



Homeland Security

Privacy Office

June 15, 2007

Ms. Marcia Hofmann
Electronic Frontier Foundation
1875 Connecticut Avenue, N.W.
Suite 650
Washington, DC 20009

Re: DHS/OS/PRIV 07-90/Hofmann request

Dear Ms. Hofmann:

Pursuant to the order of the court, this is our second partial release to your Freedom of Information Act (FOIA) request to the Department of Homeland Security (DHS), dated October 20, 2006, for DHS records concerning Passenger Name Records (PNR) from May 30, 2006 to the present including:

1. Emails, letters, reports or other correspondence from DHS officials to European Union officials concerning the transfer and use of passenger data from air carriers to the US for prescreening purposes;
2. Emails, letters, statements, memoranda or other correspondence from DHS officials to U.S. government officials or employees interpreting or providing guidance on how to interpret the undertakings;
3. Records describing how passenger data transferred to the U.S. under the temporary agreement is to be retained, secured, used disclosed to other entities, or combined with information from other sources; and
4. Complaints received from EU citizens or official entities concerning DHS acquisition, maintenance and use of passenger data from EU citizens.

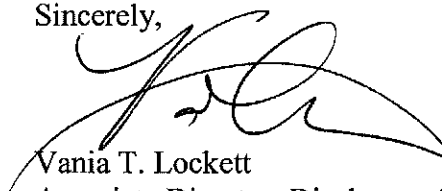
In our December 15, 2006 letter, we advised you that we had determined multiple DHS components or offices may contain records responsive to your request. The DHS Office of the Executive Secretariat (ES), the DHS Office of Policy (PLCY), the DHS Office of Privacy (PRIV), the DHS Office of Operations Coordination (OPS), the DHS Office of Intelligence and Analysis (OI&A), the DHS Office of the General Counsel (OGC), the Transportation Security Administration (TSA), and the U.S. Customs and Border Protection (CBP) were queried for records responsive to your request.

So far, a search directed to PLCY has produced 2 pages of records, to TSA 7 pages, and to PRIV 8 pages of records responsive to your request. Of those 17 pages, we have enclosed 16 pages in their

entirety and 1 page with certain information withheld pursuant to Exemptions 2 and 6 of the FOIA, 5 USC §§ 552 (b)(2) and (b)(6). FOIA Exemption 2(low) exempts from disclosure records that are related to internal matters of a relative trivial nature, such as internal administrative tracking. Exemption 6 exempts from disclosure records the release of which would cause a clearly unwarranted invasion of personal privacy. Weighed against the privacy interest of the individuals is the lack of public interest in the release of their personal information and the fact that the release adds no information about agency activities, which is the core purpose of the FOIA. Therefore, after a careful balancing of the factors supporting and opposing disclosure, redactions were made on the basis of Exemptions 2 and 6 of the FOIA.

Our office continues to process your request. If you have any questions regarding this matter, please refer to **DHS/OS/PRIV 07-90/Hofmann request**. The DHS Privacy Office can be reached at 703-235-0790 or 1-866-431-0486. Thank you for your patience as we proceed with your request.

Sincerely,



Vania T. Lockett
Associate Director, Disclosure & FOIA Operations

Enclosures: 17 pages

PNR agreement

U.S. Department of Homeland Security
Washington, DC 20528



Homeland
Security

Facsimile Transmission

To: Gilles de KERCHOVE

Fax Number: 011-00-32-2-281-12

From: Stewart Baker

Fax Number: 202-282-9598

Date: 10/6/06

Number of pages including cover: _____

If you did not receive all the pages indicated in this fax, please contact us at 202-282-_____

Dear Gilles,

Please find attached the draft interim agreement and letter of interpretation now initialed by myself, Jonathan Fuall and Irma Ertman.

In reviewing we noticed about a half dozen minor typos between the two documents (mostly left over brackets, underlinings and strikethroughs) that we should correct before final signing.

Thanks you again for your partnership in this endeavor.

Sincerely,

A handwritten signature in black ink that reads "Stewart".

Stewart Baker

U.S. Department of Homeland Security
Border & Transportation Security
3801 Nebraska Avenue
Washington, DC 20528

AGREEMENT

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

THE EUROPEAN UNION AND THE UNITED STATES OF AMERICA,

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

RECOGNISING that, in order to safeguard public security and for law enforcement purposes, rules should be laid down on the transfer of PNR data by air carriers to the [Department of Homeland Security (hereinafter 'DHS'). For the purposes of this Agreement, DHS means the Bureau of Customs and Border Protection, U.S. Immigration and Customs Enforcement and the Office of the Secretary and the entities that directly support it, but does not include other components of DHS such as the Citizenship and Immigration Services, Transportation Security Administration, United States Secret Service, the United States Coast Guard, and the Federal Emergency Management Agency.

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

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

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

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

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

¹ Vol. 69, No 131, p.41543

Handwritten signature/initials

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

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

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

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

HAVE AGREED AS FOLLOWS:

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

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

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

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

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

18
UCC SAS

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

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

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

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

FOR THE UNITED STATES OF AMERICA

Secretary Michael Chertoff
Department of Homeland Security

Date:

FOR THE EUROPEAN UNION

Date:

[Handwritten signature]
Muller 300

U.S. Department of Homeland Security
Washington, DC 20528



Homeland Security

Via Electronic Delivery

European Commission
ATTN: Director General Jonathan Faull
ADDRESS
Brussels, Belgium]

Presidency of the Council of the EU
ATTN: Ms. Irma Ertman
ADDRESS
Helsinki, Finland]

[Dear Jonathan and Markus:]

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

Sharing and Disclosure of PNR

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

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

In light of these developments and in accordance with what follows, the Undertakings should be interpreted and applied so as to not impede the sharing of PNR data by DHS with other authorities of

Handwritten initials and numbers: ft Ull 300

the U.S. government responsible for preventing or combating of terrorism and related crimes as set forth in Paragraph 3 of the Undertakings.

DHS will therefore facilitate the disclosure (without providing unconditional direct electronic access) of PNR data to U.S. government authorities exercising a counter-terrorism function that need PNR for the purpose of preventing or combating terrorism and related crimes in cases (including threats, flights, individuals, and routes of concern) that they are examining or investigating. DHS will ensure that such authorities respect comparable standards of data protection to that applicable to DHS, in particular in relation to purpose limitation, data retention, further disclosure, awareness and training, security standards and sanctions for abuse, and procedures for information, complaints and rectification. Prior to commencing facilitated disclosure, each receiving authority will confirm in writing to DHS that it respects those standards. DHS will inform the EU in writing of the implementation of such facilitated disclosure and respect for the applicable standards before the expiration of the Agreement.

Early Access Period for PNR

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

In determining when the initial push of data is to occur, DHS has discretion to obtain PNR more than 72 hours prior to the departure of a flight so long as action is essential to combat an offense enumerated in Paragraph 3. Additionally, while there are instances in which the U.S. government may have specific information regarding a particular threat, in most instances the available intelligence is less definitive and may require the casting of a broader net to try and uncover both the nature of the threat and the persons involved. Paragraph 14 is therefore understood to permit access to PNR outside of the 72 hour mark when there is an indication that early access is likely to assist in responding to a specific threat to a flight, set of flights, route, or other circumstances associated with offenses described in Paragraph 3 of the Undertakings. In exercising this discretion, DHS will act judiciously and with proportionality.

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

f *cke* *SS*

Data Retention

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

The Joint Review

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

Data Elements

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



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

Vital Interests of the Data Subject or Others

Recognizing the potential importance of PNR data in the context of infectious disease and other risks to passengers, DHS reconfirms that access to such information is authorized by paragraph 34, which provides that the Undertakings must not impede the use of PNR for the protection of the vital interests of the data subject or of other persons or inhibit the direct availability of PNR to relevant authorities for the purposes set forth in Paragraph 3 of the Undertakings. "Vital Interests" encompasses circumstances in which the lives of the data subject or of others could be at stake and includes access to information necessary to ensure that those who may carry or may have been exposed to a dangerous communicable disease can be readily identified, located, and informed without delay. Such data will be protected in a manner commensurate with its nature and used strictly for the purposes for which it was accessed.

Sincerely yours,

Stewart Baker
Assistant Secretary for Policy

TALKING POINTS

BACKGROUND

This is to provide a European audience an explanation of the privacy protections provided by the PNR interim agreement.

BEGIN TALKING POINTS

- DHS is committed to applying privacy protections for European travelers that are similar to those enjoyed by U.S. citizens and lawful permanent residents.
- As Secretary Chertoff has said, "If we want to protect the privacy of our own citizens, we are going to have to be willing to protect the privacy of our international partners and their citizens."
- These protections follow the fair information practices embodied in the U.S. Privacy Act of 1974, our Freedom of Information Act (FOIA), the E-Government Act of 2002 and other related data privacy and access authorities.
- In fact, Europe and the U.S. share many of the same privacy principles. For example, the U.S. and 15 of the 25 EU member states have signed onto the 1980 OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. The OECD guidelines are modeled along the fair information practices.
- The same fair information practices are embodied in the interim PNR agreement.
- We can offer a point-by-point summary of these principles.
- **Collection Limitation/Purpose Specification.** Similar to any collection on U.S. persons, the interim agreement requires DHS to define and limit the purpose for collecting personal information. We intend to use PNR data for combating terrorism and related crimes.

➤ **Notice/Openness.**

- The European public will be given notice of PNR information collected and maintained by DHS by publishing a System of Records Notice in the U.S. Federal Register, as well as providing a copy of the interim agreement and a letter of interpretation.
- DHS is currently revising its System of Records Notice for PNR to reflect its most current procedures. This will soon appear in the Federal Register.
- For example, we have already made such a commitment for data collected through the US-VISIT program. This system contains records on over 51 million individuals who are not U.S persons.

➤ **No Public Disclosure.** PNR is protected from disclosure to third parties under our FOIA by certain exemptions which DHS would invoke in the event that a member of the public made a request. In fact, our Supreme Court has upheld FOIA's privacy protections in the case of non-U.S. persons.

➤ **Limitations on Disclosure.** Access is limited to those officers and employees of DHS that have a need to know in accordance with their duties and to those agencies that have a need to know for purposes of combating terrorism or related crimes and in response to the vital interests of the individual or others who, for instance, may have been exposed to a dangerous communicable disease.

➤ **Data Quality.** The Privacy Act requires all agencies to maintain data in an accurate, relevant, timely, and complete fashion in order to protect individual privacy.

➤ **Accountability.** The interim agreement requires DHS to keep an audit log of the date, nature, and purpose of each disclosure of a record to any person or to another agency.

- **Training and Rules of Conduct.** The agreement requires DHS to train its employees in the rules of access to the PNR system of records and provide continuous guidance with respect to such rules and may take disciplinary measures for inappropriate use of the information.
- **Safeguards.** The agreement requires DHS to maintain technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.
- **Access.** If any data subject, regardless of whether they are a U.S. person, wants to see PNR information maintained about him or her it is possible to obtain that information under FOIA. Any individual, regardless of nationality, may pursue this right in U.S. courts.
- **Redress.**
 - The agreement requires CBP to establish an administrative process to accept requests by the public to access their records and provide opportunities for redress. If an individual has a concern after working through the administrative process with CBP, they may seek further consideration from DHS's Chief Privacy Officer.
 - [Optional: Since May 2004, when the agreement has been in place, we have not received one request.]

- o [Optional: While non-U.S. persons may not seek redress under the Privacy Act in U.S. Courts, they may access U.S. Courts under the Freedom of Information Act.]

¹ Secretary Chertoff's prepared remarks presented before the DHS Privacy Advisory Committee, December 6, 2005, available online at:
http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0765.xml

Public Affairs Guidance

PNR Data Privacy Agreement between the US and European Union

LAST MODIFIED

9/30/2006 2:00 PM

GUIDANCE:

Refer all calls to DHS Public Affairs: 202-282-8010

BACKGROUND

Passenger Name Record (PNR) is the generic name given to records created by aircraft operators or their authorized agents for each journey booked on or behalf of any passenger. The data is used by operators for their own business and operational purposes. PNR data comprises a range of elements such as date of ticket reservation, date and place of ticket issue, payment details, passenger/travel agent contact details and travel itinerary. PNR data provided to DHS provides law enforcement with a valuable source of data for risk assessment, aviation security and border enforcement.

The European Court of Justice ruled that the current arrangement between the U.S. and the European Commission was struck on an inappropriate legal basis and must be terminated by September 30th, 2006. This court decision was not against DHS ability to protect private information or the content of the agreement. Rather, the court's decision relates to the EU'S internal governmental structure and the authorities of its various entities.

TALKING POINTS

- Secretary Chertoff has initialed a draft formal U.S. /EU agreement regarding the sharing of Passenger Name Record (PNR) data.
- As we await the final ratification of the draft agreement, we expect that planes will continue to fly uninterrupted and our national security will not be impeded.
- The proposal ensures the appropriate security information will be exchanged and counter-terrorism information collected by the department will be shared, as necessary with other federal counter-terrorism agencies.
- The draft agreement has now been returned to the European Union for its final review and consideration.
- The United States has a legal and moral obligation to protect its borders, as we have a right to verify who it is admitting into the country. This department will use every legal authority at our disposal, including valuable PNR data, to secure the borders of our homeland and fulfill the trust that the American people have placed in us.

- It should be made clear that DHS is not seeking additional PNR data elements. The total number of data elements remains constant at 34. This is the same data that was permitted to be shared under the previous agreement.
- PNR data is used for our shared goal of combating terrorism while respecting fundamental rights and freedoms, notably privacy. The level of privacy protection afforded American and EU citizens remains unchanged.
- Here in the United States and in Europe, we all have to be smart and thorough in scrutinizing people seeking to enter our territory – including those who may not be on watchlists but could mean to do us harm.
- This is really a question of timing. Much of the PNR information could be gathered from travelers when they arrive in the United States, or DHS could impose visa requirements soliciting this information, but this would seriously impede travel. The only way we can avoid such a scenario is to ask for the information electronically in advance of travel.
- We look forward to finalizing an agreement on this issue with our European allies, with whom we have a great relationship

QUESTION AND ANSWERS

Q. What is PNR and what is it used for?

A: Passenger Name Record (PNR) is the generic name given to records created by aircraft operators and can include a range of elements such as date of ticket reservation, date and place of ticket issue, payment details, passenger/travel agent contact details and travel itinerary. This is data that can be obtained from a passenger during an interview with US Customs and Border Protection officers upon arrival in the United States.

Per the Aviation Transportation Security Act (ATSA) DHS collects PNR information on travelers aboard flights bound for and departing from the U.S. Our current agreement with the EU reflects this U.S. statutory requirement, which strengthens aviation and border security, while also facilitating legitimate travel.

CBP uses PNR along with other information to conduct a risk assessment of each passenger in order to identify those that may pose a threat of terrorism and other serious crime. Access to this information is a foundational element of DHS's layered strategy for aviation and border security and also facilitates legitimate travel.

Q: Will air travel be interrupted between US and Europe?

A: The appropriate security information will continue to be exchanged. Planes will continue to fly uninterrupted and our national security will not be impeded.

Q: What is DHS looking for in long term agreement with EU on PNR?

A: ~~The issue for the US comes down to the need to break stovepipes among counterterrorism and law enforcement agencies.~~ Every nation has a legal and moral obligation to protect its borders, as it has a right to verify who it is admitting into the country. This department will simply not relinquish that sovereign right, and we will use every legal authority at our disposal. Limits should not be placed on the sharing of PNR data by CBP with other elements of the U.S. government; particularly within DHS

and the Department of Justice for the investigation, analysis, and prevention of terrorism and other crimes.

Q: Who does DHS receive PNR data on?

A: DHS receives PNR data for all passengers flying to the United States.

Q: How long does DHS want to store PNR data for?

A: We would like to store PNR data for as long as it has potential relevance for law enforcement and terrorism prevention purposes. Because we know terror attacks can be in the planning stages for several years, we want to store the information for longer than the current 3.5 year agreement.

Q: When does DHS begin collecting PNR data? Do you want to get it earlier?

A: We begin collecting PNR data up to 72 hours before flights for preliminary targeting. We would like to be permitted access to PNR outside of the 72 hour mark when there is an indication that early access could assist in responding to a threat to a flight or set of flights bound for the United States.

Q: Will there be further negotiations?

A: We look forward to finalizing the draft agreement with our European allies, with whom we have a great relationship.

Q: How will DHS obtain PNR? How does this method affect privacy?

A: We have agreed to work towards a "push" system, which may be viewed as less of a privacy concern than the current "pull" model by many Europeans. This would mean that air carriers are feeding us info rather than getting it from carrier records. In implementing this model we are working with carriers and system providers to ensure all technical specifications meet DHS regulatory requirements.

Q: What is the difference between Advance Passenger Information System (APIS) and Passenger Name Record (PNR) data?

A: APIS data refers to passenger information that is collected from government-issued identity documents accepted for international travel. APIS data is most commonly collected from passports and much of this information is resident in the Machine Readable Zone. APIS data comprises data elements such as Full Name, Date of Birth, Travel Document Number, Country of Issuance, etc.

PNR is the generic name given to records created by aircraft operators or their authorized agents for each journey booked on behalf of any passenger. The data is used by operators for their own business and operational purposes. PNR data comprises a range of elements such as date of ticket reservation, date and place of ticket issue, passenger/travel agent contact details and travel itinerary.

Q: What has been done to address privacy concerns over PNR data sharing?

A: CBP has invested substantial time, capital, and expertise to bring its operations and procedures into compliance with U.S. privacy law and the 2004 EU-U.S. agreement. This is a recognizable achievement that involved implementation of state-of-the-art technology solutions for use by officers of CBP nation-wide, the establishment of detailed training programs and the implementation of new policy and procedural rules that are paired with sever penalties for misuses.

The EU is aware of these investments and has voiced its approval. On September 20 and 21, 2005, delegations from DHS and the European Commission performed the first Joint Review of the PNR Undertakings concerning PNR derived from flights between the US and the EU. Prior to the Joint Review, the DHS Privacy Office conducted an internal review of CBP policies, procedures and

technical implementation related to the data covered by the Undertakings and found CBP in full compliance with representations made in the PNR agreement. Afterwards, the EU issued its own report, which came to the same conclusion. Both of these reports are publicly available on the internet. [NOTE - PRIV report is on the DHS website]

Q: Did the European Court of Justice rule that U.S. data privacy protection is inadequate?

A: The Court did not rule against the availability of PNR data, it did not determine that privacy was violated, nor did it take a view on the content of the agreement. Rather, the court found that the European Council relied upon an inapplicable legal authority for entering into the agreement.

Q: How will the PNR agreement affect the Pre-departure APIS Notice of Proposed Rulemaking?

A: APIS is merely an automated vehicle for the collection of information from government-issued identity documents accepted for international travel. The Pre-departure APIS proposed changing the timing for APIS information already being collected under the APIS Final Rule Published on April 7, 2005. Essentially, APIS is the same as a border officer swiping or visually examining a passport presented by a traveler. The Pre-departure APIS NPRM does not contain any PNR related requirements. Thus, this rulemaking is not affected by the EU's recent PNR ruling.

b6
b6
From:
Sent: Monday, August 28, 2006 7:13 PM
To:

b6
, Rosenzweig, Paul;

Subject: FW: PNR op-ed
Attachments: PNR WPost edits.doc

FYI, a preview before your morning coffee.

b6
b2
b6
b6
From:
Sent: Monday, August 28, 2006 1:31 PM
To: Rosenzweig, Paul; Baker, Stewart;
Kraninger, Kathleen
Cc:
Subject: PNR op-ed

b6
The Washington Post is scheduled to run the PNR op-ed in tomorrow's paper. Here's a copy of the edited version I got back from them. On attachment you can see the changes they made. They look to be very minor, but let me know if you seen any thing you want to change.
Thanks

By Michael Chertoff

Imagine that our troops in Afghanistan raided an al-Qaeda safe house and captured a computer containing the cell-phone numbers of operatives in Europe. Wouldn't it be important to know whether one of those same cell phone numbers was used to book a transatlantic flight? Unfortunately, today our ability to make that connection remains limited: Information that terrorists readily share with travel agents cannot easily be shared throughout the United States government. That needs to change. Information sharing and intelligence gathering are some of our most important tools in the global war on terrorism. British authorities, in partnership with the United States and our allies, were able to disrupt the recent U.K. terror plot against passenger aircraft precisely because of timely, actionable intelligence, properly shared and acted upon before the terrorists could act. But despite the strong links we've forged with our European partners to protect our nations, we still remain handcuffed in our ability to use all available resources to identify threats and stop terrorists. In order to defeat terrorists we must limit their movement between countries and disable their worldwide networks by targeting our investigative resources. One technique currently in use by the Department of Homeland Security and a number of foreign governments is the use of name-based information, such as passenger manifests and crew lists, to screen travelers coming to the United States before they get here. These manifests allow us to identify known persons of interest on watch lists and to act upon threats before they can reach our shores — even, where possible, before they depart on their trip. But how do we thwart a terrorist who has not yet been identified? One way is by using more of the detailed information collected by airlines and travel agencies when an individual books a flight. This Passenger Name Record (PNR) data contains information, such as travel

itineraries and payment details, that can be analyzed in conjunction with current intelligence to identify high-risk travelers before they board the plane.

If we learned anything from Sept. 11, it is that we need to be better at connecting the dots of terrorist-related information. After Sept. 11, we used credit card and telephone records to identify those linked with the hijackers. But wouldn't it be better to identify such connections before a hijacker boards a plane?

By comparing PNR data and intelligence gathered on known terrorists — such as cell-phone numbers collected in Afghanistan — we can identify potential unknown threats for additional screening and enhance our ability to assess risk. At the same time, that means we will spend less time with inconvenient screening of low-risk travelers.

The U.S. government has collected PNR data on travelers aboard international flights to the United States since the early 1990s. This information is of such value that after the Sept. 11 terrorist attacks, Congress mandated its continued collection. But in the past few years European privacy concerns have limited the ability of counterterrorism officials to have broad access to data of this sort.

For example, under a current agreement with the European Union, U.S. Customs and Border Protection receives this information regularly, but it cannot routinely share it with investigators in another DHS component, Immigration and Customs Enforcement, or with the FBI — never mind with our allies in London. This information might yet identify associates of those arrested in the U.K. plot, but current rules blind us in our search for that connection.

DHS has made a strong commitment to protect personal privacy while screening international travelers. We do not profile based on race or ethnicity, but we do assess potential threats through careful analysis of individual behavior. The DHS Chief Privacy Officer has closely reviewed the PNR program to ensure that it meets standards of fair information practices and U.S. law. This includes providing a process through which travelers can seek redress if they feel their freedoms have been violated.

Protecting personal privacy is a part of responding to the post-Sept. 11 world, but it should not reflexively block us from developing new screening tools. Indeed, more data sharing leads to more precisely targeted screening, which actually improves privacy by reducing questioning and searches of innocent travelers.

All governments bear a responsibility to prevent terrorists from boarding aircraft, and information sharing is a critical way we can work together to limit terrorist mobility, screen for unknown threats and investigate terrorist cells. Smart screening — including careful and responsive analysis of travel data — will enhance security and privacy.

The writer is U.S. secretary of homeland security.