Agreement with regard to use of PNR data following termination of the agreement also differs markedly from that in the EU-Australia Agreement. Any data obtained by the Australian Customs and Border Protection Service:

"*Shall continue to be processed in accordance with the safeguards of this Agreement, including the provisions on retention and deletion of data*" (Article 23(4))

That held by the US following termination of the agreement is not subjected to a specific mention of provisions on retention and deletion. Rather, it "shall continue to be processed and used in accordance with the safeguards of this Agreement" (24(3)). The "proportionality assessment of the retained data" mentioned in the Global Approach would seem to be applicable to such situations, but neither agreement mentions the need for such an assessment.

It is also worth briefly mentioning the terms of reciprocity in each agreement. The idea of reciprocity is that analytical data obtained from the assessment and processing of PNR data will be shared by the authorities of Australia and the US with the police and judicial authorities of the EU (Europol and Eurojust) and the Member States. Both agreements have articles dealing with police, law enforcement and judicial cooperation (Article 6 EU-Australia, Article 18 EU-US). The Australian Agreement ensures "the availability, as soon as practicable, of relevant and appropriate analytical information" to European authorities. The equivalent article in the EU-US Agreement is far more restrictive in its wording, permitting the transfer of such information only to "competent" authorities, and "as soon as practicable, relevant, and appropriate". It will of course be up to the Department of Homeland Security to decide what "practicable, relevant and appropriate" mean. The Global Approach's statement that "reciprocity should be ensured" rings a little hollow when compared to the provisions of the EU-US Agreement.

[26] Ibid., p.10

Constructive criticism

The opinions of the EDPS and the A29WP raised concerns about the Commission's approach. Significant criticism stemmed from the fondness of authorities for using PNR as a law enforcement tool. As the A29WP stated:

"*There are no objective statistics of evidence which clearly show the value of PNR data in the international fight against terrorism and serious transnational crime.*"[27]

In the absence of such statistics, most of the justifications used for PNR schemes are anecdotes about particular cases where PNR data has been used to successfully apprehend an individual suspected of involvement with crime. Two such anecdotes were provided by the European Commission in its impact assessment for its own proposal for a PNR scheme covering flights into the European Union.[28] However, such anecdotes provide no proof of the necessity or proportionality of PNR schemes. As noted by the EDPS, the development of PNR schemes seems to be based more on the fact that the technological means to do so are now available, rather than on any evidence that they are effective to such a degree that they justify the systematic collection and processing of personal data of every individual on a particular flight.[29] This accusation raises serious questions about the role of defence, security and technology companies in marketing to governments technological 'solutions' for a variety of issues.

Individual rights - fundamental or flexible?

The lack of protection the Draft Agreement makes available for the data of individuals flying from the EU to the USA is indicative of the Commission's flexible approach to its standards for negotiating PNR agreements. Some particularly interesting comments from the EDPS concerned the fact that the Communication was accompanied:

"*By Recommendations for negotiations of PNR agreements with specific third countries. These Recommendations are restricted and not analysed in this opinion.*"[30]

The Recommendations have not yet come to light. However, the EDPS later goes on to point out that "the margin of manoeuvre for each international agreement should be as limited as possible",[31] implying that the Recommendations should not permit significant derogation from the guidelines laid out in the Global Approach.

---

[27] Ibid., p.3
[28] European Commission, 'Impact Assessment, Accompanying document to the Proposal for a European Parliament and Council Directive on the use of Passenger Name Record data for the prevention, investigation and prosecution of terrorist offences and serious crime', SEC(2011) 132, p.12
[29] 'Opinion of the European Data Protection Supervisor on the Communication from the Commission on the global approach to transfers of Passenger Name Record (PNR) data to third countries', p.4
[30] Ibid., p.9
[31] Ibid., p.4

The explanatory memorandum accompanying the proposed EU-Australia Agreement states that it:

"*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.*"[32]

The EU-Australia has a number of significant problems, but it contains significantly better data protection provisions that the EU-US Agreement, which bears little to no resemblance to the general criteria outlined in the Global Approach.

Overall, it seems clear that the criteria outlined in the Global Approach have little significance for the Commission's negotiators, who have apparently been willing to play fast and loose with fundamental rights, which are of course supposedly the underlying principles that bond the countries of the European Union together. Of course, the Agreements make similar claims – in the preamble to the EU-US text, both parties' "longstanding traditions of respect for individual privacy, as reflected in their laws and founding documents" are duly noted.

The EU-US Agreement is also indicative of the status of the US as the sole global superpower, with its negotiators used to setting the agenda in diplomatic relations with other countries. As the campaign group European Digital Rights Initiative has pointed out, the "far-reaching document will soon be given to the Member States and European Parliament on a "take it or take it" basis," but:

"*The European Commission appears to have forgotten that any agreement that it signs must respect existing obligations on fundamental rights. In this case, the privacy rights in the European Convention on Human Rights and the Treaty on the Functioning of the European Union must be respected. It appears almost certain that the Agreement fails to meet minimum standards for fundamental rights.*"[33]

It would in fact take a seriously distorted interpretation of both the European Convention on Human Rights and the Treaty on the Functioning of the European Union to come to the view that the provisions of the EU-US Agreement are compatible with fundamental rights.

A similar, if less harsh, accusation could be levelled at the EU-Australia Agreement. Considering that the Charter of Fundamental Rights (as incorporated into the TFEU) is now legally binding upon the institutions of the European Union, it is hard not to see the EU-US Draft Agreement as an admission by the European Commission that it is willing to participate in contravening EU law. Indeed, were the Agreement even to be approved by the European Parliament, it would have no force in US law. This is because as an agreement, unlike a treaty, it would not be presented to the US Senate for ratification and would therefore have no binding

[32] COM(2011) 280 final, p.3
[33] European Digital Rights Initiative, 'Commission Plans to Present Flawed, Illegal PNR Proposal as "Fait Accompli"', 23 May 2011,

force according to the US Constitution.[34] It thus is more of a press release than a document of legal force or significance, which serves to legitimise the Department of Homeland Security's ongoing collection and transfer of Europeans' PNR data. That collection and transfer, it has been alleged, is illegal.[35] That the European Commission is willing to carry on with such legitimation should raise serious questions when the Agreement comes before both the European and national parliaments.

It is important to note that while the Agreement and Draft Agreement both contain derogations from fundamental rights obligations, they are not isolated infringements on privacy and data protection. Rather, they are both a small part of a swiftly-expanding administrative machinery that seeks to collect and collate as much information about individuals as possible, supposedly in the name of safety and security. As noted above, the problem is not necessarily with the two PNR schemes analysed here – rather, the problem is with PNR schemes as a whole. The answer to suggestions that they are ineffective is not to suggest greater, more widespread collection of data, or even to permit such schemes to go ahead as long as they have sufficient safeguards. Rather, it is necessary to challenge the fundamental premises on which such schemes are based. The mass surveillance and monitoring of individuals' movements and activities does not lead to security for free societies. Rather, it undermines their very basis.

[34] 'European Commission wants to immunize DHS collaborators in travel surveillance and control'
[35] Ibid.

Annex 1
Comparison chart of the EU-Australia Agreement and the EU-US Draft Agreement on the use and transfer of Passenger Name Record (PNR) data

The chart below is laid out so as to allow direct comparison between the relevant articles of the Agreement and the Draft Agreement. The articles in the EU-Australia Agreement are laid out in numerical order, although this pattern is deviated from where it is necessary to bundle two different articles together so they can be compared with the relevant article(s) from the EU-USA Agreement. Comments are provided beneath relevant articles to outline the issues at hand.

Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service	**Draft Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Record data to the United States Department of Homeland Security**
Preamble	
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 the EU-Australian partnership; RECOGNISING that information sharing is a fundamental component of the fight against terrorism and serious transnational crime, and in this context	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; RECOGNlZING the right and responsibility of states to ensure the security of their citizens and protect their borders and mindful of the responsibility of

the use of Passenger Name Record (PNR) data is an essential tool; RECOGNISING the importance of preventing and combating terrorism and serious transnational crime, while respecting fundamental rights and freedoms, in particular, privacy and the protection of personal data; MINDFUL of 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, Articles 7 and 8 of the Charter of Fundamental Rights of the European Union and Article 17 of the International Covenant on Civil and Political Rights on the right to privacy; RECOGNISING that, in 2008, Australia and the EU signed the Agreement Between the European Union and Australia on the Processing and Transfer of European Union – Sourced Passenger Name Record (PNR) Data by Air Carriers to the Australian Customs Service which is applied provisionally from the time of signature but has not entered into force; NOTING that the European Parliament decided on 5 May 2010 to postpone the vote on the request for consent to that Agreement and by its Resolution of 11 November 2010 welcomed the recommendation from the European Commission to the Council of the European Union to negotiate a new agreement; RECOGNISING the relevant provisions of the Australian Customs Act 1901 (Cth) (the Customs Act), and in particular section 64AF thereof whereby, if requested, all international passenger air service operators, flying to, from or through Australia, are required to provide the Australian Customs and Border Protection Service with PNR data, to the extent that they are	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 offences and serious 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 offences and serious 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; 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

collected and contained in the air carrier's reservations and departure control systems, in a particular manner and form; RECOGNISING that the Customs Administration Act 1985 (Cth), the Migration Act 1958 (Cth), the Crimes Act 1914 (Cth), the Privacy Act 1988 (Cth), the Freedom of Information Act 1982 (Cth), the Auditor-General Act 1997 (Cth), the Ombudsman Act 1976 (Cth) and the Public Service Act 1999 (Cth) provide for data protection, rights of access and redress, rectification and annotation and remedies and sanctions for misuse of personal data; NOTING the commitment of Australia that the Australian Customs and Border Protection Service processes PNR data strictly for the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious transnational crime in strict compliance with safeguards on privacy and the protection of personal data, as set out in this Agreement; STRESSING the importance of sharing of analytical data obtained from PNR by Australia with police and judicial authorities of Member States, and Europol or Eurojust, as a means to foster international police and judicial cooperation; AFFIRMING that this Agreement does not constitute a precedent for any future arrangements between Australia and the European Union, or between either of the Parties and any State, regarding the processing and transfer of PNR data or any other form of data and noting that the necessity and feasibility of similar arrangements for sea passengers may be examined; HAVE AGREED AS FOLLOWS:	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; 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:
Comments	Even from the Preamble of the EU-US Draft Agreement it is clear that it goes beyond the purpose of investigating terrorist offences or serious transnational crime – note the provision that states 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'. There is also one mention of the need to fight "crime and terrorism", discarding the prefix of transnational or serious that is used in the rest of the Preamble. It is also noteworthy that it seems the Preamble is written in American English, with 'z' replacing 's' in a number of words, unlike the EU-Australia agreement. The EU-Australia agreement also contains specific references to the legal rules underlying access to personal information, and the possibility of rectification and deletion. The EU-US Agreement contains nothing as specific. Instead, it merely has general references to the DHS

	commitment to providing an "adequate level of data protection". A cynic might suggest that the number of references to the DHS' ability to uphold privacy and data protection rights is suggestive of the fact that they either cannot, or will not. Both agreements also confirm that discussions will take place on the collection and exchange of PNR data of persons travelling by sea to both Australia and the US. This is also being discussed by European Union Member States, as is the surveillance of movement by road.[36] The likely outcome of such discussions would be proposals for the total surveillance of all movement by vehicle, whether within or between states.		
Chapter I General Provisions			
Article 1	**Purpose**	**Article 1**	**Purpose**
	To ensure the security and safety of the public this Agreement provides for the transfer of EU-sourced PNR data to the Australian Customs and Border Protection Service. This Agreement stipulates the conditions under which such data may be transferred and used, and the manner in which the data shall be protected.		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.
Comments	Although this article merely provides an introduction, the difference in language goes some way towards indicating the substantive differences that are made apparent through a comparison of the two agreements. Whereas the EU-Australian agreement aims to 'ensure the security and safety of the public', the EU-US agreement aims to 'ensure security and to protect the life and safety of the public'. The reference to a generalised 'security' indicates the expansive approach taken in the EU-US agreement towards accessing and sharing data.		
Article 2	**Definitions**		
	For the purposes of this Agreement: (a) 'Agreement' shall mean this Agreement and its Annexes, and any amendments thereto; (b) 'personal data' shall mean any information relating		

[36] Marie Hynes, 'Statewatch Analysis: Proposal for a Directive on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime', 14 March 2011

	to an identified or identifiable natural person: an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity; (c) 'processing' shall mean any operation or set of operations which is performed upon PNR data, whether or not by automatic means, such as collection, recording, organisation, retention, adaptation or alteration, retrieval, consultation, use, disclosure by transmission or transfer, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction; (d) 'air carriers' shall mean air carriers that have reservation systems and/or PNR data processed in the territory of the European Union and operate passenger flights in international air transportation to, from or through Australia; (e) 'reservation systems' shall mean an air carrier's reservation system, departure control system or equivalent systems providing the same functionalities; (f) 'Passenger Name Record data' or 'PNR data' shall mean the information processed in the EU by air carriers on each passenger's travel requirements as listed in Annex 1 which contains the information necessary for processing and control of reservations by the booking and participating air carriers; (g) 'passenger' shall mean passenger or crew member including the captain; (h) 'sensitive data' shall mean any personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or health or sex life.		
Comments	An article clearly outlining the definitions of terms used – a standard part of the vast majority of legal agreements – are notable by their		

	absence from the EU-US agreement. Were it to enter into force, this would presumably permit unilateral interpretation of the Draft Agreement by the US authorities.		
Article 3	**Scope**	**Article 2**	**Scope**
	1. Australia shall ensure that the Australian Customs and Border Protection Service processes PNR data received pursuant to this Agreement strictly for the purpose of preventing, detecting, investigating and prosecuting terrorist offences or serious transnational crime: 2. Terrorist offences shall include: (a) acts of a person that involve violence, or are otherwise dangerous to human life or create a risk of damage to property or infrastructure, and which, given their nature and context, are reasonably believed to be committed with the aim of: (i) intimidating or coercing a population; (ii) intimidating, compelling, or coercing a government or international organisation to act or abstain from acting; (iii) seriously destabilising or destroying the fundamental political, constitutional, economic, or social structures of a country or an international organisation; (b) assisting, sponsoring or providing financial, material or technological support for, or financial or other services to or in support of, acts described in a); (c) 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 a) or b); or (d) aiding, abetting, or attempting acts described in a), b) or c). 3. Serious transnational crime shall mean any offence punishable in Australia by a custodial sentence or a detention		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 4	**Use of PNR**
			1. The United States collects, uses and processes PNR for the purposes of preventing, detecting, investigating, and prosecuting: a. Terrorist offences and related crimes, including i. Conduct that - 1. involves a violent act or an act dangerous to human life, property, or infrastructure; and 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

	order for a maximum period of at least four years or a more serious penalty and as it is defined by the Australian law, if the crime is transnational in nature. A crime is considered as transnational in nature in particular if: (a) it is committed in more than one country; (b) it is committed in one country but a substantial part of its preparation, planning, direction or control takes place in another country; (c) it is committed in one country but involves an organised criminal group that engages in criminal activities in more than one country; or (d) it is committed in one country but has substantial effects in another country. 4. In exceptional cases, PNR data may be processed by Australia where necessary for the protection of the vital interests of any individual, such as risk of death, serious injury or threat to health. 5. In addition, for the purpose of supervision and accountability of public administration and the facilitation of redress and sanctions for the misuse of data, PNR data may be processed on a case-by-case basis where such processing is specifically required by Australian law.		by mass destruction, assassination, kidnapping, or hostage-taking. ii. Activities constituting an offense with in 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. 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.
Comments	The use of PNR that US authorities are permitted by the agreement is significantly broader than that permitted to the Australian authorities. The idea of a 'serious threat' and the 'protection of vital interests of any individual' have no definitions or explanations attached. The equivalent article in the EU-Australia Agreement (3(4)) provides some clarity on this, although the phrasing – 'such as' – could be interpreted more widely than is desirable. The EU-US Draft Agreement also outlines the ability of a court to order the use of PNR information, but provides no justificatory criteria – presumably a judge could demand it be used in the investigation or prosecution of a case related to any particular misdemeanour, rather than just terrorism or serious transnational crime. EU-US Article 4(3) also makes clear that the DHS will be using PNR information to screen passengers whom they consider to represent a risk or threat on grounds other than related to terrorism or serious transnational crime. On what basis these decisions will be made is unclear. The Commission is encouraging the adoption of an agreement that steps way over the bounds laid down by the Global Approach, which states that 'PNR data should be used only for law enforcement and security purposes to fight terrorism and serious transnational crime.'[37] Furthermore, changes from earlier drafts also widen the scope. Article 4(3) previously read "To ensure border security, for the purposes set forth in Article I, 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 for the uses as outlined in paragraph 1 of this		

[37] COM(2010) 492 final, p.8

	Article." The removal of the first and last phrases loosens the grounds on which PNR data may be used, and for what it may be used.		
Article 4	**Ensuring provision of PNR data**	**Article 3**	**Provision of PNR**
	1. Air carriers shall provide PNR data contained in their reservation systems to the Australian Customs and Border Protection Service. They shall not be prevented by any provision of the law of either Party from complying with relevant Australian law which obliges them to so provide the data. 2. Australia shall not require air carriers to provide PNR data elements which are not already collected or held in their reservation systems. 3. Should PNR data transferred by air carriers include data beyond those listed in Annex 1, the Australian Customs and Border Protection Service shall delete it.		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.
Comments	The EU-Australia agreement is far more comprehensive with regard to the requirements placed on air carriers, with 4(2) noting specifically that the Australian authorities cannot place new requirements on carriers to collect data. The EU-USA agreement is nowhere near as clear. It also notes that the provision of PNR data will take place 'in accordance with DHS standards and consistent with this agreement' – those standards can presumably be as broad or demanding as the DHS wishes.		
Chapter II Safeguards applicable to the processing of PNR data			
Article 5	**Adequacy**	**Article 19**	**Adequacy**
	Compliance with this Agreement by the Australian Customs and Border Protection Service shall, within the meaning of relevant EU data protection law, constitute an adequate level of protection for PNR data transferred to the Australian Customs and Border Protection Service for the purpose of this		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.		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.
Comments	The idea that the DHS is able to provide a level of protection of an adequate level within the meaning of relevant EU data protection law is laughable. The DHS is exempt from the US Privacy Act 1974, and 'no privacy or data protection laws apply to PNR data held by the DHS'.[38] Even if it the DHS was subject to standards equivalent to EU data protection law, the law used as a basis for PNR negotiations according to the Commission's Global Approach is Framework Decision 2008/977/JHA 'on the on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters'. This has a number of serious loopholes in itself.		
Article 6	**Police and judicial cooperation**	**Article 18**	**Police, law enforcement and judicial cooperation**
	1. The Australian Customs and Border Protection Service shall ensure the availability, as soon as practicable, of relevant and appropriate analytical information obtained from PNR data to police or judicial authorities of the Member State concerned, or to Europol and Eurojust, within the remit of their respective mandates, and in accordance with law enforcement or other information sharing agreements or arrangements between Australia and any Member State of the European Union, Europol or Eurojust, as applicable. 2. A police or judicial authority of a Member State of the European Union, or Europol or Eurojust, within the remit of their respective mandates, may request access to PNR data or relevant and appropriate analytical information obtained from PNR data which is necessary in a specific case to prevent, detect, investigate, or prosecute within the European Union a terrorist offence or serious transnational crime. The Australian Customs and Border Protection Service shall, in accordance with the agreements or arrangements referred to in 1, make such information available.		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 specialised 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 serious 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 serious transnational crime. 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

[38] 'European Commission wants to immunize DHS collaborators in travel surveillance and control'

			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.
Comments	While the Australian authorities are bound to 'ensure, the availability, as soon as practicable, of relevant and appropriate analytical information obtained from PNR data' to EU authorities, the US authorities will do so 'as soon as practicable, relevant, and appropriate', giving far more room to manoeuvre when making decisions regarding whether to supply information to EU Member State or EU authorities. Further conditions are applied in the EU-USA agreement through Article 18(3), giving the US authorities far more control over the information they extract from PNR data. Were the DHS to decide not to share any such information – if it were not 'practicable, relevant, and appropriate' – then they would not be obliged to do so.		
Chapter III Modalities of Transfers			
Article 7	**Data protection and non-discrimination**	**Article 9**	**Non-discrimination**
	1. PNR data shall be subject to the provisions of the Privacy Act 1988 (Cth) (Privacy Act) which governs the collection, use, storage and disclosure, security and access and alteration of personal information held by most Australian Government departments and agencies. 2. Australia shall ensure that the safeguards applicable to the processing of PNR data under this Agreement and relevant national laws apply to all passengers without discrimination, in particular on the basis of nationality or country of residence or physical presence in Australia.		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.

Comments	Note the qualifier – 'unlawful' – that applies to discrimination exercisable by US authorities.		
Article 8	**Sensitive data**	**Article 6**	**Sensitive data**
	Any processing by the Australian Customs and Border Protection Service of sensitive PNR data shall be prohibited. To the extent that the PNR data of a passenger which is transferred to the Australian Customs and Border Protection Service include sensitive data, the Australian Customs and Border Protection Service shall delete it.		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 which 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 the U.S. law for the purpose of a specific investigation, prosecution or enforcement action.
Comments	The exemptions for the DHS require little explanation. Suffice to say that US authorities would essentially be able to do as they wish with sensitive data under the proposed agreement, as long such activity is approved by a DHS senior manager. When assessing the Commission's Global Approach, the EDPS remarked that there should be 'a complete exclusion of the processing of sensitive data, as a principle'.[39] The Commission included exceptions in its own Global Approach which the EDPS considered too broad, and those here are even broader.		

[39] 'Opinion of the European Data Protection Supervisor on the Communication from the Commission on the global approach to transfers of Passenger Name Record (PNR) data to third countries', p.6

Article 9	Data security and integrity	Article 5	Data security
	1. To prevent accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access or any unlawful forms of processing: (a) PNR data-processing equipment shall be held in a secure physical environment, and maintained with high-level systems and physical intrusion controls; (b) PNR data shall be stored separately from any other data. For the purpose of matching, data may flow to the PNR system, but not from the PNR system to other databases. Access to the PNR system shall be limited to a restricted number of officials within the Australian Customs and Border Protection Service who are specifically authorised by the Chief Executive Officer to process PNR data for the purpose of this Agreement. These officials shall access the PNR system in secure work locations that are inaccessible to unauthorised individuals; (c) Access to the PNR system, by the officials described in b) shall be controlled by security access systems such as layered logins using a user ID and password; (d) Access to the network of the Australian Customs and Border Protection Service and any data contained in the PNR system shall be audited. The audit record generated shall contain the user name, the work location of the user, the date and time of access, the content of the query and the number of records returned; (e) All PNR data shall be transferred from the Australian Customs and Border Protection Service to other authorities in a secure manner; (f) The PNR system shall ensure fault detection and reporting; (g) PNR data shall be protected against any manipulation, alteration or addition or corruption by		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, or 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

	means of malfunctioning of the system; (h) No copies of the PNR database shall be made, other than for disaster recovery back-up purposes. 2. Any breach of data security, in particular leading to accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access or any unlawful forms of processing shall be subject to effective and dissuasive sanctions. 3. The Australian Customs and Border Protection Service shall report any breach of data security to the Office of the Australian Information Commissioner, and notify the European Commission that such a breach has been reported.		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.
Article 17	**Logging and documentation of PNR data**		
	1. All processing, including accessing and consulting or transfer of PNR data as well as requests for PNR data by the authorities of Australia or third countries, even if refused, shall be logged or documented by the Australian Customs and Border Protection Service for the purpose of verification of lawfulness of the data processing, self-monitoring and ensuring appropriate data integrity and security of data processing. 2. Logs or documentation prepared under paragraph 1 shall be used only for oversight and auditing purposes including investigation and resolution of matters pertaining to unauthorised access. 3. Logs or documentation prepared under paragraph 1 shall be communicated on request to the Australian Information Commissioner. The Australian Information Commissioner shall use this information only for the oversight of data protection and for ensuring proper data processing as well as data integrity and security.		
Comments	The EU-Australia agreement's provisions regarding data integrity and security are far more stringent than the equivalent provisions contained in the EU-USA agreement. While only 'a restricted number of officials within the Australian Customs and Border Protection Service who are specifically authorised' will be able to access and process PNR data, in the US 'access to PNR shall be secured and limited to specifically		

	authorised officials' – these could presumably be from any governmental department or agency. It is also noted in the Australian agreement that the individuals granted access must be authorised by the 'Chief Executive Officer' in order to 'process PNR data for the purpose of this agreement'. The EU-Australia agreement also makes clear that 'data may flow to the PNR system, but not from the PNR system to other databases', something afforded no attention in the EU-US agreement. With regard to 'privacy incidents' (in EU-USA parlance), in Australia such incidents 'shall be subject to effective and dissuasive sanctions', whereas in the US the 'DHS may take disciplinary action against persons responsible for any privacy incident'. The US is also under no obligation to report any breaches of data security to any other authority, while in Australia such breaches must be reported to the Australian Information Commissioner and the European Commission. The agreement as it stands makes no provision for any form of external oversight for routine operations, let alone cases of potential illegality. The requirements mandated by Article 17 of the EU-Australia agreement are incorporated into Article 5(6) of the EU-US agreement. The fact that the EU-US provisions are shoehorned into a single article is indicative of the lower level of oversight they provide with regard to logging and documenting the processing of and access to PNR data. For the US authorities, for example, the requirement to keep logs and documentation is not accompanied by a requirement to verify the lawfulness of the processing applied to it. This is because the processing the EU-US agreement allows the US authorities to undertake flies in the face of EU data protection law.		
Article 10	**Oversight and accountability**	**Article 14**	**Oversight**
	1. Compliance with data protection rules by the government authorities processing PNR data shall be subject to the oversight by the Australian Information Commissioner who, under the provisions of the Privacy Act, has effective powers to investigate compliance by agencies with the Privacy Act, and monitor and investigate the extent to which the Australian Customs and Border Protection Service complies with the Privacy Act. 2. The Australian Customs and Border Protection Service has arrangements in place under the Privacy Act for the Australian Information Commissioner to undertake regular formal audits of all aspects of Australian Customs and Border Protection Service's EU-sourced PNR data use, handling and access policies and procedures. 3. The Australian Information Commissioner will, in particular, hear claims lodged by an individual regardless of their		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 act ion, 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, regard less of nationality, country of origin, or place of residence. 2. In addition, application of this Agreement by the United

	nationality or country of residence, concerning the protection of his or her rights and freedoms with regard to the processing of personal data. The individual concerned will be informed of the outcome of the claim. The Australian Information Commissioner will further assist individuals concerned with exercising their rights under this Agreement, in particular rights of access, rectification and redress. 4. Individuals also have the right to lodge a complaint with the Commonwealth Ombudsman regarding their treatment by the Australian Customs and Border Protection Service.		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.
Comments	These two articles make clear the differences between the data protection frameworks Australia and the US. While in Australia a system exists much like that of the UK, with an Information Commissioner holding powers laid down by statutory law, in the US such oversight is to be exercised by the DHS Chief Privacy Officer. It appears from Article 14 of the US agreement that the holder of this post has no statutory legal powers. A recent analyses of the EU-US Draft Agreement stated baldy that 'the DHS Chief Privacy officer has no independence or record of autonomy, and has recently been called before a Congress oversight committee to explain her role in a FOIA scandal'.[40]		
Article 11	**Transparency**	**Article 10**	**Transparency**
	1. Australia shall request air carriers to provide passengers with clear and meaningful information in relation to the collection, processing and purpose of the use of PNR data. Preferably this information will be provided at the time of booking. 2. Australia shall make available to the public, in particular on relevant government websites, information on the purpose of collection and use of PNR by the Australian Customs and Border Protection Service. This shall include information on how to request access, correction and redress.		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. 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

[40] 'European Commission wants to immunize DHS collaborators in travel surveillance and control'

			of, and on how to request access, correction and redress.
Comments	This seems to be one instance of the EU-US agreement containing more stringent provisions than the EU-Australia agreement, although it is not a topic of enormous importance when compared to the infringements of individual rights represented by numerous other articles.		
Article 12	**Right of access**	**Article 11**	**Access for individuals**
	1. Any individual shall have the right to access his or her PNR data, following a request made to the Australian Customs and Border Protection Service. It shall be provided without undue constraint or delay. This right is conferred by the Freedom of Information Act 1982 (Cth) (Freedom of Information Act) and the Privacy Act. The right of access shall further extend to the ability to request and to obtain documents held by the Australian Customs and Border Protection Service as to whether or not data relating to him or her have been transferred or made available and information on the recipients or categories of recipients to whom the data have been disclosed. 2. Disclosure of information pursuant to paragraph 1 may be subject to reasonable legal limitations applicable under Australian law to safeguard the prevention, detection, investigation, or prosecution of criminal offences, and to protect public or national security, with due regard for the legitimate interest of the individual concerned. 3. Any refusal or restriction of access shall be set out in writing to the individual within thirty (30) days or any statutory extension of time. At the same time, the factual or legal reasons on which the decision is based shall also be communicated to him or her. The latter communication may be omitted where a reason under paragraph 2 exists. In all of these cases, individuals shall be informed of their right to lodge a complaint against the decision of the Australian Customs and Border Protection Service. This complaint will be lodged with the Australian Information Commissioner. They		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 [*sic*] such PNR subject to the provisions of paragraph 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.

	shall be further informed of the means available under Australian law for seeking administrative and judicial redress. 4. Where an individual submits a complaint to the Australian Information Commissioner as referred to in paragraph 3, individual shall be formally advised of the outcome of the investigation of the complaint. He or she shall at least receive a confirmation whether his or her data protection rights have been respected in compliance with this Agreement. 5. The Australian Customs and Border Protection Service shall not disclose PNR data to the public, except to the individuals whose PNR data have been processed or their representatives.		
Comments	Note the additional provision in Article 1 of the EU-Australia agreement – 'The right of access shall further extend to the ability to request and to obtain documents held by the Australian Customs and Border Protection Service as to whether or not data relating to him or her have been transferred or made available and information on the recipients or categories of recipients to whom the data have been disclosed'. Although this is limited by the standard freedom of information gambit regarding 'reasonable legal limitations', it at least provides the individual with more thorough access to information about themselves than is possible under the EU-USA agreement. Indeed, it has been noted that 'while it is technically true that anyone is entitled to request anything under FOIA, agencies are not required to comply with all such requests. DHS has claimed in response to such requests that much PNR data is exempt from disclosure under FOIA. Every response we have seen to a request for PNR data has invoked FOIA exemptions to withhold some portion of the requested information'.[41] It seems that regardless of what the Draft Agreement says, the options for access to information for individuals whose data is held by the DHS are strictly limited, if not worthless. Earlier drafts contained a fifth sub-article – "This Article shall apply to PNR irrespective of when it was collected". This has been removed from the final text of the agreement.		
Article 13	**Right of rectification and erasure**	**Article 12**	**Correction or rectification for individuals**
	1. Any individual shall have the right to seek the rectification of his or her PNR data processed by the Australian Customs and Border Protection Service where the data is inaccurate. Rectification may require erasure.		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

[41] Ibid.

	2. Requests for the rectification of PNR data held by the Australian Customs and Border Protection Service may be made directly to the Australian Customs and Border Protection Service pursuant to the Freedom of Information Act or the Privacy Act. 3. The Australian Customs and Border Protection Service shall make all necessary verifications pursuant to the request and without undue delay inform the individual whether his or her PNR data have been rectified or erased. Such notification shall be set out to the individual in writing within thirty (30) days or any statutory extension of time and provide information on a possibility of a complaint against the decision of the Australian Customs and Border Protection Service to the Australian Information Commissioner and otherwise on the means available under Australian law for seeking administrative and judicial redress. 4. Where an individual lodges a complaint to the Australian Information Commissioner as referred to in paragraph 3, the individual shall be formally advised of the outcome of the investigation.		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.
Comments	The EU-Australia agreement places the Australian Customs and Border Protection Service under obligation to rectify incorrect information about an individual. In the case of data held by the US authorities, individuals 'may seek… correction or rectification' of their information, with only the 'possibility of erasure or blocking'. In the Australian case, where the data is inaccurate, '[r]ectification may require erasure', a significantly more strongly-worded provision. The EU-US agreement also fails to specify the authority to which individuals can apply for correction of their data. Although it may be inferred that this is the DHS, the lack of clarity may lead to individuals having to seek a court order to obtain correction. As with Article 11, a sub-article stating that "This Article shall apply to PNR irrespective of when it was collected" has been removed from the final text.		
Article 14	**Right of redress**	**Article 13**	**Redress for individuals**
	1. Any individual shall have the right to effective administrative and judicial redress in case any of his or her		1. Any individual regardless of nationality, country of origin, or place of residence whose personal data and personal

	rights referred to in this Agreement have been violated. 2. Any individual who has suffered damage as a result of an unlawful processing operation or of any act incompatible with rights referred to in this Agreement shall have the right to apply for effective remedies, which may include compensation from Australia. 3. The rights referred to in paragraphs 1 and 2 shall be afforded to individuals regardless of their nationality or country of origin, place of residence or physical presence in Australia.		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 TRlP) to resolve travel-related inquiries including 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.
Comments	Once again the provisions of the EU-US agreement set a considerably lower bar than those of the EU-Australia agreement. It is possible to seek administrative and judicial redress under the Australian agreement 'in case any of [the individual's] rights referred to in this Agreement have been violated', while under the US agreement this is only possible if an individual's personal data and information 'has been processed and used in a manner inconsistent with this Agreement'. Considering that the agreement has a wide-variety of 'get-out clauses' for US authorities to do as they wish with personal data, there is a wide variety of behaviour which would be considered illegal elsewhere, but is not inconsistent with the Agreement. While reference is made to provision of US law in 13(3), the EU negotiating party have manifestly failed to draft an agreement which upholds those rights accorded to individuals under the European Convention of Human Rights and the Charter of		

	Fundamental Rights of the European Union, let alone the provisions outlined in the Global Approach. Again, a sub-article stating that "This Article shall apply to PNR irrespective of when it was collected" has been removed from the text.		
Article 15	**Automated processing of PNR data**	**Article 7**	**Automated individual decisions**
	1. The Australian Customs and Border Protection Service or other government authorities listed in Annex 2 shall not take any decision which significantly affects or produces an adverse legal effect on a passenger solely on the basis of the automated processing of PNR data. 2. The Australian Customs and Border Protection Service shall not carry out the automated processing of data on the basis of sensitive data.		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.
Comments	The failure of the EU-US agreement to make specific provisions regarding the use of sensitive data indicates that the DHS and other US agencies will likely be undertaking the automated processing of data on the basis of sensitive data; in other words, profiling. The claim that adverse actions affecting individuals' legal interests will not be taken solely on the basis of automated processing of PNR simply requires one person to sign or stamp a piece of paper to insert human agency into the process. That individual does not necessarily have to apply critical attention to the documents with which they are presented following automated processing.		
Article 16	**Retention of data**	**Article 8**	**Retention of data**
	1. PNR data shall be retained not longer than five and a half years from the date of the initial receipt of PNR data by the Australian Customs and Border Protection Service. During this period PNR data shall be retained in the PNR system only for the purpose of preventing, detecting, investigating and prosecuting terrorist offences or serious transnational crime, and in the following manner: (a) From the initial receipt to three years, all PNR data shall be accessible to a limited number of the Australian Customs and Border Protection Service's officials specifically authorised by the Chief Executive Officer of the Australian Customs and Border Protection Service to identify passengers who may be		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 elements shall be masked out: (a) name(s); (b) other names on PNR; (c) all available contact information (including originator information);

	potential persons of interest; (b) From three years after initial receipt to the end of the five and a half year period, PNR data shall be retained in the PNR system but all data elements which could serve to identify the passenger to whom PNR data relate shall be masked out. Such depersonalized PNR data shall be accessible only to a limited number of Australian Customs and Border Protection Service officials specifically authorised by the Chief Executive Officer of the Australian Customs and Border Protection Service to carry out analyses related to terrorist offences or serious transnational crime. Full access to PNR data shall be permitted only by a member of the Senior Executive Service of the Australian Customs and Border Protection Service if it is necessary to carry out investigations for the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious transnational crimes. 2. To achieve depersonalization, the following PNR elements shall be masked out: (a) name(s); (b) other names on PNR, including number of travellers 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) information, to the extent that it contains any information capable of identifying a natural person; and (e) any collected advance passenger processing (APP) or advance passenger information (API) data to the extent that it contains any information capable of identifying a natural person. 3. Notwithstanding paragraph 1, PNR data required for a specific investigation, prosecution or enforcement of penalties		(d) General Remarks, including other supplementary information (OSI), special service information (SSI), and special service request (SSR); and (e) any collected APIS information. 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 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 elements 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.

	for terrorist offences or serious transnational crime may be processed for the purpose of that investigation, prosecution or enforcement of penalties. PNR data may be retained until the relevant investigation or prosecution is concluded or the penalty enforced. 4. Upon the expiry of the data retention period specified in paragraphs 1 and 3, PNR data shall be permanently deleted.		
Comments	As noted by MEP Jan Philip Albrecht, 'a blanket retention of personal data for five or even more years is a huge infringement of data protection principles'.[42] In this regard both agreements violate those principles, although the US authorities are awarded a significantly greater retention period than their counterparts in Australia. Both the A29WP and the EDPS recommend the deletion of PNR data as soon as it has been processed and nothing requiring investigation has been found. The US agreement essentially permits the retention of data for an indeterminate period, if doing so is deemed necessary. Furthermore, an article from an earlier draft of the EU-US Agreement has been removed from the final version. This article demanded that: "Upon entry into force of this Agreement, PNR held by DHS will be masked in accordance with paragraph 2 within one year of that date". It also worth noting again the more specific provisions made with regard to access by Australian officials, who have to be authorised by the Chief Executive Officer of the Australian Customs and Border Protection Service. As regards the US, the plan is to allow access for 'a limited number of specifically authorised individuals'. There is no mention of whom they are to be authorised, and the term 'limited' does not necessarily have a great deal of significance when it comes to agencies dealing with US security – as became apparent following a mass release of US cables by the organisation WikiLeaks, over three million individuals had access to information marked as 'secret'.[43]		
Article 18	**Sharing PNR data with other government authorities of Australia**	**Article 16**	**Domestic sharing**
	1. The Australian Customs and Border Protection Service may share PNR data only with those government authorities of Australia which are listed in Annex 2 and only pursuant to the following safeguards: (a) Receiving government authorities shall afford to PNR data the safeguards as set out in this Agreement. (b) Data shall be shared strictly for the purposes stated		1. DHS may share PNR only pursuant to a careful assessment of the following safeguards: (a) Exclusively as consistent with Article 4; (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;

[42] Alan Travis, 'US to store passenger data for 15 years', *The Guardian*, 25 May 2011,
[43] Editorial, 'WikiLeaks: Open Secrets', *The Guardian*, 28 November 2010,

	in Article 3; (c) Data shall be shared only on a case-by-case basis unless the data has been depersonalized; (d) Prior to the sharing, the Australian Customs and Border Protection Service shall carefully assess the relevance of data to be shared. Only those particular PNR data elements which are clearly demonstrated as necessary in particular circumstances shall be shared. In any case, the minimum amount of data possible shall be shared. (e) Receiving government authorities shall ensure that the data is not further disclosed without the permission of the Australian Customs and Border Protection Service, which permission shall not be granted by the Australian Customs and Border Protection Service except for the purposes stated in Article 3 of the Agreement. 2. The list of authorities set forth in Annex 2 may be amended by exchange of diplomatic notes between the Parties, to include: (a) any successor departments or agencies of those which are listed in Annex 2; and (b) any new departments and agencies established after the entry into force of this Agreement whose functions are directly related to preventing, detecting, investigating or prosecuting terrorism or serious transnational crime; and (c) any existing departments and agencies whose functions become directly related to preventing, detecting, investigating or prosecuting terrorism or serious transnational crime. 3. When transferring analytical information containing PNR data obtained under this Agreement, the safeguards applying to PNR data in this Article shall be respected. 4. Nothing in this article prevents the disclosure of PNR data where necessary for the purposes of Article 3 (4) and (5) and		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 10.		
Comments	Both Article 3 of the EU-Australia agreement and Article 4 of the EU-US agreement contain exemptions as regards the sharing of PNR data with other government authorities, but Article 4 of the EU-US agreement permits a far greater number of ways through which various authorities will be able to receive PNR data. Articles 18 and 16 also have clear discrepancies, with the EU-Australian agreement again providing far more stringent requirements with regard to the sharing of data. The Commission's Global Approach calls for the transfer of PNR data only 'to other government authorities with powers in the fight against terrorism and serious transnational crime, and which afford the same protections as those afforded by the recipient agency under the agreement in accordance with an undertaking to the latter',[44] The A29WP demanded that the Commission go further and called 'for a limited list of clearly defined authorities permitted to receive PNR data to be included as an annex to each future agreement'.[45] For Australia, those authorities are listed. There is no such list for the US.		
Article 19	**Transfers to authorities of third countries**	**Article 17**	**Onward transfer**
	1. The Australian Customs and Border Protection Service may transfer PNR data only to specific third country authorities pursuant to the following safeguards: (a) The Australian Customs and Border Protection Service is satisfied that the receiving third country authority has agreed to afford to the data transferred the same safeguards as set out in this Agreement; (b) Only a third country authority whose functions are directly related to preventing, detecting, investigating and prosecuting terrorist offences or serious transnational crime may receive PNR data; (c) Data shall be transferred for the exclusive purpose of preventing, detecting, investigating and prosecuting terrorist offences or serious transnational crime as defined in Article 3; (d) Data shall be transferred only on a case-by-case		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

[44] COM(2010) 492 final, p.9
[45] 'Opinion 7/2010 on European Commission's Communication on the global approach to transfers of Passenger Name Record (PNR) data to third countries', p.7

	basis; (e) Prior to the transfer, the Australian Customs and Border Protection Service shall carefully assess the relevance of data to be transferred. Only those particular PNR data elements which are clearly demonstrated as necessary in particular circumstances shall be transferred. In any case, the minimum amount of data possible shall be transferred; (f) Where the Australian Customs and Border Protection Service is aware that data of a citizen or a resident of a Member State is transferred, the competent authorities of the concerned Member State shall be informed of the matter at the earliest appropriate opportunity; (g) the Australian Customs and Border Protection Service is satisfied that the receiving third country authority has agreed to retain PNR data only until the relevant investigation or prosecution is concluded or the penalty enforced or are no longer required for the purposes set out in Article 3(4), and in any case no longer than necessary; (h) the Australian Customs and Border Protection Service is satisfied that the receiving third country authority has agreed not to further transfer PNR data; (i) The Australian Customs and Border Protection Service shall ensure, where appropriate, that the passenger is informed of a transfer of his or her PNR data. 2. When transferring analytical information containing PNR data obtained under this Agreement, the safeguards applying to PNR data in this Article shall be respected. 3. Nothing in this article prevents the disclosure of PNR data where necessary for the purposes of Article 3 (4).		1-4 of this Article shall be respected.
Comments	The differing lengths of these two articles provide a visual note as to the greater level of protection provided for data transferred from Australia to a third country. Those states receiving data from the US authorities must, on the basis of 'express understandings… incorporate		

	data privacy protections comparable to those applied to PNR by DHS as set out in this agreement'; this translates to data privacy protections that are either flimsy or so widely interpretable as to be irrelevant (it could also be argued that an 'express understanding' is nothing more than a verbal agreement). The language of Article 17 of the EU-US agreement makes this clear not just by statements such as that just quoted, but also in the fact that it is not just the DHS who will be transferring data to third countries. The supposed necessity of the DHS sharing such information with other US authorities means that it is 'the United States' who may 'transfer PNR to competent government authorities of third countries', rather than any specific authorities.

Chapter IV
Implementing and Final Provisions

Article 20	**The method of transfer**	**Article 15**	**Method of PNR transmission**
	For the purpose of this Agreement, the Parties shall ensure that air carriers transfer to the Australian Customs and Border Protection Service PNR data exclusively on the basis of the push method and in accordance with the following procedures: (a) Air carriers shall transfer PNR data by electronic means in compliance with technical requirements of the Australian Customs and Border Protection Service or, in case of technical failure, by any other appropriate means ensuring an appropriate level of data security. (b) Air carriers shall transfer PNR data using an agreed messaging format. (c) Air carriers shall transfer PNR data in a secure manner using common protocols required by the Australian Customs and Border Protection Service.		1. For the purposes of this Agreement, carriers shall transfer PNR to DHS using the "push" method, in furtherance of the need for accuracy, timeliness and completeness of PNR. 2. Carriers shall transfer PNR to DHS by secure electronic means in compliance with the technical requirements of DHS. 3. Carriers shall transfer PNR to DHS in accordance with paragraphs I 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 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 [sic] 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
Article 21	**The frequency of transfer**		
	1. The Parties shall ensure air carriers transfer to the Australian Customs and Border Protection Service all requested		

	PNR data of passengers as described in Article 20 at a maximum of five scheduled points in time per flight, with the first point being up to 72 hours before scheduled departure. The Australian Customs and Border Protection Service shall communicate to air carriers the specified times for the transfers. 2. In specific cases where there is an indication that early access is necessary to respond to a specific threat related to terrorist offences or serious transnational crime, the Australian Customs and Border Protection Service may require an air carrier to provide PNR data prior to the first scheduled transfer. In exercising this discretion, the Australian Customs and Border Protection Service shall act judiciously and proportionately and use exclusively the push method. 3. In specific cases where there is an indication that access is necessary to respond to a specific threat related to terrorist offences or serious transnational crime, the Australian Customs and Border Protection Service may require an air carrier to transfer PNR data in between or after regular transfers referred to in paragraph 1. In exercising this discretion, the Australian Customs and Border Protection Service shall act judiciously and proportionately and use exclusively the push method.		otherwise provide access.
Comments	The 'push' method referred to in these articles means that 'air carriers transfer ('push') the required PNR data to the authority requesting them, thus allowing air carriers to retain control of what data is provided. The 'push' method is considered to offer a higher degree of data protection and should be mandatory for all air carriers'. The other option available is the 'pull' method, 'under which the competent authorities of the Member State requiring the data can reach into (access) the air carrier's reservation system and extract ('pull') a copy of the required data'.[46] Clearly the push method provides a higher degree of protection for individuals' personal data held by airline carriers. While both Australian and US authorities are provided with the ability to demand data from airlines in exceptional situations (Articles 21(2) and 15(5) respectively), the Australian agreement makes clear that only the push method can be used in such circumstances. However, Article 15(5) of the US agreement states that the DHS will be able to 'require carriers to otherwise provide such access [to PNR]' where the regular transfers of PNR do not meet DHS requirements. The DHS are in fact already able to do this, as long as the PNR data is hosted on a		

[46] COM(2011) 32 final, p.16

	Computer Reservation System (CRS) either in the US, or on the CRS of a company with an office in the US: 'the DHS or other U.S. government agencies can obtain both active and archived PNR data from any of these CRSs with a "National Security Letter" or under the recently-renewed "business records" provisions of the USA-PATRIOT Act'.[47] The Draft Agreement does nothing to remedy this, and by failing to mention and specifically make provisions preventing such occurrences it effectively permits their continuation.		
Article 22	**Non-derogation/Relationship to other instruments**	**Article 21**	**Implementation and non-derogation**
	1. This Agreement shall not create or confer 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 limit rights or safeguards contained in the laws of Australia. 3. Nothing in this Agreement shall derogate from existing obligations under any bilateral mutual legal assistance instruments between Australia and Member States of the European Union to assist with a request to obtain data for evidence in criminal proceedings concerning terrorism or serious transnational crime.		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.
Comments	The lack of an article in the EU-US agreement noting that it does not limit 'rights or safeguards' provided under US law is rather worrying.		
Article 23	**Dispute resolution and suspension of the agreement**	**Article 24**	**Resolution of disputes and suspension of agreement**
	1. Any dispute arising from the interpretation, application or implementation of this Agreement and any matters related thereto shall give rise to consultation between the Parties with a view to reaching a mutually agreeable resolution, including providing an opportunity for either Party to comply within a reasonable time. 2. In the event that consultations do not result in a resolution		I. 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

[47] 'European Commission wants to immunize DHS collaborators in travel surveillance and control'

	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 120 days from the date of such notification, unless otherwise agreed. 3. Any suspension shall cease as soon as the dispute is resolved to the satisfaction of Australia and the EU. 4. Notwithstanding any suspension of this Agreement, all data obtained by the Australian Customs and Border Protection Service under the terms of this Agreement shall continue to be processed in accordance with the safeguards of this Agreement, including the provisions on retention and deletion of data.		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.
Comments	As with other provisions, the EU-US agreement provides less stringent requirements for the US authorities, in this instance essentially preventing any future dispute regarding the nature of the agreement. Whereas the EU-Australia agreement permits consultation following '[a]ny dispute arising from the interpretation, application or implementation of this Agreement', consultations under the EU-US agreement can only occur following disputes arising from the implementation of the agreement.		
Article 24	**Consultation and review**	**Article 23**	**Review and evaluation**
	1. The Parties shall notify each other, where appropriate before adoption, of any legislative or regulatory changes which may materially affect the implementation of this Agreement. References in this Agreement to Australian legislation shall be deemed to include any successor legislation. 2. The Parties shall jointly review the implementation of this Agreement and any matters related thereto one year after the entry into force of this Agreement and regularly thereafter within the duration of this Agreement and additionally as requested by either Party. The Parties agree that the review should in particular look into the mechanism of masking out data according to Article 16(1)(b), any difficulties related to the operational efficiency or cost effectiveness of the mechanism, and experience acquired with similar mechanisms in other mature PNR schemes, including the EU scheme. In the		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 confidentiality of the discussions. For the purpose of the joint review, DHS shall ensure

	event that an operationally efficient and cost effective mechanism is not available, access to the data will instead be restricted by archiving, and may be accessed only in the way that depersonalized data is accessed under Article 16. 3. The Parties shall agree in advance of the joint review its modalities 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 Australia shall be represented by the Australian Customs and Border Protection Service. The teams may include experts on data protection and law enforcement. Subject to applicable laws, any participants to the joint review shall be required to respect confidentiality of the discussions and have appropriate security clearances. For the purpose of the joint review, the Australian Customs and Border Protection Service shall ensure access to relevant documentation, systems and personnel. 4. The Parties shall evaluate the Agreement, in particular its operational effectiveness no later than four years after its entry into force. 5. Following the joint review, the European Commission shall present a report to the European Parliament and to the Council of the European Union. Australia shall be given an opportunity to provide written comments which shall be attached to the report. 6. Since the establishment of an EU PNR system could change the context of this Agreement, if and when an EU PNR system is adopted, the Parties shall consult to determine whether this Agreement would need to be adjusted accordingly.		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 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 this 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.
Comments	While the EU and Australian authorities are under obligation to inform each other regarding any 'legislative or regulatory changes which may materially affect the implementation of this Agreement', there is no such requirement for authorities to do the same regarding the EU-US agreement. When the time comes to review the agreements, the EU and US authorities are also under no obligation to discuss those issues highlighted for intention in the EU-Australia agreement, in particular 'the mechanism of masking out data according to Article 16(1)(b)'.		
Article 25	**Termination**	**Article**	**Termination**

		25	
	1. Either Party may terminate this Agreement at any time by written notification through diplomatic channels. Termination shall take effect 120 days from the date of receipt of such notification, or as otherwise agreed. 2. Notwithstanding any termination of this Agreement, all data obtained by the Australian Customs and Border Protection Service under the terms of this Agreement shall continue to be processed in accordance with the safeguards of this Agreement, including the provisions on retention and deletion of data.		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. 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.
Comments	Article 25(3) of the EU-US agreement makes termination of the agreement far more difficult than any of the provisions in Article 25 of the EU-Australia agreement.		
Article 26	**Duration**	**Article 26**	**Duration**
	1. Subject to Article 25, this Agreement shall remain in force for a period of seven years from the date of entry into force. 2. Upon the expiry of the period set forth in paragraph 1, 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 data obtained by the Australian Customs and Border Protection Service under the terms of this Agreement shall continue to be processed in accordance with the safeguards of this Agreement, including the provisions on retention and deletion of data.		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 un less 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	**PNR data received prior to the entry into force of this agreement**		
	Australia shall treat any PNR data held by the Australian Customs and Border Protection Service at the time of the entry into force of this Agreement in accordance with the provisions of this Agreement. However, no data shall be required to be masked out before 1 January 2015.		
Article 28	**Territorial application**		
	1. Subject to paragraphs 2 to 4, this Agreement shall apply to the territory in which the Treaty on European Union and the Treaty on the Functioning of the European Union are applicable and to the territory of Australia. 2. This Agreement will only apply to Denmark, the United Kingdom or Ireland, if the European Commission notifies Australia in writing that Denmark, the United Kingdom, or Ireland has chosen to be bound by this Agreement. 3. If the European Commission notifies Australia before the entry into force of this Agreement that it will apply to 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. 4. If the European Commission notifies Australia after the entry		

	into force of this Agreement that it applies to 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 Australia.		
Article 29	**Final provisions**	**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 replaces the Agreement between the European Union and Australia on the Processing and Transfer of European Union – Sourced Passenger Name Record (PNR) Data by Air Carriers to the Australian Customs Service done at Brussels on 30 June 2008, which will cease to apply upon the entry into force of this Agreement.		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 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.