



Homeland Security

Privacy Office

December 7, 2007

Ms. Marcia Hofmann
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110

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

Dear Ms. Hofmann:

This is our fifteenth 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 Privacy Office (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 U.S. Customs and Border Protection (CBP) were queried for records responsive to your request. In our July 27, 2007 letter, we advised you that we expanded our search to include U.S. Immigration and Customs Enforcement (ICE).

Continued searches of the DHS components produced an additional 44 documents, consisting of 185 pages, responsive to your request. I have determined that 3 documents, consisting of 6 pages, are releasable in their entirety; 25 documents, consisting of 104 pages, are releasable in part; and 16 documents, consisting of 75 pages, are withholdable in their entirety. The releasable information is enclosed. The withheld information, which will be noted on the *Vaughn* index

when completed, consists of names, telephone numbers, email addresses, deliberative material, legal opinions, law enforcement information, and homeland security information. I am withholding this information pursuant to Exemptions 2, 5, 6, 7(C), and 7(E) of the FOIA, 5 USC §§ 552 (b)(2), (b)(5), (b)(6), (b)(7)(C), and (b)(7)(E).

FOIA Exemption 2(low) exempts from disclosure records that are related to internal matters of a relatively trivial nature, such as internal administrative tracking. FOIA Exemption 2(high) protects information the disclosure of which would risk the circumvention of a statute or agency regulation. Included within such information may be operating rules, guidelines, manuals of procedures for examiners or adjudicators, and homeland security information.

FOIA Exemption 5 protects from disclosure those inter- or intra-agency documents that are normally privileged in the civil discovery context. The deliberative process privilege protects the integrity of the deliberative or decision-making processes within the agency by exempting from mandatory disclosure opinions, conclusions, and recommendations included within inter-agency or intra-agency memoranda or letters. The release of this internal information would discourage the expression of candid opinions and inhibit the free and frank exchange of information among agency personnel. The attorney-client privilege protects confidential communications between an attorney and his client relating to a legal matter for which the client has sought professional advice. It applies to facts divulged by a client to his attorney, and encompasses any opinions given by an attorney to his client based upon, and thus reflecting, those facts, as well as communications between attorneys that reflect client-supplied information.

FOIA 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.

FOIA Exemption 7(C) protects records or information compiled for law enforcement purposes that could reasonably be expected to constitute an unwarranted invasion of personal privacy. This exemption takes particular note of the strong interests of individuals, whether they are suspects, witnesses, or investigators, in not being unwarrantably associated with alleged criminal activity. That interest extends to persons who are not only the subjects of the investigation, but those who may have their privacy invaded by having their identities and information about them revealed in connection with an investigation. Based upon the traditional recognition of strong privacy interest in law enforcement records, categorical withholding of information that identifies third parties in law enforcement records is ordinarily appropriate. As such, I have determined that the privacy interest in the identities of individuals in the records you have requested clearly outweigh any minimal public interest in disclosure of the information. Please note that any private interest you may have in that information does not factor into this determination.

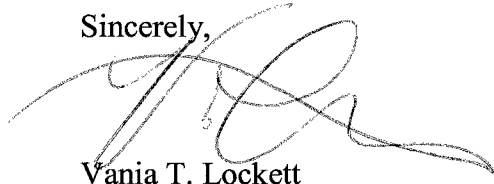
Finally, FOIA Exemption 7(E) protects records compiled for law enforcement purposes, the release of which would disclose techniques and/or procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law.

We have completed our search for responsive documents. We identified 8 documents, consisting of 51 pages, which were classified by agencies outside of DHS. We referred those 8 documents

to the original classification authorities and asked them to conduct a declassification review and return the documents to us for further processing. Other than these 8 classified documents that have been sent outside our agency for review, this completes our processing of all documents deemed responsive to your FOIA request, except for those documents that are being held for DHS classification review. Our office continues to process your request insofar as it relates to the documents being held for classification review.

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,

A handwritten signature in black ink, appearing to read 'V. Lockett', with a large, sweeping flourish extending to the right.

Vania T. Lockett
Associate Director, Disclosure & FOIA Operations

Enclosures: 110 pages

[redacted] (b6)
From: [redacted] (b6)
Sent: Tuesday, September 26, 2006 10:48 AM
To: [redacted] (b6)
Cc: [redacted] (b6); Scardaville, Michael; [redacted] (b6)
Subject: RE: PNR and the President's Civil Liberties board

Thanks [redacted] (b6) for some reason. I thought we had done a PIA for PNR specifically, but I must say I tend to get confused about those documents quite frequently [redacted] (b6) should know if we did!).

65
Mike- [redacted]

[redacted] (b6)
Office of Chief Counsel
U.S. Customs and Border Protection
Phone: [redacted] (b2)
Fax: [redacted] (b2)
Email: [redacted] (b6)

This document, and any attachment(s) hereto, may contain confidential and/or sensitive attorney-client privileged, attorney work-product, and/or U.S. Government information, and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please consult with the CBP Office of Chief Counsel before disclosing any information contained in this e-mail.

Michael* [redacted] (b6) [redacted] (b2 b6) Scardaville,
[redacted] (b6) 09/26/2006 10:30 AM [redacted] (b6) (b6 b2)
Liberties [redacted] (b6) [redacted] (b6) [redacted] (b6 b2)
Subject: RE: PNR and the President's Civil
board

Will defer to [redacted] (b6) to explain but as I understand it, the existing SORN that covers all PNR data is still the 1998 TECS SORN. (the PIA for the new system is still in draft). The only distinction in how US person PNR data is treated would be for those US persons who

(1)

are arriving on EU originating flights - their PNR (as well as all other persons) would be subject to filters put in place by CBP pursuant to the PNR Agreement and Undertakings and announced in the Fed Register. For all non-EU originating flights, all US person PNR collected by CBP is not subject to any special filtering.

[b6]
Director of International Privacy Policy DHS, Privacy Office Tel [REDACTED] b6

b6
b7
The harsh reality is that data protectors run the risk of being only a tiny force of irregulars equipped with pitchforks and hoes waging battle against large technocratic and bureaucratic forces equipped with lasers and nuclear weapons. --David Flaherty, Protection Privacy in Surveillance Societies.

This communication, along with any attachments, is covered by federal and state law governing electronic communications and may contain confidential and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of this message is strictly prohibited. If you received this in error, please reply immediately to the sender and delete the message. Thank you.

From: [REDACTED] b6 b2
Sent: Monday, September 25, 2006 5:51 PM
To: Scardaville, Michael; [REDACTED] b6]
Subject: Re: PNR and the President's Civil Liberties board

All,

Paul met with the President's civil liberties board today and discussed PNR with them. He had one take away from the call, specifically to respond to a question about how we treat U.S. citizen PNR stored in CBP databases.
Can you put together a short write up for him to send to them?

Thanks

Mike

Michael Scardaville
Special Assistant/International Policy Advisor Office of Policy Development U.S.
Department of Homeland Security
[REDACTED] b2

L b6]

From: Scardaville, Michael [b2]
Sent: Saturday, September 30, 2006 2:28 PM
To: [b6]
Cc: Rosenzweig, Paul
Subject: Fw: REVISED PNR PAG
Attachments: EU-US PNR Agreement PAG.doc



EU-US PNR Agreement PAG.doc (E

Any thoughts.

Sent from my BlackBerry Wireless Handheld

----- Original Message -----

From: Agen, Jarrod
To: Rosenzweig, Paul; Sciara, Nicolle; Baker, Stewart; Scardaville, Michael; 'Isles, Adam' [b2]] Knocke, William R; [b6]]
[b6 b2]]
Sent: Sat Sep 30 14:02:16 2006
Subject: REVISED PNR PAG

<<EU-US PNR Agreement PAG.doc>>
I believe this incorporates all the latest...please review. I'll also adjust S1 statement.

TALKING POINTS

* [Secretary Chertoff has [b5] initialed []]

* [b5]] counter-terrorism information collected by the Department will be shared, as necessary with other federal agencies.

* [b5]]

* The [b5] agreement has now been returned to the European Union for its final review and consideration.

* [b5]] the appropriate security information will [b5]] be exchanged. Planes will continue to fly uninterrupted and our national security will not be impeded.

(2)

* [b5] has a legal and moral obligation to protect its borders, as [b5] has a right to verify who it is admitting into the country. This department [b5] will use every legal authority at our disposal, including valuable PNR data, to secure [b5]

* 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. [b5]

* [b5] Here in the United States and in Europe, we all have to be smart and thorough in scrutinizing people seeking to [b5] including those who may not be on watchlists but could mean to do us harm.

* This is really [b5] question of timing. Much of the PNR information could be gathered from travelers when they arrive in the United States, or DHS could impose [b5] 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 [b5] on this issue with our European allies, with whom we have a great relationship [b5]

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. 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 store the info 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: With there be further negotiations?

A: We look forward to finalizing [b5] with our European allies, with whom we have a great relationship [b5]

Q: [b5]]

A: We have agreed to work towards a "push" system, which is [b5] This would mean that air carriers are feeding us into [b5]]

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 b5 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: b5
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.

b5 found b5 CBP b5 in full compliance with representations made in the PNR agreement. CBP has invested substantial time, capital, and expertise to bring its operations and procedures into compliance. This is a recognizable achievement,
b5

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: b5
APIS is merely an automated vehicle for the collection of information from government-issued identity documents accepted for international travel. 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.

From: [b6 b2]
To: "Mike Scardaville" [b2]
Date: Saturday, September 30, 2006 03:43PM
Subject: Re: REVISED PNR PAG

Mike--there is a typo in one of the last Q and As--"sever" instead of "severe" penalties.

[b6]
Office of Chief Counsel (Enforcement)
US Customs and Border Protection
Phone: [b2]
Fax: [b2]

----- Original Message -----

From: "Scardaville, Michael" [b2]
Sent: 09/30/2006 03:28 PM
To: [b6 b2]
Subject: FW: REVISED PNR PAG

From: Rosenzweig, Paul
Sent: Saturday, September 30, 2006 3:24 PM
To: Agen, Jarrod; Sciara, Nicolle; Baker, Stewart; Scardaville, Michael; 'Isles, Adam'; Knocke, William R; Bergman, Cynthia; 'Montgomery, Kathleen'
Subject: RE: REVISED PNR PAG

All

Mike Scardaville and [b6] added the following edits for your consideration. I think they make the product a little clearer and invite your thoughts

P

Paul Rosenzweig

[

b2

(3)

]

[b2]

[b2]

From: Agen, Jarrod
Sent: Saturday, September 30, 2006 2:02 PM
To: Rosenzweig, Paul; Sciara, Nicole; Baker, Stewart; Scardaville, Michael; 'Isles, Adam'; Knocke, William R; Bergman, Cynthia; 'Montgomery, Kathleen'
Subject: REVISED PNR PAG

I believe this incorporates all the latest....please review. I'll also adjust S1 statement.

TALKING POINTS

- Secretary Chertoff has [b5] initialed [b5]
- [b5] counter-terrorism information collected by the Department will be shared, as necessary with other federal agencies.
- [b5]
- The [b5] agreement has now been returned to the European Union for its final review and consideration.
- [b5], the appropriate security information will [b5] be exchanged. Planes will continue to fly uninterrupted and our national security will not be impeded.
- [b5] has a legal and moral obligation to protect its borders, and [b5] has a right to verify who it is admitting into the country. This department [b5] will use every legal authority at our disposal, including valuable PNR data, to secure [b5]
- 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.

[b2]

- PNR data is used for our shared goal of combating terrorism while respecting fundamental rights and freedoms, notably privacy. ()

b5

- () Here in the United States and in Europe, we all have to be smart and thorough in scrutinizing people seeking to () including those who may not be on watchlists but could mean to do us harm.

b5

- 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 () on this issue with our European allies, with whom we have a great relationship ()

b5

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. 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

(

b2

)

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 store the info 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: With there be further negotiations?

A: We look forward to finalizing b5 with our European allies, with whom we have a great relationship b5

Q: b5

A: We have agreed to work towards a "push" system, which is b5 This would mean that air carriers are feeding us info b5

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 [b5] 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: [b5]
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.

[b5] found [b5] CBP [b5] in full compliance with representations made in the PNR agreement. CBP has invested substantial time, capital, and expertise to bring its operations and procedures into compliance. This is a recognizable achievement. [b5]

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: [b5]
> APIS is merely an automated vehicle for the collection of information from government-issued identity documents accepted for international travel. 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.

[66]

From: Baker, Stewart [b2]
Sent: Saturday, September 30, 2006 5:55 PM
To:

b2
b6

Rosenzweig, Paul;

Subject: FW: STATEMENT BY HOMELAND SECURITY SECRETARY MICHAEL CHERTOFF ON PASSENGER NAME RECORD AGREEMENT WITH EUROPEAN UNION

From: DHS Press Office
Sent: Saturday, September 30, 2006 4:34 PM
Subject: STATEMENT BY HOMELAND SECURITY SECRETARY MICHAEL CHERTOFF ON PASSENGER NAME RECORD AGREEMENT WITH EUROPEAN UNION

Press Office
U.S. Department of Homeland Security

Press Release

September 30, 2006
Contact: (202) 282-8010

STATEMENT BY HOMELAND SECURITY SECRETARY MICHAEL CHERTOFF ON PASSENGER NAME RECORD AGREEMENT WITH EUROPEAN UNION

I am pleased to announce that following our negotiations with representatives of the European Union (EU), I have initialed a draft formal U.S. /EU agreement regarding the sharing of Passenger Name Record (PNR) data. Most importantly, 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. Importantly, 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 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.

The recently uncovered terror plot concerning flights from the United Kingdom to the United States is evidence that terrorists continue to target our aviation industry, specifically U.S. bound flights from Europe. Free and open information sharing between the United States and Europe has proven to be a valuable weapon to combat terrorists before they can do harm. The transfer of PNR data by air carriers to our department is an absolute necessity to safeguarding air travel and public security.

(4)

I want to thank the European Union negotiators for their cooperation and look forward to finalizing an agreement on this issue with our European allies, with whom we have a great relationship on a number of other security-related matters, and indeed to an international approach on PNR analysis.

###

From: "Baker, Stewart" [b2]

To:

b2
b6

"Rosenzweig, Paul"

Date: Saturday, September 30, 2006 06:23PM

Subject: PNR press points

This is not for release but provides useful talking points and background on the PNR issue.

From: Agen, Jarrod [mailto:[b2]]

Sent: Saturday, September 30, 2006 5:34 PM

To: [b6] ; Myers, Julie L; Allen, Charles; [b6] Hawley, Kip; Ahern, Jayson P; Kraninger, Kathleen; Isles, Adam; Sciara, Nicolle; AGEN, JARROD; Baker, Stewart; Rosenzweig, Paul; Scardaville, Michael; Knocke, William R; [b6]

Cc: [b6] Klundt, Kelly R; Smith, Nick J; Kelly, Kevin; Cannatti, Ashley

Subject: FINAL PNR PAG

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 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.

Attachments:(Click the filename to launch)

FINAL EU-US PNR Agreement PAG.doc

From: STEVEN L BASHA/NE/USCS
To: "ALFONSO ROBLES" [Redacted] Low (b)(2)/(b)(6)
cc: "SCOTT FALK" [Redacted] Low (b)(2)/(b)(6) (b)(6)
[Redacted] Low (b)(2)/(b)(6)
Date: Thursday, October 05, 2006 09:01AM
Subject: Fw: TECS SORN Routine Use Interpretation

Fyi

Steve

----- Original Message -----

From: [Redacted] (b)(6) [Redacted] Low (b)(2)/(b)(6)
Sent: 10/05/2006 08:46 AM
To: [Redacted] (b)(6) [Redacted] Low (b)(2)/(b)(6)
Cc: "Basha, Steven L" [Redacted] Low (b)(2)/(b)(6) (b)(6)
[Redacted] Low (b)(2)/(b)(6)
Subject: RE: TECS SORN Routine Use Interpretation

[Redacted] (b)(6)

[Redacted] (b)(5) - Attorney client & deliberative
[Redacted]
[Redacted] (b)(6)

[Redacted] (b)(6)
Deputy Associate General Counsel (Enforcement)
Department of Homeland Security
[Redacted] Low (b)(2)/(b)(6)

This communication, along with any attachments, is covered by federal and state law governing electronic communications and may contain confidential and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of this message is strictly prohibited. If you have received this in error, please reply immediately to the sender and delete this message. Thank you.

-----Original Message-----

From: [Redacted] (b)(6) [Redacted] Low (b)(2)/(b)(6)
Sent: Thursday, October 05, 2006 8:27 AM
To: [Redacted] (b)(6)
Cc: Basha, Steven L
Subject: TECS SORN Routine Use Interpretation


[Redacted] Low (b)(2)

(6)

(b)(5) - Attorney client & deliberative (b)(6)



Low (b)(2)



(b)(5) - Attorney client & deliberative (b)(6)



(See attached file: TICS_and_System_w_2_Records.doc)

(b) (5)

Office of Chief Counsel
U.S. Customs and Border Protection

Low (b)(2) (b)(5)



This document, and any attachment(s) hereto, may contain confidential and/or sensitive attorney-client privileged, attorney work-product, and/or U.S. Government information, and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please consult with the CBP Office of Chief Counsel before disclosing any information contained in this e-mail.

Low (b)(2)



[b6]

From: [b6 b2]
Sent: Wednesday, October 25, 2006 3:52 PM
To: [b6]
Subject: Re: FW: PNR - very rough draft of checklist

Attachments: PNR checklist for components (10 17 2006) clean [b6] comments)-mseds ([b6] comments 10-25-06).doc; PNR checklist for components (10 17 2006) clean [b6] comments)-mseds.doc



PNR checklist for components (... components (...

Ok--here are my comments (I fear my redlines may appear as the same color--pink--as yours, making your review a bit more complicated). FYI--I also sent the outbound authorities memo to SB this afternoon for approval--with any luck I may have that to you in the morning if he likes it! (See attached file: PNR checklist for components (10 17 2006) clean [b6] comments)-mseds [b6] comments 10-25-06).doc)

[b6]
Office of Chief Counsel
U.S. Customs and Border Protection
Phone [b2]
Fax: [b2]
Email: [b6 b2]

This document, and any attachment(s) hereto, may contain confidential and/or sensitive attorney-client privileged, attorney work-product, and/or U.S. Government information, and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please consult with the CBP Office of Chief Counsel before disclosing any information contained in this e-mail.

[b6 b2]

To: [b6 b2]

checklist
10/25/2006 03:01
PM

cc:
Subject: FW: PNR - very rough draft of

Here it is - [b6]

[b6]
Senior Counsel
Department of Homeland Security
Office of the General Counsel
[, Washington, D.C. 20528
Fax: b2]

This communication, along with any attachments, is covered by federal and state law governing electronic communications and may contain confidential and legally privileged

3

information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of this message is strictly prohibited. If you have received this in error, please reply immediately to the sender and delete the message. Thank you.

-----Original Message-----

From: Scardaville, Michael
Sent: Tuesday, October 24, 2006 12:50 PM
To: [b6]
Subject: RE: PNR - very rough draft of checklist

My thoughts attached.

Mike

[b2]

-----Original Message-----

From: [b6]
Sent: Tuesday, October 24, 2006 11:29 AM
To: Scardaville, Michael
Subject: Fw: PNR - very rough draft of checklist

Mike - know you looked at this before, but did you have additional comments now that this is just the brief summary and we're doing additional, more in-depth documents? Also looking for comments from cbp and po. [b6]

----- Original Message -----

From: [b6]
To: 'Sales, Nathan' [b2 b6]
Scardaville, Michael [b2 b6]
Sent: Tue Oct 17 16:23:20 2006
Subject: RE: PNR - very rough draft of checklist

This has quick cbp edits, and I incorporated [b6] comment 7 into the text, but probably want a thorough scrub on this all around before going forward - [b6]

[b6]

Senior Counsel

Department of Homeland Security

Office of the General Counsel

[Washington, D.C. 20528

b2

Fax: []

This communication, along with any attachments, is covered by federal and state law governing electronic communications and may contain confidential and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of this message is strictly prohibited. If you have received this in error, please reply immediately to the sender and delete the message. Thank you.

From: Sales, Nathan [mailto:[b2]

Sent: Tuesday, October 17, 2006 1:44 PM
To: [b6] Scardaville, Michael; [b6]
Subject: RE: PNR - very rough draft of checklist

Here are my edits, [b6] I think this is pretty close. As we discussed on the phone, the majority of my comments are line edits, but there are two bigger-ticket items as well.

Best,

NAS

Nathan A. Sales
Deputy Assistant Secretary for Policy Development
Department of Homeland Security

[b2]

From: [b6 b2]
Sent: Tuesday, October 17, 2006 12:06 PM
To: Scardaville, Michael; [b6]
Cc: Sales, Nathan
Subject: PNR - very rough draft of checklist

All - [

b5

] [b6]

[b6]

Senior Counsel
Department of Homeland Security
Office of the General Counsel
[Washington, D.C. 20528

b2

Fax:]

This communication, along with any attachments, is covered by federal and state law

governing electronic communications and may contain confidential and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of this message is strictly prohibited. If you have received this in error, please reply immediately to the sender and delete the message. Thank you.

(See attached file: PNR checklist for components (10 17 2006) clean [b6] comments) -mseds.doc)

(b)(6)

[Redacted]

From: (b)(6) [Redacted] low (b)(7) (b)(6)
Sent: Thursday, October 26, 2006 12:29 PM
To: Scardaville, Michael
Cc: Sales, Nathan; [Redacted] (b)(6)
Subject: RE: PNR Access Requests and CBP Field Guidance

Attachments: PNRsummary for components (10 25 2006) clean-mseds.doc



PNRsummary for components (10 ...

Mike--do we need to add a footnote re our discussions re Switzerland and Iceland to this memo?

(b)(6)

[Redacted]
Office of Chief Counsel
U.S. Customs and Border Protection

Email: [Redacted] low (b)(7) (b)(6)

This document, and any attachment(s) hereto, may contain confidential and/or sensitive attorney-client privileged, attorney work-product, and/or U.S. Government information, and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please consult with the CBP Office of Chief Counsel before disclosing any information contained in this e-mail.

"Scardaville,
Michael"

To: "Sales, Nathan"

<Mike.Scardaville

cc: "[Redacted] [Redacted] (b)(6)

Subject: RE: PNR Access Requests and CBP
Guidance

Field

10/26/2006 11:55
AM

(b)(6)

A couple of edits responding to [Redacted]'s comments in the track changes version.

Mike

low (b)(7) (b)(6)
-----Original Message-----

From: Sales, Nathan
Sent: Thursday, October 26, 2006 9:01 AM
To: Scardaville, Michael
Subject: FW: PNR Access Requests and CBP Field Guidance

Mike, will you please look at this and let me know if it's ready to go to the components? I'd like to circulate it by noon. Thanks.

Nathan A. Sales
Deputy Assistant Secretary for Policy Development Department of Homeland Security

-----Original Message-----

From: [Redacted] (b)(7)(F)
Sent: Wednesday, October 25, 2006 10:34 PM
To: Sales, Nathan
Subject: RE: PNR Access Requests and CBP Field Guidance

Apologies for the delay - didn't get the last changes until late today.
Attaching a clean and redlined version as reviewed by Mike, Privacy, and CBP (OFO and Chief Counsel). Please let me know if you think other revisions are necessary. Thx, [Redacted]

[Redacted] (b)(7)(F)
Senior Counsel
Department of Homeland Security
Office of the General Counsel
Washington, D.C. 20528

This communication, along with any attachments, is covered by federal and state law governing electronic communications and may contain confidential and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of this message is strictly prohibited. If you have received this in error, please reply immediately to the sender and delete the message. Thank you.

-----Original Message-----

From: Sales, Nathan
Sent: Wednesday, October 25, 2006 9:24 AM
To: [Redacted] (b)(7)(F)
Subject: RE: PNR Access Requests and CBP Field Guidance

Great. Thanks for the update. I'd like to get this to the components early today, so I appreciate the quick turnaround.

Best,
NAS

Nathan A. Sales
Deputy Assistant Secretary for Policy Development Department of Homeland Security

-----Original Message-----

From: [Redacted] (b)(7)(F)
Sent: Wednesday, October 25, 2006 9:23 AM
To: Sales, Nathan
Subject: Re: PNR Access Requests and CBP Field Guidance

Have most comments on the summary and am waiting for one last review of the revision - [Redacted]

----- Original Message -----

From: Sales, Nathan
To: Scardaville, Michael; [Redacted] (b)(7)(F)
Sent: Wed Oct 25 09:21:14 2006
Subject: RE: PNR Access Requests and CBP Field Guidance

Morning, all. Are we in a position to circulate the revised versions of the documents we discussed at Monday's meeting? Please let me know where things stand with the request letters and the thumbnail summary.
Thanks much.

Best,
NAS

Nathan A. Sales
Deputy Assistant Secretary for Policy Development Department of Homeland Security

[REDACTED]

(b)(6)
(b)(7)(C)

-----Original Appointment-----

From: [REDACTED] <CTR> On Behalf Of Sales, Nathan

Sent: Wednesday, October 18, 2006 1:34 PM

To: Scardaville, Michael; [REDACTED]

Subject: Updated:PNR Access Requests and CBP Field Guidance

When: Monday, October 23, 2006 9:30 AM-11:00 AM (GMT-05:00) Eastern Time (US & Canada).

Where: 17002 conference room

(b)(6)
(b)(7)(C)

<<Draft PNR request from components (10.17.2006).doc>> <<Draft PNR approval from CBP (10.17.2006).doc>> (See attached file: PNRsummary for components (10 25 2006) clean-
mseds.doc)

[b6]

From: [b6 b2]
Sent: Monday, October 30, 2006 1:26 PM
To: [b6]
Subject: 'Fw: PNR implementation - CBP letters

Attachments: PNR access invitation from CBP (10.27.2006).doc; PNR access request from components (10.27.2006).doc; PNR access approval from CBP (10.27.2006).doc



PNR access invitation from CBP.. PNR access request from compon... PNR access approval from CBP (.

fyi--apparently we were not copied on this. I would characterize this as "cart before the horse", since i am still reviewing the field guidance....

[b6]
Office of Chief Counsel
U.S. Customs and Border Protection
Phone: [b2]
Fax: [b2]
Email: [b6 b2]

This document, and any attachment(s) hereto, may contain confidential and/or sensitive attorney-client privileged, attorney work-product, and/or U.S. Government information, and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please consult with the CBP Office of Chief Counsel before disclosing any information contained in this e-mail.

----- Forwarded by [b6] /NE/USCS on 10/30/2006 01:25 PM -----

[b6 b2]
10/30/2006 01:19 PM
To: [b6]
cc:
Subject: PNR implementation -- CBP letters

[b6]
Office of Field Operations
Customs and Border Protection

[b2] fax
----- forwarded by [b6] NE/USCS on 10/30/2006 01:19 PM -----

"Sales, Nathan"
To: "Jacksta, Bob M"
"Kraninger, Kathleen"

[b6 b2]
10/27/2006 06:23 PM

[b6 b2]

b6
b2

"Baker, Stewart"

"Scardaville, Michael"

Subject: PNR implementation -- CBP letters

Team,

I am attaching three document templates to this email: (1) an invitation from CBP to the components indicating the new availability of PNR data; (2) a request from the components for access to PNR; and (3) an approval from CBP granting access to the components. My goal is for CBP and the relevant components to be able to personalize these letters by adding the requested information, and exchange them, by COB Tuesday of next week.

The letters are fairly self-explanatory, but I wanted to draw several features to the group's attention. First, please note that [

b5

Second, the request letter from the components to CBP includes [

b5]

[b5]
A word on timing. The Secretary is personally very interested in the progress we are making on implementing the new PNR agreement. I am scheduled to brief him on our efforts on Wednesday of next week. I need to be able to tell him [

b5
→ So we really need to make this happen by Tuesday.

Thanks again. We're not to home plate yet, but I think we're rounding third. I really appreciate this group's hard work on, and dedication to, an initiative that is of the highest priority to the Secretary.

Best,
NAS

Nathan A. Sales
Deputy Assistant Secretary for Policy Development Department of Homeland Security

[b 2]

(See attached file: PNR access invitation from CBP (10.27.2006).doc) (See attached file: PNR access request from components (10.27.2006).doc) (See attached file: PNR access approval from CBP (10.27.2006).doc)

From: [Redacted] *low (b)(2) (b)(6)*
To: [Redacted]
Date: Monday, November 27, 2006 02:11PM
Subject: Re: PNR Access Requests and CBP Field Guidance

[Redacted]

*(b)(5)
A/C
Delib*

[Redacted] *(b)(6)*
Office of Chief Counsel (Enforcement)
US Customs and Border Protection

[Redacted] *(b)(6) low (b)(2)*
Sent from my Blackberry

----- Original Message -----

From: [Redacted] *(b)(6) low (b)(2)*
Sent: 11/27/2006 01:57 PM
To: [Redacted] *(b)(6) low (b)(2)*
Subject: FW: PNR Access Requests and CBP Field Guidance

Probably need to revisit this with mike - he mentioned it again today -

[Redacted] *(b)(6)*
Senior Counsel
Office of General Counsel
Department of Homeland Security

(b)(6) low (b)(2)

-----Original Message-----

From: Scardaville, Michael [Redacted] *(b)(6) low (b)(2)*
Sent: Friday, October 27, 2006 1:43 PM
To: [Redacted] Scardaville, Michael
Cc: [Redacted]
Subject: RE: PNR Access Requests and CBP Field Guidance

(b)(6)

Thanks.

I also just had an idea. [Redacted]

*(b)(5)
A/C
Delib*

Mike
[Redacted]

(b)(6) low (b)(2)

-----Original Message-----

Low (b)(2)
[Redacted]

(1)

low (b)(2)
(b)(6)

From: [redacted]
Sent: Friday, October 27, 2006 12:53 PM
To: Scardaville, Michael
Cc: [redacted]
Subject: RE: PNR Access Requests and CBP Field Guidance

(b)(6)

Here is the scanned copy (both in one doc)--copying [redacted] also in case (b)(6)
she
does not have a copy either. [redacted] (b)(6)
(See attached file: iceland-switzerland PNR arrangements.pdf)

[redacted]
Office of Chief Counsel
U.S. Customs and Border Protection

(b)(6)
low (b)(2)

This document, and any attachment(s) hereto, may contain confidential and/or sensitive attorney-client privileged, attorney work-product, and/or U.S. Government information, and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please consult with the CBP Office of Chief Counsel before disclosing any information contained in this e-mail.

"Scardaville,
Michael"

[redacted]
[redacted]

To: [redacted]

low (b)(2)
(b)(6)

cc:
Subject: RE: PNR Access
Guidance

Requests and CBP Field
10/27/2006 09:57
AM

low (b)(2)
(b)(6)

Can you fax me the Swiss agreement at [redacted]? Also am I correct in recalling that Iceland was covered by an exchange of letters? If so, can you please send those as well?

Mike
[redacted]

-----Original Message-----
From: [redacted]
Sent: Friday, October 27, 2006 9:34 AM
To: [redacted]

low (b)(2)
(b)(6)

Low (b)(2)
[redacted]

Cc: [redacted] Scardaville, Michael; Sales, Nathan;
Subject: Re: PNR Access Requests and CBP Field Guidance

(b)(6)

[redacted]

(b)(5) - AK

Office of Chief Counsel
U.S. Customs and Border Protection

(b)(6)

[redacted]

low (b)(2)
(b)(6)

This document, and any attachment(s) hereto, may contain confidential and/or sensitive attorney-client privileged, attorney work-product, and/or U.S. Government information, and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please consult with the CBP Office of Chief Counsel before disclosing any information contained in this e-mail.

[redacted]
10/27/2006 09:32
AM

To: [redacted]
cc: [redacted]

[redacted]

"Sales, Nathan"
[redacted]

low (b)(2)
(b)(6)

Requests and CBP Field
[redacted]

Subject: Re: PNR Access
Guidance (Document link:
[redacted])

b5

[redacted]. As a technical issue, we cannot carve out access within the system to the Swiss and Icelandic flights just as we could not carve out access to EU flights under the old agreement.

(S)(G)
[Redacted]
Office of Field Operations
Customs and Border Protection
[Redacted]

low (b)(2)
(b)(6)

[Redacted]
[Redacted]
10/27/2006 08:52
[Redacted] "Sales, Nathan"
AM
[Redacted]

To: [Redacted]
cc: [Redacted]

(b)(6)
low (b)(2)

[Redacted]
[Redacted]

Requests and CBP Field
[Redacted]

Subject: Re: PNR Access
Guidance (Document link:
[Redacted])

Just a reminder-- [Redacted]
[Redacted]

(b)(5)-
AC
Debit

(S)(G)
[Redacted]
Office of Chief Counsel
U.S. Customs and Border Protection
[Redacted]

low (b)(2)
(b)(6)

This document, and any attachment(s) hereto, may contain confidential and/or sensitive attorney-client privileged, attorney work-product, and/or U.S. Government information, and is not for release, review, retransmission, dissemination or use by anyone other than the intended recipient. Please consult with the CBP Office of Chief Counsel before disclosing any information contained in this e-mail.

[Redacted] (S)(G)

Low (b)(2)
[Redacted]

[Redacted]
10/27/2006 08:15
AM
[Redacted]
[Redacted]
[Redacted]
Requests and CBP Field
[Redacted]

To: "Sales, Nathan"
cc: [Redacted]
[Redacted]

(S)(6)
low (b)(2)

Subject: Re: PNR Access
Guidance (Document link: [Redacted])

Here are the revised letters.

(See attached file: Draft PNR request from components (10262006).doc) (See attached file: Draft PNR access invitation from CBP (10262006).doc) (See attached file: Draft PNR Access Approval letter (10272006).doc)

If you have any questions, please let me know.
Thanks,

[Redacted] (S)(6)
Office of Field Operations
Customs and Border Protection
[Redacted] low (b)(2)
(S)(6)

"Sales, Nathan"
[Redacted]
Michael"

To: "Scardaville,
[Redacted]

[Redacted]
10/26/2006 09:05
AM
[Redacted]
[Redacted]
[Redacted]
[Redacted]

[Redacted]
[Redacted]
[Redacted]

low (S)(2)
(S)(6)

Low (b)(2)
[Redacted]

Requests and CBP Field

cc:

Subject: Re: PNR Access
Guidance

(b)(6)
[redacted] thanks for sending the updated "checklist.". CBP, please give me the status of the revised letters. Thanks.

Sent from my BlackBerry Wireless Handheld

----- Original Message -----

From: Sales, Nathan

To: Scardaville, Michael; [redacted] (b)(6)

Sent: Wed Oct 25 09:21:14 2006

Subject: RE: PNR Access Requests and CBP Field Guidance

Morning, all. Are we in a position to circulate the revised versions of the documents we discussed at Monday's meeting? Please let me know where things stand with the request letters and the thumbnail summary. Thanks much.

Best,
NAS

Nathan A. Sales
Deputy Assistant Secretary for Policy Development
Department of Homeland Security
[redacted]

low (b)(2)
(b)(6)

-----Original Appointment-----

From: [redacted] On Behalf Of Sales, Nathan

Sent: Wednesday, October 18, 2006 1:34 PM

To: Scardaville, Michael; [redacted] 17002 Conference room (Large); [redacted] (b)(6)

Subject: Updated:PNR Access Requests and CBP Field Guidance

When: Monday, October 23, 2006 9:30 AM-11:00 AM (GMT-05:00) Eastern Time (US & Canada).

Where: 17002 conference room

<<Draft PNR request from components (10.17.2006).doc>> <<Draft PNR approval from CBP (10.17.2006).doc>>

[Redacted] (b)(6)

From: [Redacted]
Sent: Friday, January 19, 2007 9:04 AM (b)(6)
To: [Redacted]
Subject: PNR Data Retention

Attachments: PNR Agreement US 10.19.06.pdf; 061010 Signed PNR Interpretations.pdf; PNR summary for components (10.27.2006 FINAL).doc; (errata clean) FINAL PNR Undertakings of DHS-CBP 5-25-04.doc



PNR Agreement US 10.19.06.pdf ... Interpretati... components (10... FINAL PNR Under...

low
(b)(2)
(b)(6)

From: [Redacted]

Sent: Thursday, January 18, 2007 1:12 PM
To: [Redacted]
Subject: Re: PNR Data Retention

(b)(6)

[Redacted]
12/07/2006 02:10 PM

To: [Redacted]
Cc: [Redacted]
Subject: PNR Data Retention

low
(b)(2)
(b)(6)

[Redacted] (b)(6)

Here is the current status with respect to EU PNR Data Retention. Please note that I have included relevant extracts as well as related documents below. You may or may not want to include all of this information so I wanted you know it is there.

PNR Data Retention was defined in the EU PNR Undertakings signed on May 27, 2004 as follows: All EU PNR Data can be retained for 3.5 years. Data that has been accessed during the 3.5 year period may be retained for an additional 8 years.

Following the decision by the EU court to not recognize the undertakings agreement, an interim agreement was signed on October 19, 2006 by DHS and October 16, 2006 by the EU. This interim agreement did not specifically address retention periods, so the periods specified in the original undertakings are being used until a final agreement can be negotiated. The interim agreement expires July 31, 2007. Negotiations on the final agreement are scheduled to begin in January 2007.

The DHS Assistant Secretary for Policy issued a memo documenting interpretations of the

(10)

interim agreement highlighting how the interim agreement "will have expired before Paragraph 15 of the Undertakings requires 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."

DHS also issued a PNR Summary for Components that reiterated how the 3.5 year agreement is not expected to impact PNR data retention before a new agreement is reached.

As documented in the SORN and PIA published by DHS during the last month, PNR Data that is not associated with flights between the US and the EU will be retained for up to forty years. "Generally, data maintained specifically by ATS will be retained for up to forty years. Certain data maintained in ATS may be subject to other retention limitations pursuant to applicable arrangements (e.g., PNR information derived from flights between the U.S. and the European Union). Cost and performance impact of data retention may lead to retention periods less than forty years."

Please let me know if you have any questions or need anything else.

Thanks,



(b)(6)

Extract from EU PNR Undertakings signed on May 27, 2004

Storage of PNR Data

12) Subject to the approval of the National Archives and Records Administration (44 U.S.C. 2101, et seq.), CBP will limit on-line access to PNR data to authorized CBP users. These authorized CBP users would include employees assigned to analytical units in the field offices, as well as employees assigned to the National Targeting Center. As indicated previously, persons charged with maintaining, developing or auditing the CBP database will also have access to such data for those limited purposes.

for a period of seven (7) days, after which the number of officers authorized to access the PNR data will be even further limited for a period of three years and 6 months (3.5 years) from the date the data is accessed (or received) from the air carrier's reservation system. After 3.5 years, PNR data that has not been manually accessed during that period of time,

will be destroyed. PNR data that has been manually accessed during the initial 3.5 year period will be transferred by CBP to a deleted record file. Although the PNR record is not technically deleted when it is transferred to the Deleted Record File, it is stored as raw data (not a readily searchable form and, therefore, of no use for "traditional" law enforcement investigations) and is only available to authorized personnel in the Office of Internal Affairs for CBP (and in some cases the Office of the Inspector General in connection with audits) and personnel responsible for maintaining the database in CBP's Office of Information Technology, on a "need to know" basis, where it will remain for a period of eight (8) years before it is destroyed. This schedule, however, would not apply to PNR data that is linked to a specific enforcement record (such data would

remain accessible until the enforcement record is archived). With respect to PNR which CBP accesses (or receives) directly from air carrier reservation systems during the effective dates of these Undertakings, CBP will abide by the retention policies set forth in the present paragraph, notwithstanding the possible expiration of the Undertakings pursuant to paragraph 46 herein;

Extracts from DHS Memo Providing PNR Summary for Components

CBP

As under the previous arrangement, CBP ? the entity that, pursuant to statute, receives PNR data from air carriers flying to and from the U.S. ? will continue to access 34 PNR data elements listed in Appendix A of the Undertakings to the extent carriers store such data in their reservation and departure control systems. CBP will also have access to additional frequent flyer information under the new

interpretations of the Undertakings, to the extent any of the data elements listed in Appendix A may be obtained within the frequent flier field. Although sensitive data will continue to be restricted, the new interpretations recognize that even sensitive information may be used in some instances to protect the vital interests of the data subject or others.

...
Data retention: Components/Agencies must certify that for any PNR data they receive and retain, they will observe the retention periods set forth in Paragraph 15 of the Undertakings for the duration of the interim agreement. As the shortest retention period in that paragraph is 3.5 years, and this provision is expected to be renegotiated before any destruction of data would be necessary, this standard is unlikely to have any practical impact on the retention of PNR.

Documents related to the interim agreement and related interpretation and communication from DHS:

(See attached file: PNR Agreement US 10.19.06.pdf) (See attached file: 061010 Signed PNR Interpretations.pdf)

(See attached file: PNR summary for components (10.27.2006 FINAL).doc)

Here is the last copy I have of the Undertakings:

(See attached file: (errata clean) FINAL PNR Undertakings of DHS-CBP 5-25-04.doc)

[REDACTED] (b)(6)
Sr. Financial Analyst, SAIC, supporting the Targeting and Analysis Systems Program Office
Department of Homeland Security U.S. Customs and Border Protection
[REDACTED]

10/11
(b)(2)
(b)(6)

Overview

- PNR Information
- PNR Data Elements
- ATS-P PNR Page
- ATS PNR Data Flow Overview
- Current Use of PNR Data
- US/EU PNR Sharing Agreement



Homeland
Security

~~For Official Use Only~~

PNR Information

- Travelers provide data to airlines or travel agents
- Airlines use data to manage passenger carriage business
 - Issue tickets, track reservations, assign seats, track frequent fliers
- DHS/CBP collected PNR data since 1992 on a voluntary basis
- Air Transport Security Act of 2001
 - Mandates electronic transmission of PNR to CBP
 - Transmitted up to 72 hours before takeoff



U.S. DEPARTMENT OF
HOMELAND SECURITY

~~For Official Use Only~~

Passenger Name Record (PNR) Data Elements

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



Homeland
Security

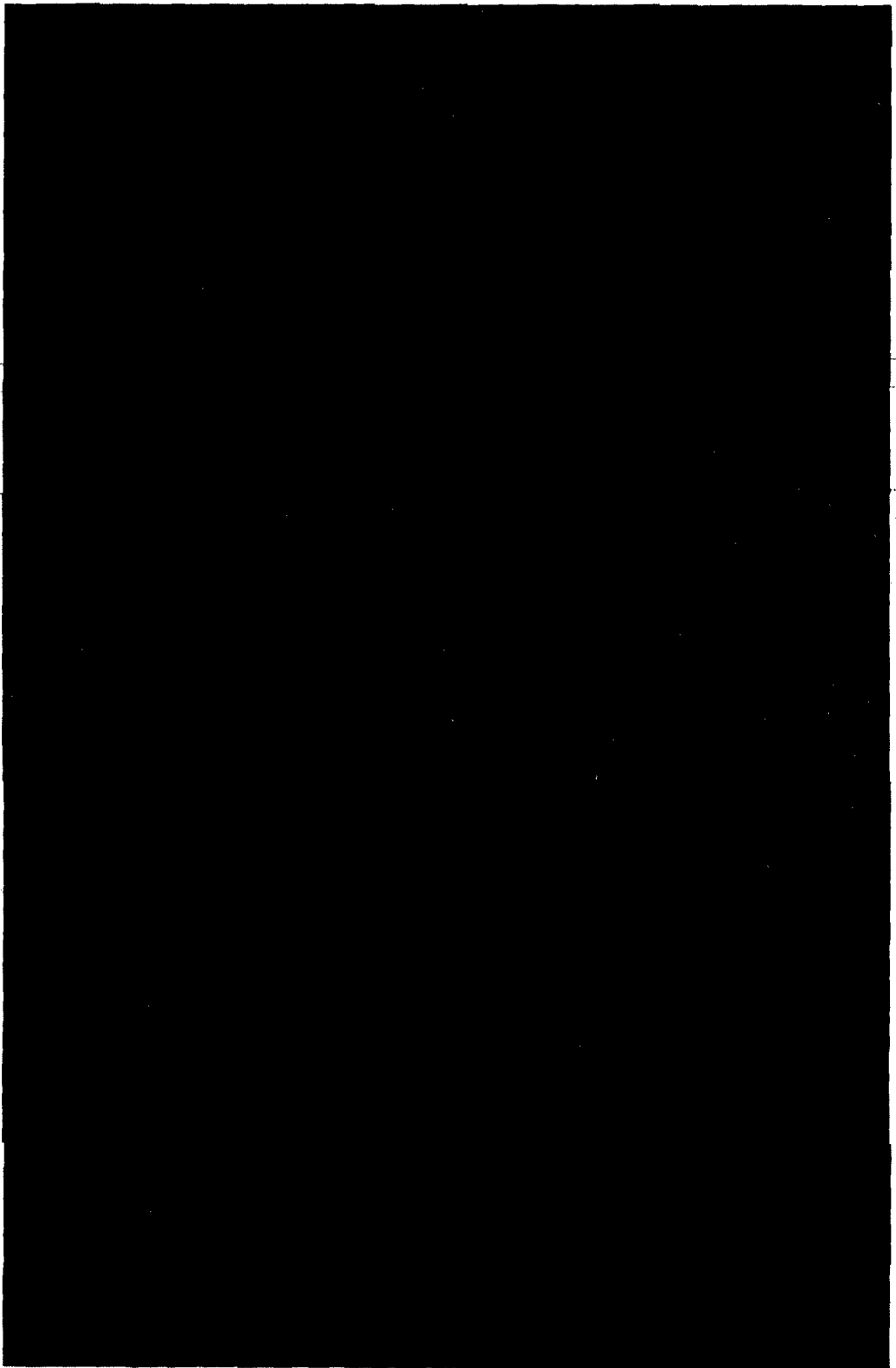
~~For Official Use Only~~

* Restricted field

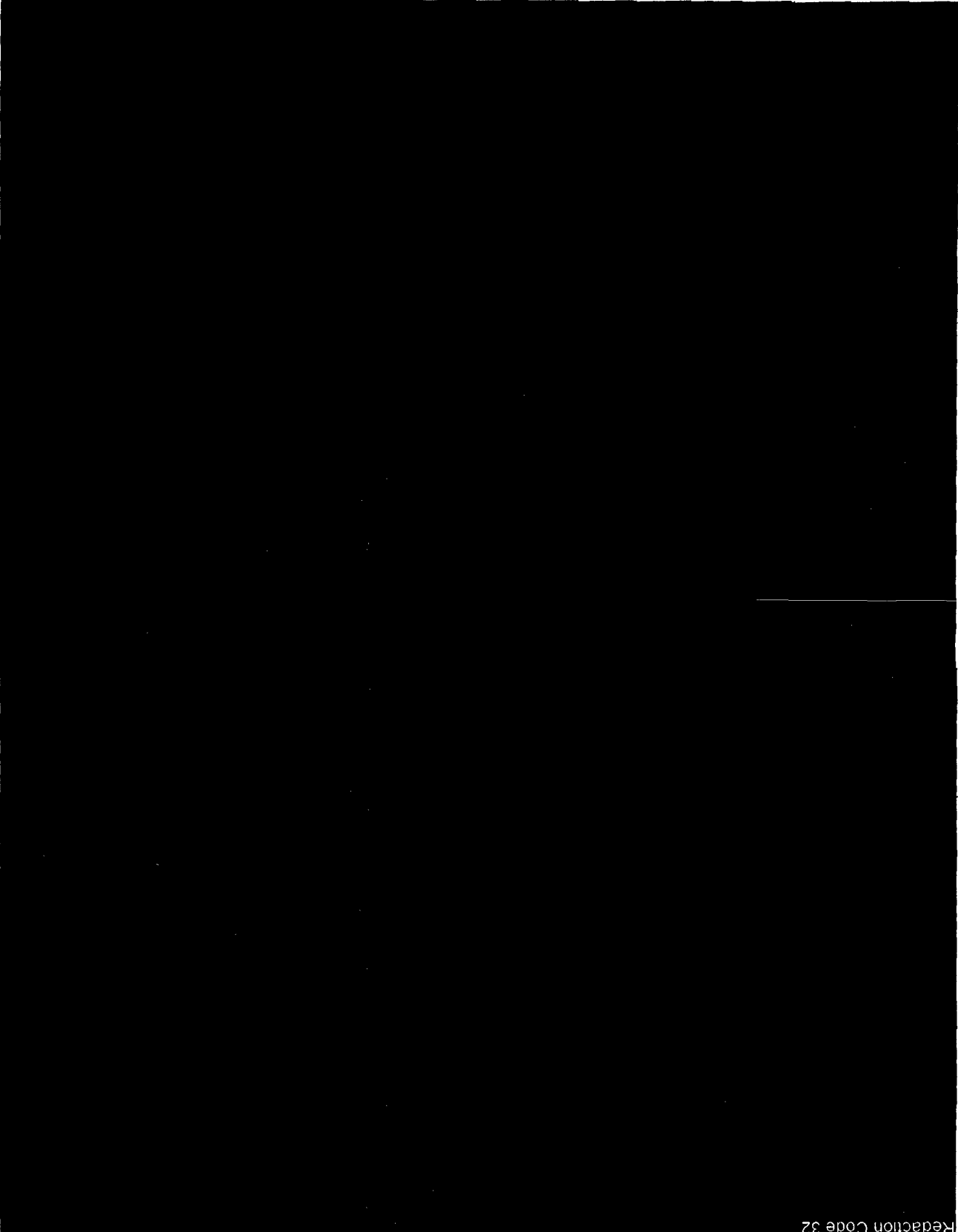


SECRET

~~For Official Use Only~~



2544
021E
1979

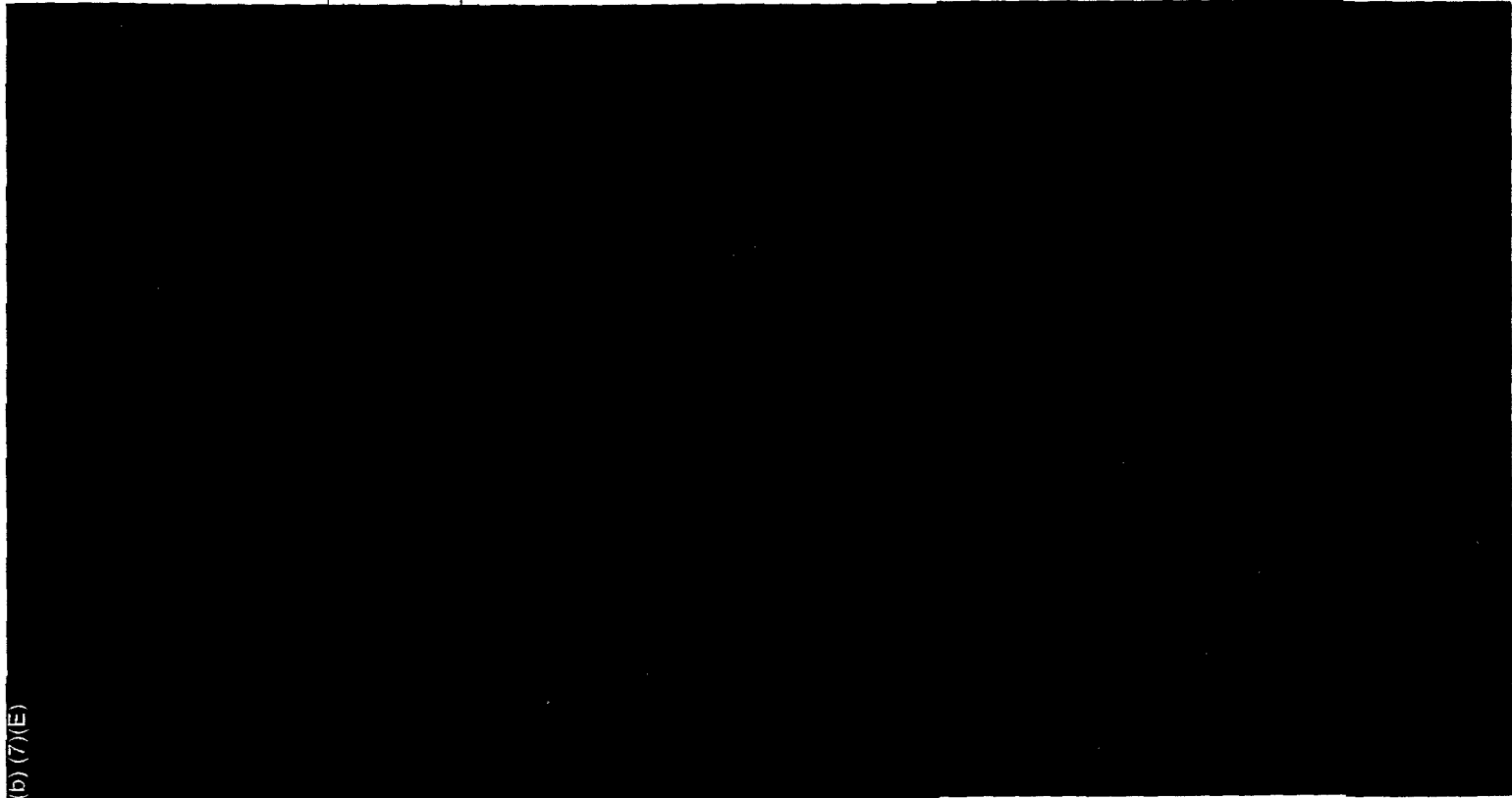


Redaction Code 32

1341 P 9
E 7
99

ATS PNR Data Flow Overview

b6
b2 Hsh
b7E



(b) (7)(E)



CONFIDENTIAL
SECRET

~~For Official Use Only~~

Current use of PNR data

- DHS/CBP primarily uses to support in-bound targeting of international flights
 - PNR Data fed into Automated Targeting System—Passenger (ATS-P)
 - PNR is one of several data feeds into this system

b2 High
b7E

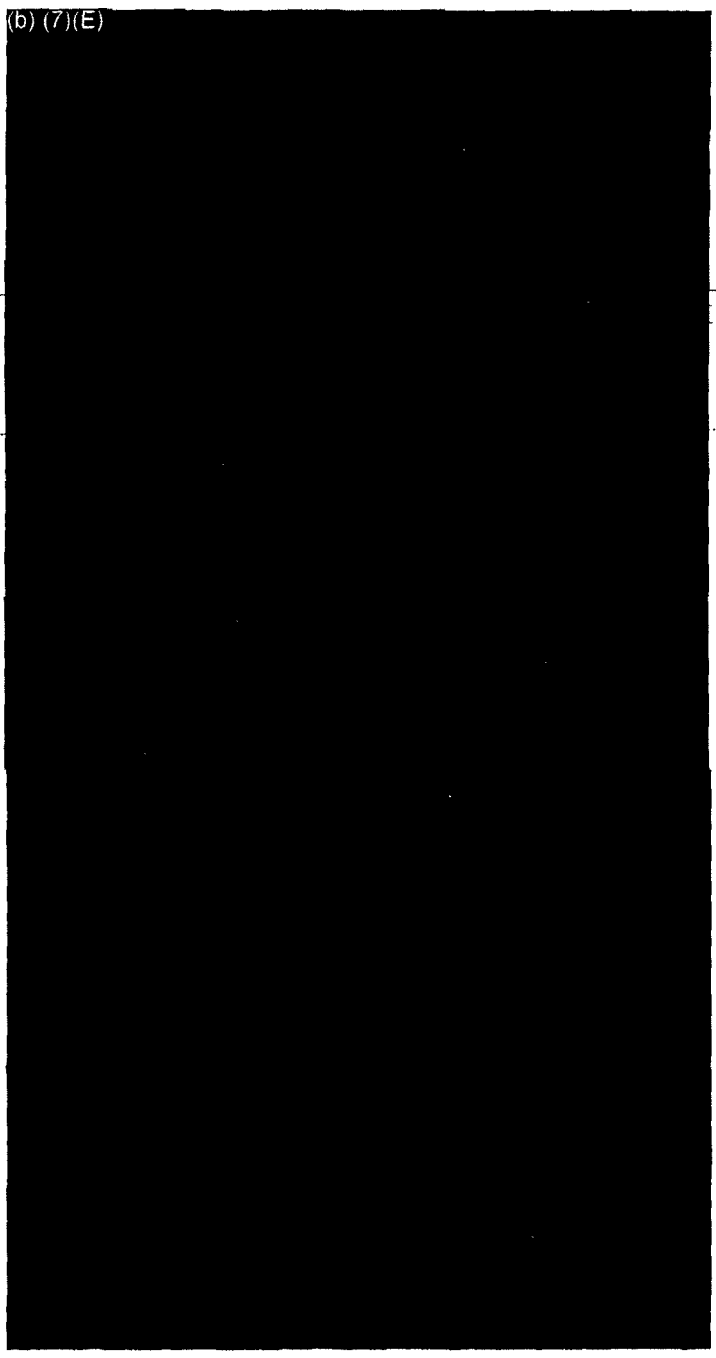


Homeland
Security

~~For Official Use Only~~

Link and Pattern Analysis Examples

b2
b7c
b7d



(b) (7)(E)



SECRET

~~For Official Use Only~~

Chronology of U.S.-EU Engagement

- 2003: CBP Issues Interim Final Rule
- May 2004: DHS concludes an international agreement with the EU on CBP's access to and use of PNR
 - May 2004: The "Undertakings" are published in the Federal Register
- September 2005: U.S.-EU Joint Review
- May 2006: European Court of Justice rules against the European Commission
- October 2006: Interim replacement agreement signed



Homeland
Security

~~For Official Use Only~~

October 2006 U.S.-EU Agreement

- * Allows for greater flexibility in sharing PNR for counterterrorism purposes
 - Some DHS offices now have access equal to CBP's.
 - "Facilitated disclosure" of PNR to other agencies of the United States Government

b2 High
b7E



Home Land
Security

~~For Official Use Only~~

(U) TALKING POINTS

1. (U//~~FOUO~~) Background information on the Passenger Name Record (PNR) issue for today's PNR strategy meeting

(U//~~FOUO~~) *The EU Court recently ruled that the PNR agreement with the United States was invalid, but delayed the effective date of its decision until September 30, 2006 in an attempt to resolve the jurisdictional problems beforehand.* To fix the problem, the EU has obtained authority from the Member States to renegotiate the PNR Agreement under the Third Pillar. This Agreement currently requires the EU to notify the United States that it will terminate the current Agreement on September 30, 2006 and has set a goal of establishing a new agreement by this date.

(U//~~FOUO~~) Before 11 September 2001, the U.S. Government knew very little about the people getting on planes bound for the United States. After the attacks, airlines were required to provide information about their U.S.-bound passengers. Some of this information - name, contact information, and the like - was drawn from information supplied to the airline as part of the reservation process. DHS/CBP uses this reservation information, known as PNR data, to screen for no-fly violators and terrorist suspects prior to arrival, and even before the plane departs, protecting against mid-flight hijackings and bombings.

- (U//~~FOUO~~) CBP automatically accesses PNR data from European carriers up to 72 hours in advance of a flight. During this pre-departure period, information is screened against CBP automated systems and risk scores are generated from this data. In some cases, particularly at foreign airports where CBP maintains a presence through the Immigration Advisory Program, coordinated law enforcement action is also planned in advance with local authorities. Analysis continues up to arrival and is further supported by the collection of manifest information.

(U//~~FOUO~~) In May 2004, the United States entered into an agreement with the EU regarding the transmission of PNR data from European air carriers to the USG. The Agreement stipulates that CBP's use of PNR is deemed "adequate" by European standards as long as the USG adheres to numerous detailed prescriptions worked out with EU negotiators (but unilaterally implemented by DHS).

- Restrictions on Information Sharing With Other Agencies: The Agreement states that no other government authority (domestic or foreign) may have direct access to or receive bulk transfers of PNR through CBP databases. As a consequence, DHS is precluded from sharing PNR information for broad analytical purposes or for matters not related to terrorism or serious "transnational" crimes.
- Restrictions on Access to Data Within CBP: Data is available for a short time. Seven days after completion of a travel itinerary, access to PNR data is limited to a small number of officers. Further, CBP is only allowed to store PNR on EU

flights for 3.5 years (11.5 years if it has been accessed manually) unless the data has been linked to an enforcement file. High (b)(2)/(b)(7)(E) LE

- Data Elements The Agreement currently limits CBP's access to 34 data elements, while a carrier's system may include upwards of 50 fields. Other data fields may provide pertinent information. High (b)(2)/(b)(7)(E) LE

Some of these prescriptions are difficult to justify since the adoption of the Intelligence Reform and Terrorism Prevention Act and Executive Order 13388;

b2 High
b7E

- PNR information is the feeder data for CBP's automated threshold targeting system, which uses intelligence-derived information as the basis for developing 'rules' in a risk-based weighting system, using certain characteristics (for example (b)(7)(E) to identify potentially suspicious travelers for additional scrutiny. CBP automatically screens all individuals traveling to the United States through their Automated Targeting System-Passenger (ATS-P). This system will highlight certain individuals as high risk, which will cue CBP inspectors to conduct addition screening of these passengers.
- The PNR data fields include over 30 separate fields, the majority of which are biographic data on individual passengers. High (b)(2)/(b)(7)(E) LE
- CBP intelligence analysts use PNR data to conduct additional research and lead development on individual travelers at the behest of other USG organizations such as the FBI and CIA.
- Due to strict limitations on data sharing of PNR information, only select CBP personnel have access to this information. The EU Agreement specifically

¹ CBP can share PNR data with other law enforcement agencies, but only on a case-by-case basis and only for the purpose of combating terrorism and serious transnational crimes. This restriction prevents PNR information from being shared in bulk with the intelligence and law enforcement community, and it denies those agencies direct access to the records. (b)(7)(E)

b2H

restricts the dissemination of this data to CBP due to EU data protection considerations. Consequently, other DHS components, including I&A were required to make case-by-case requests for PNR information.

b2H

(b) (7)(E)

3. (U//~~FOUO~~) DHS Way Ahead

(b) (5)

b2H
b7E

(b)(5) - Delib

- (U//~~FOUO~~) EU is trying to re-impose data protection limitations on PNR data. If successful, this will be the first time that the EU has extended commercial data protection rules to law enforcement information. The EU's negotiating position is consistent with a larger plan to subject all law enforcement data sharing to enhanced privacy rules.

² This concern is consistent with Executive Order 13388 and the President's Memorandum issued on December 16, 2006 to Heads of Executive Departments and Agencies on "Guidelines and Requirements in Support of Information Sharing Environment."

The Office of Intelligence uses PNR data to research information from the intelligence and law enforcement communities on a daily basis. High (b)(2)/(b)(7)(E) LE

[Redacted]

Some recent examples of PNR successes:

1. (b)(6)/(b)(7)(C)/(b)(7)(E)
[Redacted]

High (b)(2)/(b)(7)(E) LE
[Redacted]

2. (b)(2)/(b)(6)/(b)(7)(C)/(b)(7)(E)
[Redacted]

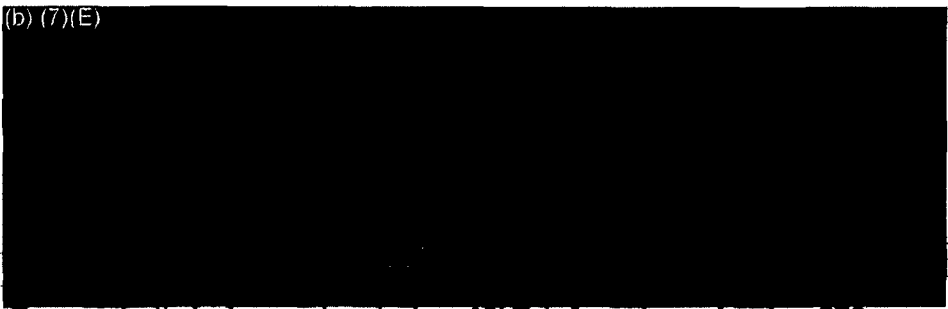
3. High (b)(2)/(b)(7)(E) LE
[Redacted]

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~(U//FOUO)~~ Intelligence Value of PNR Data

b2H

(b) (7)(E)



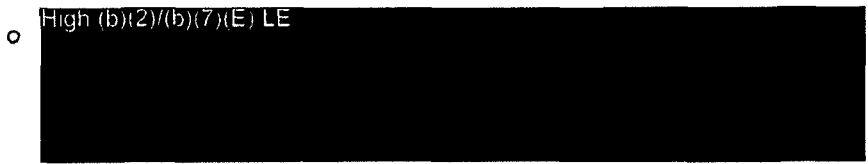
- Due to strict limitations on data sharing of PNR information, only select CBP personnel have access to this information. The EU Agreement specifically restricts the dissemination of this data to CBP due to EU data protection considerations

b5
b2 High
b7E

High (b)(2)/(b)(7)(E) LE



High (b)(2)/(b)(7)(E) LE



b2 High
b7E

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

**Guidelines for Use and Disclosure of Passenger Name Record (PNR) Data
Obtained from Flights between the United States and European Union Countries,
Iceland and Switzerland¹**

**I. Use of PNR Information by U.S. Customs and Border Protection (CBP)
Personnel**

A) Permissible Purposes: CBP personnel who are authorized to access Passenger Name Record (PNR) data through CBP's systems in connection with their official duties, may do so strictly for purposes of preventing and combating:

- 1) terrorism and related crimes;
- 2) other serious crimes that are transnational in nature; and
- 3) flight from warrants or custody for the crimes described in (1) and (2), above.

B) Available Data Elements: CBP's computer system is designed to provide authorized CBP personnel with routine access through its Automated Targeting System-Passenger (ATS-P) to 34 specific data elements that may be available in a PNR related to a flight between the United States and the European Union (EU), Iceland and Switzerland. A list of those specific data elements are shown in Attachment "B." An automated feature within ATS-P has been developed to make only those data elements available to the user for such flights.

- 1) Other Service Information (OSI), Special Service Request (SSI/SSR): Although these fields are part of the 34 available data elements mentioned above, these fields will generally be "blocked" by CBP's system to prevent routine review by authorized users. In the event that an individual is identified as high risk or to be of particular concern, a supervisor may authorize the CBP system to make the OSI and SSI/SSR fields of the subject's PNR available to the reviewing authorized user. High (b)(2)/(b)(7)(E) LE

¹ A list of EU countries is provided in Attachment "A." For information regarding the handling of PNR data obtained in connection with flights between the U.S. and countries outside the EU, Iceland and Switzerland, please consult appropriate directives regarding the use, handling and disclosure of Automated Targeting System (ATS) and Treasury Enforcement Communication Systems (TECS) information, as well as any other authorities of more general application.

- 2) **"Sensitive" Data:** Certain PNR codes and terms which may appear in a PNR have been identified as "sensitive" and are filtered and deleted by CBP's automated system to prevent review by authorized users. A list of the mutually agreed upon "sensitive" codes/terms is contained in Attachment "C." There will be an indicator in the PNR that a term or code has been deleted.

C) **Timing of Access:**

- 1) **Routine Access:** The Automated Targeting System (ATS) will pull PNR data no earlier than 72 hours prior to departure of the flight,

(b) (7)(E)

This will be done to identify any changes in the information. The PNR data from the automated pulls or pushes will be available within ATS-P. Any other pulls or pushes will be considered non-routine.

- 2) **Non-Routine Access:** All pulls of PNR data for flights between the U.S., and the EU, Iceland and Switzerland performed from the ATS Reservation Monitoring System (ResMon) are manual pulls and considered non-routine. If CBP obtains advance information that person(s) of specific concern may be traveling on a flight between the United States and the EU, Iceland or Switzerland, non-routine pulls or pushes of the PNR must be coordinated with the National Targeting Center (NTC). When coordinating with the NTC to verify that this information has not yet been pulled or pushed by any other authorized user, please indicate whether the PNR in question is an EU, Iceland or Switzerland PNR. Then the access to do the manual pull must be authorized by a supervisor, if deemed appropriate and granted by the automated feature. This access will be available to the user at the supervisor's discretion.

High (b)(2)/(b)(7)(E) LE

D) Limitations on Access: Based on the individual's *user role*, certain authorized CBP personnel will have on-line access to PNR through CBP systems for a period of seven days after the last day of travel as indicated in the PNR. Following the first seven days, on-line access to such PNR will be limited to authorized personnel with the pertinent *user role* as indicated in Attachment "D." PNR associated with flights between the United States and the EU, Iceland and Switzerland from the date of the arrangement with each country, respectively, will only be available on-line in CBP's system for three years and six months, unless it is linked to a specific enforcement record.

II. Disclosure of PNR Information by CBP Officers

A) Treatment of Department of Homeland Security (DHS) and Component


Agencies: DHS and its component agencies will be treated as "third agencies" for purposes of transfers of PNR (i.e., such entities will be subject to the same rules and conditions as non-DHS government authorities).

B) Discretionary Disclosures to Other Government Authorities

1) Eligible Authorities: PNR information may be disclosed on a case-by-case basis to the following third parties (based on requests from such Eligible Authority or initiated by CBP):

- a) Disclosure to other government authorities, including foreign government authorities, provided such authority has law enforcement or counter-terrorism functions, and the disclosure is consistent with a purpose identified above in paragraph I(A). Disclosures to such government authorities should only be made if it is determined that:
 - i) the receiving government authority is responsible for preventing, investigating or prosecuting violations of, or enforcing or implementing, a statute or regulations related to the purpose of the request; and
 - ii) CBP is aware of an indication of a violation or potential violation of law.
- b) Disclosure to relevant government authorities, where disclosure of the PNR data is necessary to protect the vital interests of the subject of the PNR or of other persons (for example, in the case of significant health emergencies or epidemics).

2) Disclosure Procedures and Conditions

- a) **Requests from Eligible Authorities:** If an eligible authority (as defined in paragraph II(B)(1)) is requesting information which would include PNR data, a written request from that eligible authority must explain the specific information requested and the reason(s) for the request. This written request may be submitted via e-mail by the requesting eligible authority and must be submitted prior to the disclosure of any PNR information. Only under exigent circumstances may PNR information be disclosed based on a verbal request. If this occurs, a written request must be submitted as soon as possible following the disclosure of the PNR information based on verbal representations.
- b) **Review of Purpose:** Review the request to insure that the purpose for obtaining the data relates to the purposes for which that Eligible Authority is permitted to receive PNR data (see paragraph II(B)(1) above).
- c) **Record of Disclosure:** All disclosures (regardless of the citizenship or residence of the data subject), whether pursuant to the request of an eligible authority, or CBP-initiated to such eligible authority must be recorded in accordance with the following procedures:
- i) A PNR Disclosure Form and CF 191 must be completed to document the release of information. This feature is now automated within ATS-P and can be generated when accessing the PNR or after accessing the PNR. The system will generate the required forms and pre-populate some of the information.
High (b)(2)/(b)(7)(E) LE

- Note:** The procedure described in Section II(B)(2)(c)(i) above for recording disclosures of PNR apply to all disclosures of PNR, including PNRs derived from flights between the U.S. and countries other than the EU, Switzerland, and Iceland. As mentioned above the system will generate the required forms applicable to the PNR that is being disclosed.
- ii) Include with the transfer of the PNR data, the cover letter that will be automatically generated to the eligible authority.
- iii) Each Field Office must develop and implement local procedures to ensure all disclosures of PNR are disclosed according to the current policies and procedures. Paper copies will no longer be

forwarded to the Executive Director, Traveler Security and Facilitation.

- iv) The automated disclosure packet should include: PNR Disclosure Form, CF-191 (for all disclosures), the appropriate cover letter, and the pertinent PNR data disclosed. All written requests for disclosures are to be maintained by the office that disclosed the information for audit purposes.

-
- d) Marking of Transmitted PNR Data: Copies of PNR data (including any portion of any PNR) furnished to an Eligible Authority in accordance with this guidance must contain the following statements:

"Property of U.S. Customs and Border Protection"

"This document is provided to your agency for its official use only and remains the PROPERTY OF U.S. CUSTOMS AND BORDER PROTECTION (CBP).

This document contains confidential personal information of the data subject ("Official Use Only") and confidential commercial information and may not be disclosed to any third party without the express prior written authorization of CBP."


D) Mandatory Disclosures of PNR

- 1) Subpoenas or other legally mandated disclosures (other than under the Freedom of Information Act or Privacy Act): CBP Officers should immediately contact their Associate or Assistant Chief Counsel's Office for guidance in responding. In responding to such demands, reasonable efforts should be taken to protect the confidentiality of such data, as permitted.
- 2) Freedom of Information Act (FOIA) Requests (5 U.S.C. 552)
 - a) Requests by the Data Subject: First party requests for PNR data shall be handled in accordance with the normal CBP procedures for responding to FOIA requests, except that CBP will not assert any exemptions based on the fact that the data is confidential personal information of that data subject (5 U.S.C. 552(b)(6)) or that it is confidential commercial information of the air carrier (5 U.S.C. 552(b)(4)).

- b) Requests by Persons Other than the Data Subject: Third party requests for PNR data shall be handled in accordance with normal CBP FOIA procedures. CBP officials shall generally treat such PNR data as confidential personal information of the data subject and confidential commercial information of the air carrier (5 U.S.C. 552(b)(4), (6)).

3) Privacy Act Requests (5 U.S.C. 552a): First party requests for information pursuant to the Privacy Act shall be handled in accordance with normal established procedures.

III. Correction of PNR Data:

- A) If a request by a passenger is made in the field with respect to the disclosure or correction of a PNR, the Field Officer will follow the normal established procedures for FOIA requests or amendment of TECS records, as applicable.
- B) If designated personnel from the National Targeting and Security office determine that information contained in a PNR is inaccurate (whether independently identified by CBP or upon the request of the data subject or his legal representative (e.g., EU Data Protection Authority), a note will be linked to the PNR record within ATS-P to document that the data was determined to be inaccurate and will include the correct information. High (b)(2)/(b)(7)(E) LE
- 

Attachment "A"

List of European Union (EU) Countries (as of 11/17/05):

Austria
Belgium
Cyprus
Czech Republic
Denmark
Estonia
Finland
France
Germany
Greece
Hungary
Ireland
Italy
Latvia
Lithuania
Luxembourg
Malta
Poland
Portugal
Slovakia
Slovenia
Spain
Sweden
The Netherlands
United Kingdom

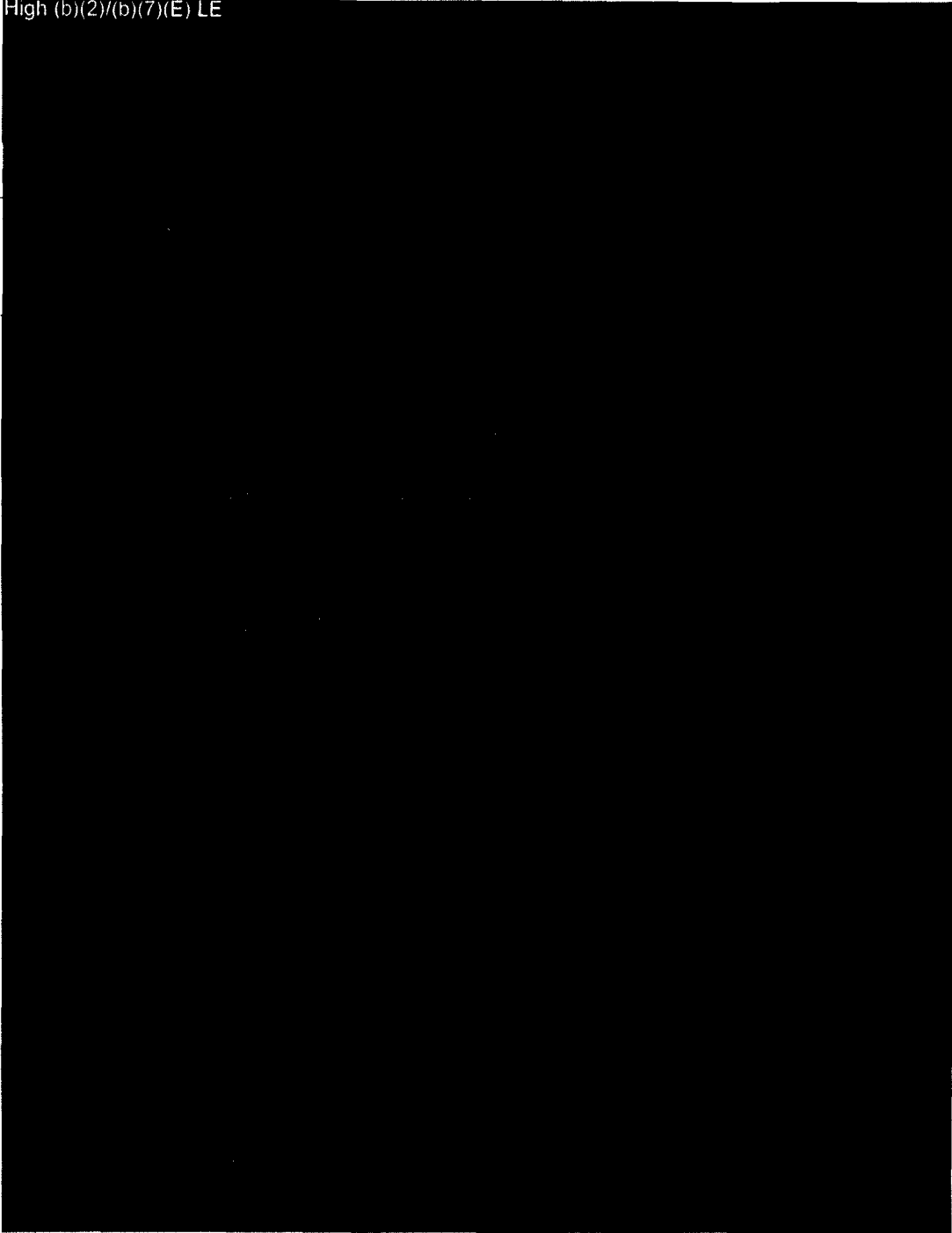
Attachment "B"

**List of PNR Data Elements CBP May Access in Connection with
Flights between the United States and the European Union Countries,
Iceland and Switzerland**


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

Attachment "C"

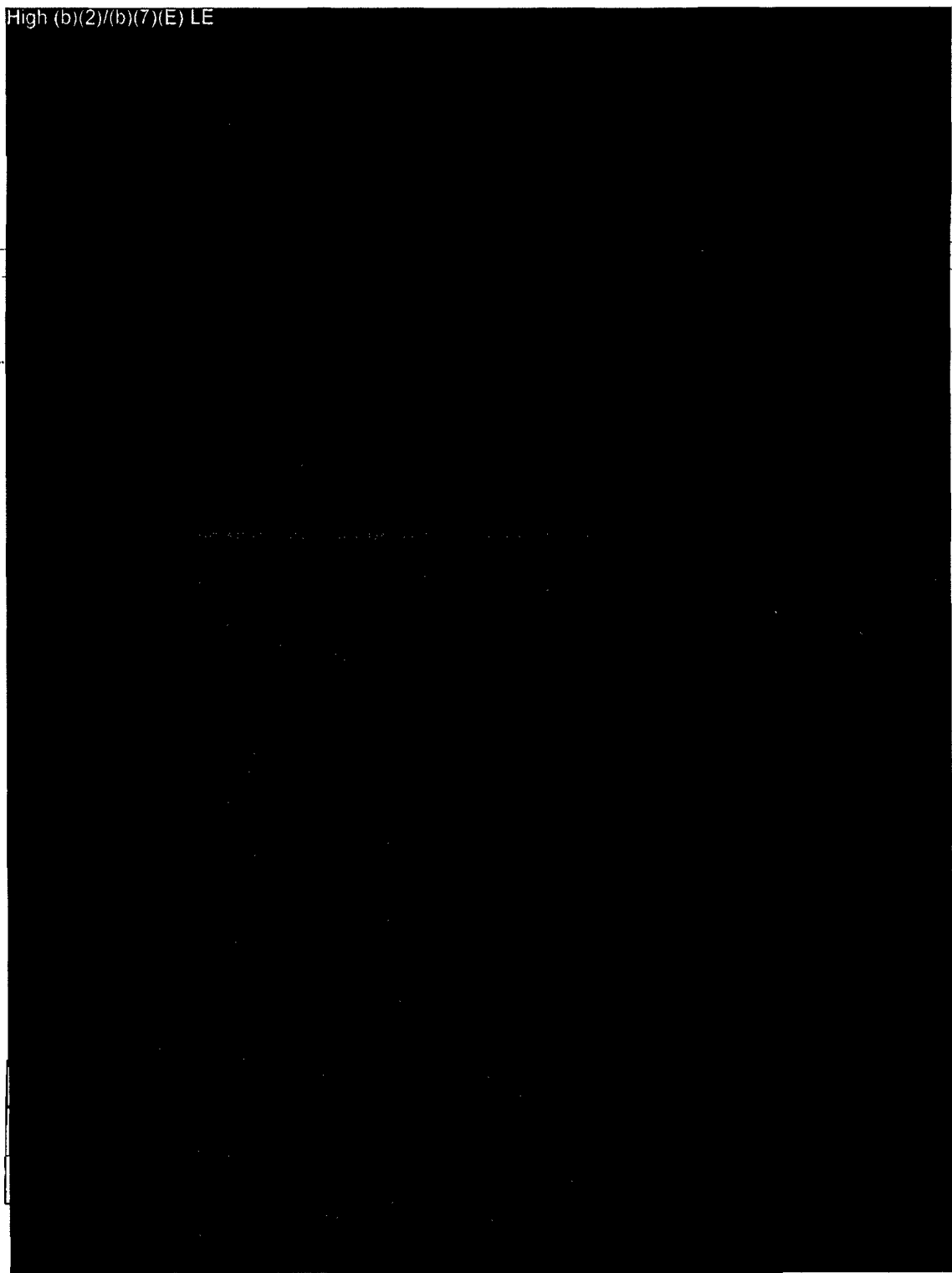
High (b)(2)/(b)(7)(E) LE



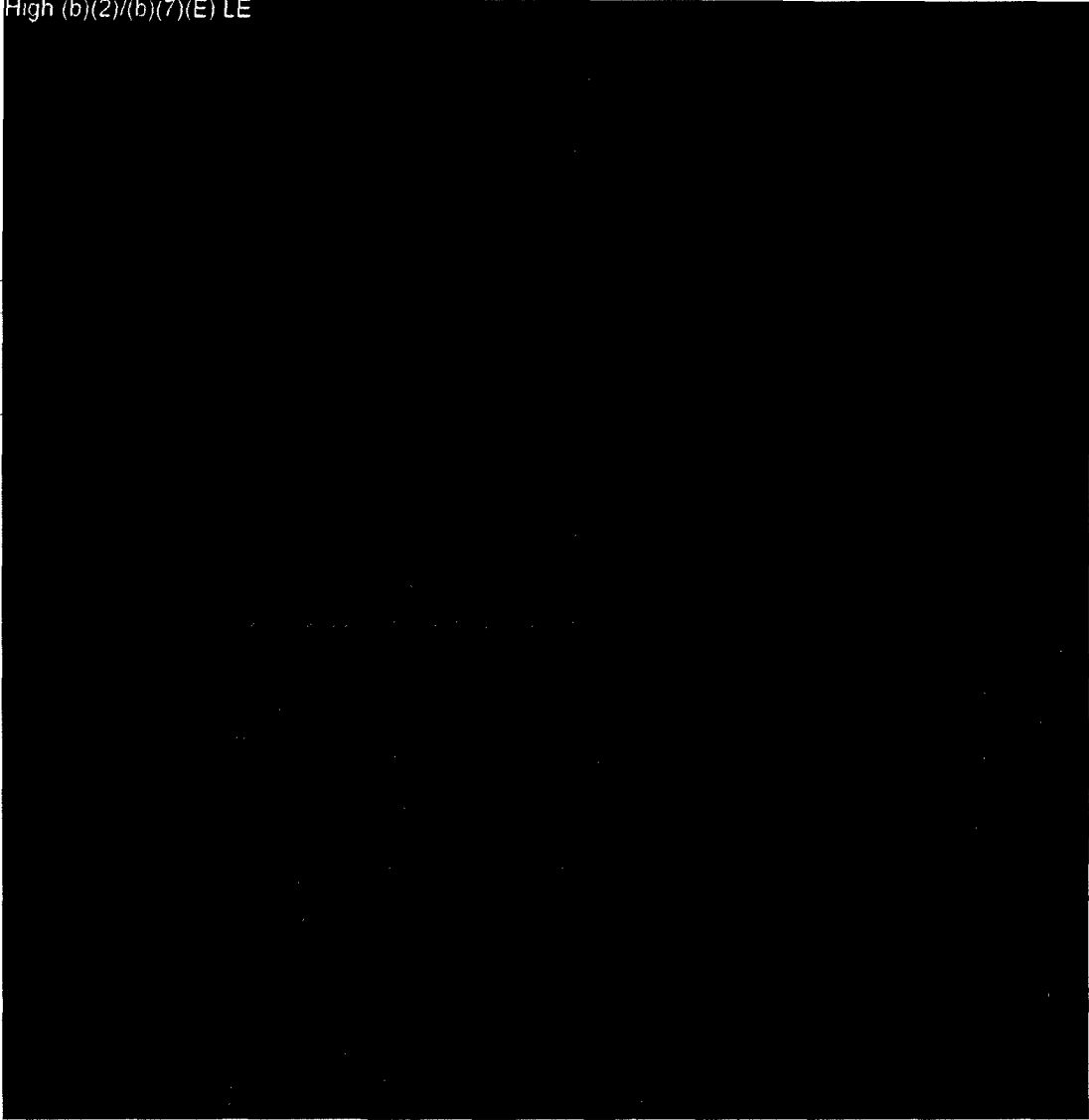
High (b)(2)/(b)(7)(E) LE



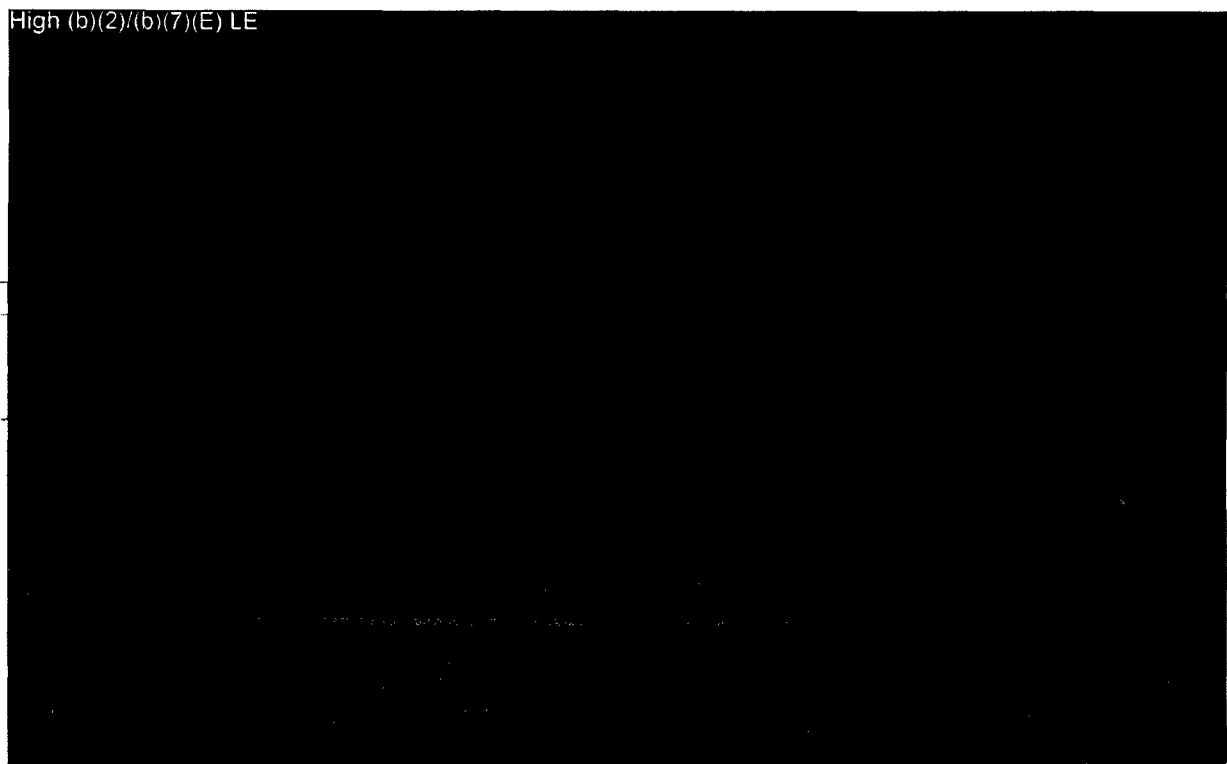
High (b)(2)/(b)(7)(E) LE



High (b)(2)/(b)(7)(E) LE



High (b)(2)/(b)(7)(E) LE



~~FOR OFFICIAL USE ONLY~~

ATTACHMENT A: STATUS OF INTERNAL PNR SHARING

- CBP has been sharing PNR information with certain DHS entities under the interim EU agreement since December 2006. [b2 High b7E]
- These components were the first to receive PNR data because they are deemed "DHS entities" for purposes of the revised Undertakings.
- [b2 High b7E] They also have been trained in its proper use, and have been instructed that any misuse will subject them to discipline.
- [b2 High b7E]
- Initially, PNR sharing at DHS has been accomplished through a series of letters between CBP and the other components. Those interim letters will be superseded by a DHS-wide management directive, which currently is in the final stages of development.
- In the interim letters, the components indicate that they will comply with the terms of the PNR Undertakings, ensure that personnel follow CBP's policies on PNR use and disclosure, and discipline those who do not.
- The management directive also will make PNR data available to other Department components [b2 High b7E] It has been necessary to apply special use and disclosure rules to these components, because they are not deemed to be "DHS entities" under the interim agreement.
- In particular, the Undertakings only permit "non-DHS entities" like TSA to access PNR information through "facilitated disclosure" (not via "direct access"). And the Undertakings limit their use of PNR to investigations of terrorism; they may not use PNR to combat "serious transnational crimes."

~~FOR OFFICIAL USE ONLY~~

(16)

Proposed Federal Register Notice to Announce Interim Arrangement

DEPARTMENT OF HOMESLAND SECURITY

**Interim Agreement Between the European Union and the United States Regarding
the Transfer of Passenger Name Record Data**

AGENCY: [b5]

ACTION: General Notice

On July 9, 2004, [b5] Customs and Border
Protection (CBP), had issued a document on May 11, 2004 (referred to as the
"Undertakings") containing [b5] representations regarding the manner in which CBP
would handle certain Passenger Name Record (PNR) data relating to flights between the
United States and EU member states.

[b5]

[b5]

[insert text of interim agreement]

RP 03-29
ADM-9-03-RR:RD:BS
914892 bc

**DEPARTMENT OF HOMELAND SECURITY
BUREAU OF CUSTOMS AND BORDER PROTECTION**

RIN 1651-XXXX

**Interim Agreement Between the European Union and the United States Regarding
the Transfer of Passenger Name Record Data**

AGENCY: Bureau of Customs and Border Protection; DHS.

ACTION: General Notice.

SUMMARY: This Notice is intended to update a General Notice published in the Federal Register (69 FR 41543), advising that the Department of Homeland Security (DHS), Customs and Border Protection (CBP), had issued a document on May 11, 2004 (referred to as the "Undertakings") containing [b5] representations regarding the manner in which [b5] would handle certain Passenger Name Record (PNR) data relating to flights between the United States and European Union (EU) member states. This Notice describes updates and adjustments to the Undertakings to reflect changes in the law and circumstances surrounding these data transfers.

EFFECTIVE DATES: This Notice is effective [Insert date of publication in the FEDERAL REGISTER].

FOR FURTHER INFORMATION CONTACT: [b6 b2]

SUPPLEMENTARY INFORMATION:

Background

On July 9, 2004, a [b5]

[b6] Customs and Border

Protection (CBP), had issued a document on May 11, 2004 (referred to as the

"Undertakings") containing [b5] representations regarding the manner in which CBP would handle certain Passenger Name Record (PNR) data relating to flights between the

United States and European Union (EU) member states. [b5]

10

these Undertakings were understood to provide the foundation (b) (5)

to enter into an agreement with the United States that permitted the transfer of PNR data to CBP consistent with applicable EC law. (b) (5)

as a consequence of the determination of the European Court of Justice that the agreement had been concluded on an inapplicable basis under European Union law.

On October 19, 2006, the United States and the EU concluded an agreement to last until July 31, 2007. This agreement was accompanied by a letter of the United States updating (b) (5) the Undertakings to reflect changes in the law and circumstances surrounding this data transfer. The letter was discussed extensively with the EU, and the EU has acknowledged it without objection. Copies of the agreement and letter are (b) (5) All representations contained in the Undertakings, as published (b) (5) are to be interpreted consistent with the October 19, 2006 agreement and its accompanying letter, (b) (5)

Both the agreement and the Undertakings shall terminate on July 31, 2007, unless extended.

- [b5] has a legal and moral obligation to protect its borders, as ^{b5} ✓ as a right to verify who it is admitting into the country. This department < b5 >

< b5 >

Deleted: b5

- 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.

Deleted: b5

- < b5 > 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.

Deleted: b5

Deleted: b5

- *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.*

Deleted: b5

Deleted: b5

- We look forward to finalizing < b5 > on this issue with our European allies, with whom we have a great relationship.

Deleted: b5

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 C 65 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 C 65 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 severe penalties for misuses.

Deleted: _____
Deleted: _____
Deleted: _____
Deleted: _____
Deleted: _____
Deleted: _____
Deleted: _____
Deleted: _____

} b5

Deleted: 65

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]

Deleted: b5

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.

Deleted: 1
Deleted: b5
Deleted: b5

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.

Deleted:
Deleted: b5
Deleted:
Deleted:

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 authorised agents for each journey booked on or behalf of any passenger. The data is used by operators for their own (b) (5) 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. (b) (5)

The European Court of Justice ruled that the (b) (5)

TALKING POINTS

- Secretary Chertoff has (b) (5) initialed (b) (5)
- (b) (5) counter-terrorism information collected by the Department will be shared, as necessary with other federal agencies.
- (b) (5)
- The (b) (5) agreement has now been returned to the European Union for its final review and consideration.
- (b) (5) the appropriate security information will (b) (5) be exchanged. Planes will continue to fly uninterrupted and our national security will not be impeded.

- [b5] has a legal and moral obligation to protect its borders, as [b5] has a right to verify who it is admitting into the country. This department [b5] will use every legal authority at our disposal, including valuable PNR data, to secure [b5]
- 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. [b5]
- [b5] Here in the United States and in Europe, we all have to be smart and thorough in scrutinizing people seeking to [b5] including those who may not be on watchlists but could mean to do us harm.
- This is really [b5] 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 [b5] 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 [b5] on this issue with our European allies, with whom we have a great relationship [b5]

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. 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 store the info 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: With there be further negotiations?

A: We look forward to finalizing **(b)(5)** with our European allies, with whom we have a great relationship **(b)(5)**

Q: (b)(5)

A: We have agreed to work towards a "push" system, which is **(b)(5)**
(b)(5) This would mean that air carriers are feeding us info **(b)(5)**

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 **(b)(5)** 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: **(b)(5)** 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.

[b5] found [b5] CBP [b5] in full compliance with representations made in the PNR agreement. CBP has invested substantial time, capital, and expertise to bring its operations and procedures into compliance. This is a recognizable achievement, [b5]

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: [b5]

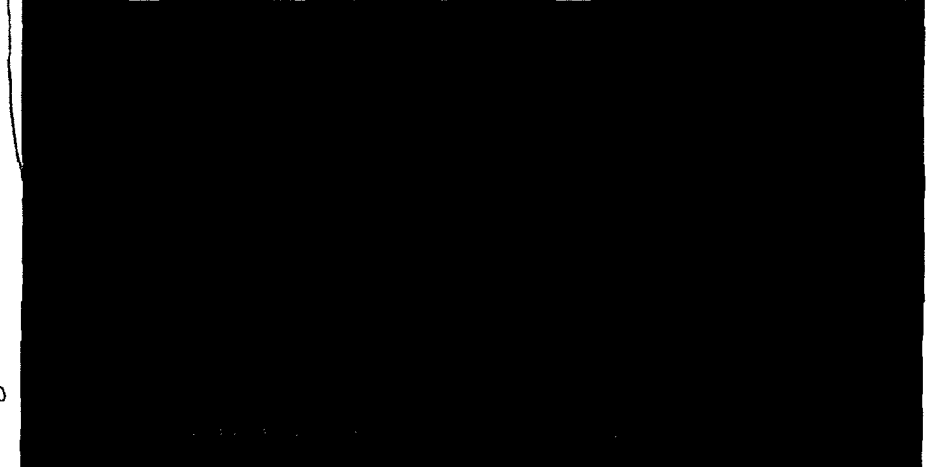
APIS is merely an automated vehicle for the collection of information from government-issued identity documents accepted for international travel. Essentially, APIS is the same as a border officer swiping or visually examining a passport presented by a traveler. The Pre-departure APIS NPRM does not contain any PNR related requirements. Thus, this rulemaking is not affected by the EU's recent PNR ruling.

Update on Implementation of the October 2007 Interim PNR Agreement

P 12

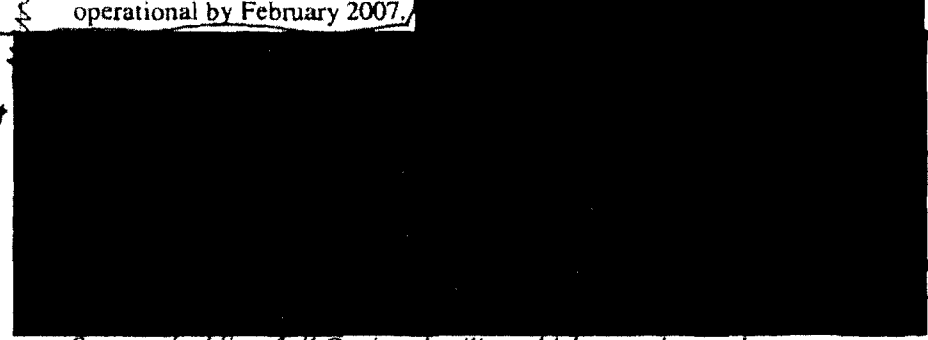
1. Migration to Push:

a. Within the last two weeks Amadeus has provided a limited set of British Airways data for testing. The CBP Office of Information Technology is currently testing this download for compatibility with CBP formatting.



High (b)(2)
(b)(7)(E)
(b)(5) - Delta

e. Delays on the part of Amadeus and its clients have yet again pushed back the timetable for implementation. After the conclusion of the Interim Agreement, CBP was optimistic that it willing carriers could be operational by February 2007.



high
(b)(2), (b)(7)(E)
b(6)
b(5)

g. See attached list of all Carriers detailing which are using push.

2. PNR Sharing with Other Agencies:

a. DHS has completed a policy on access for DHS agencies other than CBP that fall within the agreements definition of DHS. The policy requires these offices and agencies to accept all CBP regulations on access to and use of ATS-P and PNR, including those tied to the Undertakings and the Agreement. Each agency head must confirm their intent to implement these rules in writing and under their signature.

Michael Scardaville, PLCY/OIA

21

-
-
- b. To date, access has been extended to Immigration and Customs Enforcement (ICE) and Intelligence and Analysis (I&A). Authorized persons in these offices (as vetted by their home agency and CBP) have active accounts and are using the system.

(b)(3)(E)
high b(2)



PNR Questions from Mike Scardaville

Question one: Whether or not CBP has abandoned any plans for the use of PNR due to the limitations in the undertakings (i.e. screening for other offenses).

Answer: No

Question two: Statistics on requests by other agencies for information that may include PNR and the number of times PNR had to be denied to requesting agencies because they did not meet the requirements of the US-EU PNR arrangement. On this later request, we'd like to cast a wide net, including any statistics from the field.

Answer: The answer to the first part of the above question was sent to Mike Scardaville previously and has been copied in below:

b2H
b7E

[REDACTED]

CBP denied this request as a result of the U.S.-EU PNR international agreement.

b2H
b7E

[REDACTED]

[REDACTED]

These requests were denied as a result of the U.S.-EU PNR international agreement.

↑
b2H
b7E

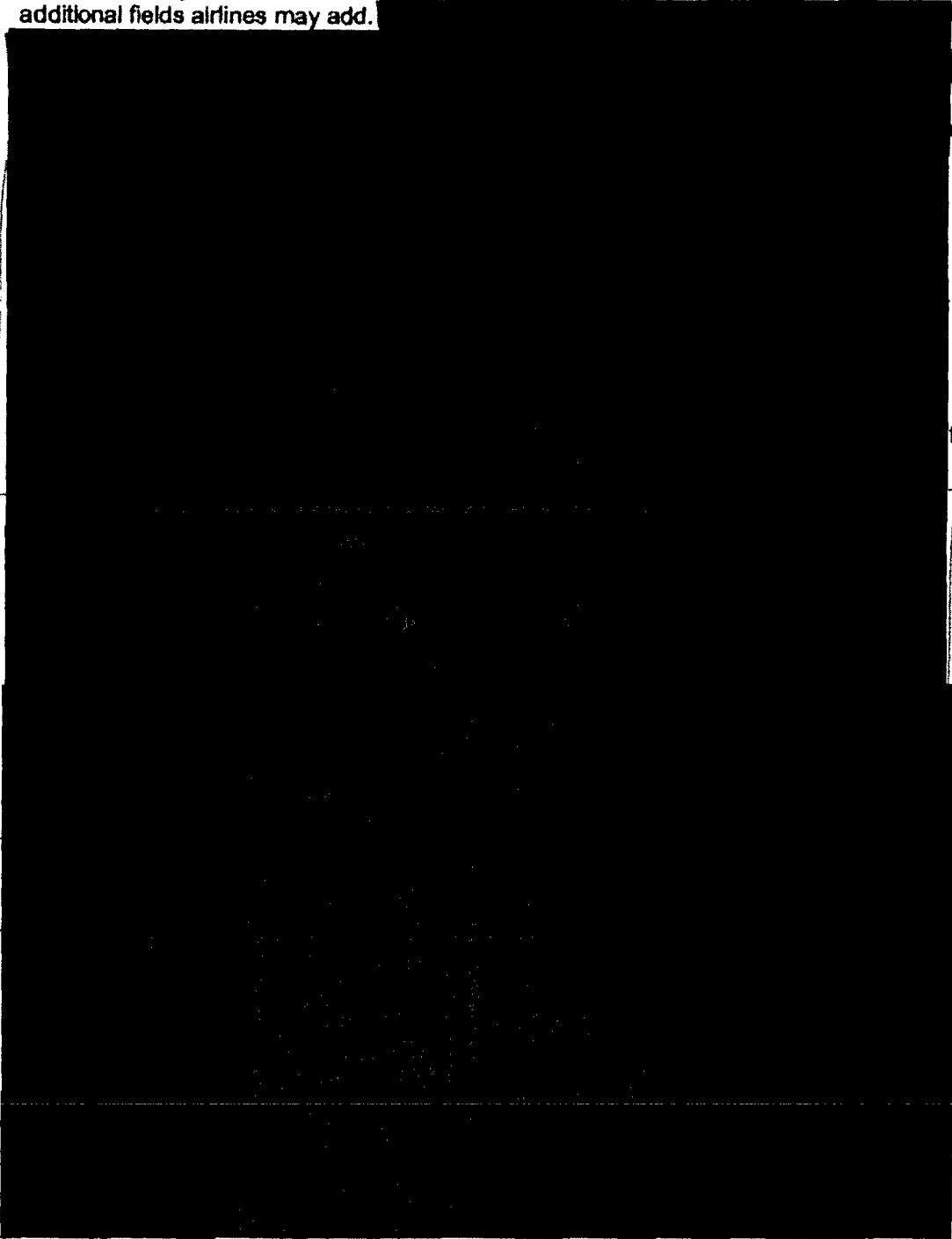
[REDACTED]

b2H
b7E

[REDACTED]

Additionally, all ATS access requests are passed through CBP Headquarters personnel and are granted by CBP Headquarters (i.e., CBP field components cannot grant access to these systems).

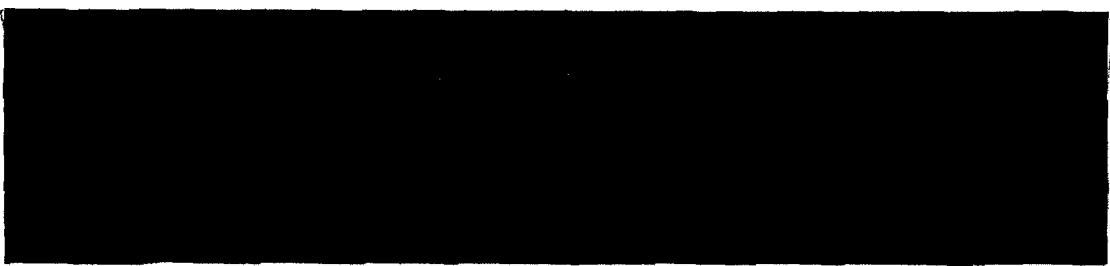
CBP is currently limited to 34 data elements and is required to renegotiate to get any additional fields airlines may add.



b2H
b7E

(b) (7) (C)
(b) (7) (D)

(b)(3)
(b)(7)(D)
(b)(7)(E)



b5
b2H
b7E

-
-
-
- PNR is primarily used by U.S. Customs and Border Protection to screen all passengers flying between the United States and a foreign place to identify persons who pose a high risk for terrorism and serious crimes.

[REDACTED]

high (6/12)
(b)(7)(E)

- CBP accesses PNR from most air carriers by a method generically described as "pull." That is, CBP's automated systems retrieve PNR from the air carrier's reservation systems through an established link. This method of accessing PNR grew out of the original voluntary program during which this was determined by most air carriers to be the easiest and most cost-effective way to make it available to CBP.
- For the last few years CBP has been working with air carriers to develop a system in which they will transmit or "push" this data to CBP and presently 15 carriers are utilizing this method. As part of our new interim agreement with the EU, the United States has agreed to move expeditiously to bring more carriers on line with this push system.

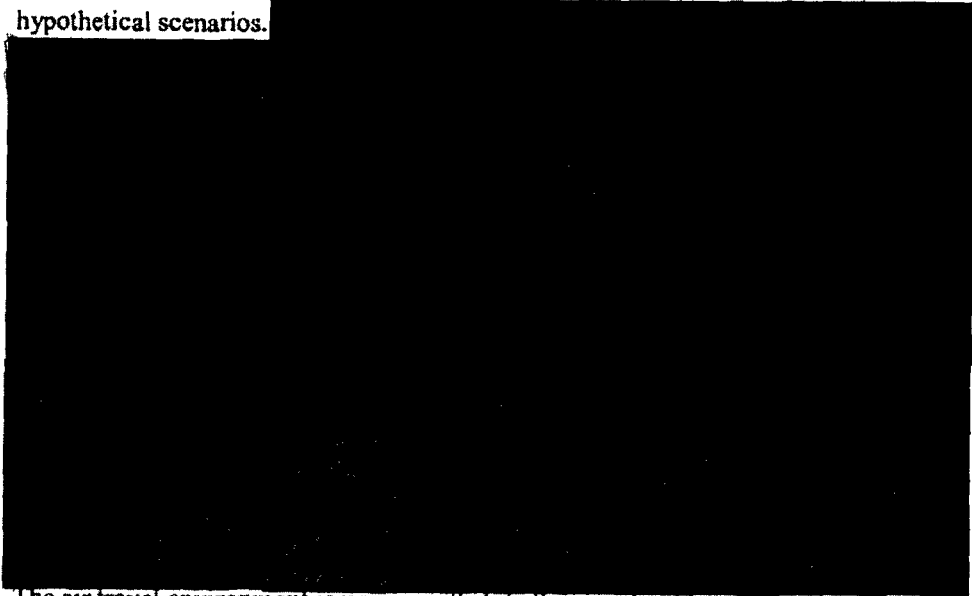
- A properly constructed push system is actually a more robust system. Not only does it more effectively meet some European views on privacy, but when data is transmitted in real time it ensures that CBP officers will always have the most up-to-date information available.
- However, we recognize that some carriers may not be willing to invest in a system that supports a real-time push. In such cases, however, carriers must agree to a scheduled push with the initial push no later than 72 hours before a flight and be able to provide an unscheduled push upon request 24-7.

➤ [REDACTED]

b5
b2H
b7E

- PNR also allows us to look for suspected patterns of activity. It's important to note that when I say we are looking for patterns we are not profiling people based on the meal preferences, the number of beds in their hotel room, their religion, or

hypothetical scenarios.



- The air travel environment is unique in that it allows us to obtain such information in advance. However, many of the same systems are used to analyze travelers at the land and sea borders. In fact, roughly the same analytical systems are used, however advance information is collected through participation in voluntary, registered traveler programs such as FAST, NEXIS and SENTRI with the bulk of data collected at the actual point-of-entry.
- As you know, DHS recently concluded a new agreement with the European Union on CBP's collection and use of PNR. Throughout the negotiations on this agreement both sides agreed on the imperative to support screening and investigations. The main improvement in the 2006 agreement was the establishment of a facilitated interpretation of the information sharing provisions of the 2004 Agreement.
- Of course, the 2006 Agreement is a short-term instrument that provides us with more time to fully explore the lessons learned in combating terrorism and transnational crime over the last 5 years and develop a more constructive and flexible arrangement next year that will protect privacy while ensuring that law enforcement can better coordinate its investigations.

In DHS's long term vision for PNR we would also like to change the government-to-industry dynamic. Over the last 3 years the transportation industry has been caught in the middle of a philosophical debate between the United States and Europe with little commercial value but potentially great impact. You risked fines or the disruption of services imposed by one side if you listened to the directions of the other. Part of our goal moving forward is to change this dynamic and help industry become part of the answer.

- A significant way this can be done is by providing notice to your passengers that the personal data they provide in booking this trip may be

provided to government authorities for the purposes of combating terrorism and transnational crime and perhaps seeking their consent prior to booking.

- Notice and consent are foundational legal concepts in all developed privacy regimes. By providing notice in advance, perhaps through a revision to the contract of carriage, we can give people a choice, advance privacy interests and promote uniformity instead of regionalism.
 - We recognize that this may require adjustments to current and planned business processes and will look to you for advice on how such a regime could work with minimal economic impact.
-
-
-
-
-

FOR OFFICIAL USE ONLY

Passenger Name Records

Talking Points:

- Emphasize the criticality of PNR data for efficient border screening, particularly for passengers from VWP countries. (Only if necessary: remind the listener of the legal basis under U.S. (ATSA) and International (Chicago Convention) law).
- PNR is primarily used by U.S. Customs and Border Protection to screen all passengers flying between the United States and a foreign place to identify persons who pose a high risk for terrorism and serious crimes. The diversity of data in a PNR allows for analysis to identify possible ties to suspected terrorist or other criminal activity.

- [b7E
b2 High]

- PNR data is particularly valuable as a counter-terrorism tool because it provides us with information not available on the manifest that allows us to make connections between known threats and associates who we have not previously been identified as associated with terrorist activity. It allows us to look for suspected patterns of activity. It's important to note that when I say we are looking for patterns we are not profiling people based on the meal preferences, the number of beds in their hotel room, the religion etc. However, at times investigations show a pattern of activity that can help us identify guilty parties. For example that airline ticket counter agents are adding bags filled with illicit material such as drugs or weapons to an innocent traveler's reservation and coconspirators are removing these extra bags as they are unloaded from the plane.
- In our efforts to combat terrorism, drugs, human smuggling and sex tourism, for example, we have frequently been able to identify other cohorts of known criminals on the same or other flights, supporting numerous arrests. CBP is the primary user of PNR data, although DHS's border investigative arm, Immigration and Customs Enforcement has more limited but equally powerful experience with using the data.

PNR Success Stories

Aviation & Border Security

➤ On [] a suspect [] identified as traveling from [] to [] via [] Upon pulling his PNR, []

b2 High
b7E

FOR OFFICIAL USE ONLY

Drafted by: Michael Scardaville, Deputy Director of European and Multilateral Affairs, PLCY/OIA

Contact: [] b2

(24)

FOR OFFICIAL USE ONLY

another traveler was identified as traveling on the same reservation. DHS had no previous derogatory records on the second passenger. The [] was removed from the United States and second subject was allowed to withdraw his application for admission. Similar cases have been found from [] and []

➤ A series of PNR's generated by [] in March 2005 identified linkages

[]

b2
b7E

➤ On [] CBP used PNR to identify linkages between an [] on the No-Fly list and a traveler []

➤ On March 11, 2005 CBP arrested two individuals for smuggling drugs from London to Chicago. Upon analyzing their PNR the use of a common credit card was found. Further analysis of this credit card's reservation history found a 3rd traveler had used the same card and listed a second credit card. Analysis of this new credit card number identified 3 additional travelers. 3 of the 4 new travelers were arrested during subsequent travel with drugs.

➤ On [] CBP analysis of PNR for a flight from [] to Chicago identified 3 passengers that may have been seeking to use fraudulent travel documents. CBP alerted the air carrier who performed a thorough review of all three travelers documents prior to boarding. One was denied boarding by the airline. The two remaining travelers were referred to CBP secondary upon arrival in the United States. Both subjects were determined to be part of a human smuggling organization and they were smuggling the first subject. Additionally, one subject was identified as a member of the Yazuka crime syndicate.

b2 High
b7E

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

➤ CBP has used PNR to identify practices adopted by users of fraudulent documents to identify the operation of a human smuggling ring in Costa Rica. []

b2 High b7E

Transnational Crimes

➤ ICE used Dominican PNR to identify and dismantle a human smuggling ring between the Dominican Republic and the United States. In this case 7 women were traveling to the United

FOR OFFICIAL USE ONLY

Drafted by: Michael Scardaville, Deputy Director of European and Multilateral Affairs, PLCY/OIA

Contact: [] b2 []

FOR OFFICIAL USE ONLY

States with children other than their own under their own children's passports. Through an analysis of the first suspects PNR a pattern in which the children constantly did not make the return flight was identified. By looking for this pattern, DHS identified the remaining 6 smugglers. Once the suspects were identified, lookouts were placed in APIS for pending arrivals. Ultimately this case resulted in the arrests of seven alien smugglers and one previously deported adult alien, ten expedited removals, the disruption of an organization responsible for successfully smuggling thirty-seven individuals, and the increased awareness by CBP officers of a simple and highly effective alien smuggling technique.

- Upon identifying a suspected sexual predators intent to travel to Bangkok, ICE was able to identify two travel agencies specializing in sex tourism and a number of other predators traveling to Asia for the same purpose. Through this ongoing case ICE has identified reservation patterns employed by sex tourism companies, including diversification of flight reservations culminating in a central location. It also facilitated ICE's ability to marshal surveillance resources by monitor the individual's movements.
- ICE has also used PNR to identify coconspirators of individuals on a watchlist. Through APIS data CBP identified a suspected Venezuelan heroin smuggler due to arrive in the United States. By analyzing PNR, a second individual was found to be traveling on the same reservation and was also arrested with drugs.
- ICE was also able to use PNR to support the early identification of a money launderer for the Hells Angels Motorcycle Gang. Investigatory intelligence indicated that this individual was due to make a brief stop in New York City while traveling between the Caribbean and Canada. PNR was able to allow ICE to identify, in advance, the airport he would be arriving into, arrange for him to be followed to a criminal meeting and be arrested. If ICE had been limited to APIS data in this case it is likely that they would not have had enough lead time to make the arrest.
- ICE has also used PNR to reinvigorate a variety of cases in which critical evidence was tied to telephone numbers with fictitious subscriber data. Since criminals used these phone numbers in making travel reservations, ICE was able to identify valid leads as well as to clear individuals who's names were used unbeknownst to them in phone service provider records.

Watch Out For/If Asked:**FOR OFFICIAL USE ONLY**

Drafted by: Michael Scardaville, Deputy Director of European and Multilateral Affairs,
PLCY/OIA

Contact: [b 2]

FOR OFFICIAL USE ONLY

Page 2

Background:

Passenger Name Record is a generic name for that information that may be collected from each passenger by travel agents and airlines and stored in their record systems for the purpose of managing a flight. While the records held by each carrier can vary dramatically, it typically includes information such as name, contact information, payment method, information about a traveler's baggage. PNR differs significantly from Advance Passenger Information System (APIS) data, which is developed from the carriers manifest and is largely derived from the information on the traveler's passport. APIS data is confirmed biographic data while PNR includes preliminary biographic information and other transactional data elements by which a person or activity may be identified.

The former U.S. Customs Service (now, U.S. Customs and Border Protection) began using PNR from air carriers on a voluntary basis in 1996, initially in an effort to facilitate the clearing of low risk travelers – a function it still serves today. However, after the terrorist attack on September 11, 2001, Congress required the U.S. Customs Service to mandate access to PNR data to support its border security screening, particularly to identify persons who may constitute a high risk for terrorism. [**Background note:** 1996 is the first year Customs began collecting PNR data in an automated system. In 1992 we Customs worked with the airlines to screen PNR data via their computer systems located in the airline's offices at each airport.]

Consistent with the Aviation and Transportation Security Act of 2001, each air carrier operating passenger flights in foreign air transportation to or from the United States must provide the Department of Homeland Security (DHS) Bureau of Customs and Border Protection (CBP) with electronic access to passenger name record (PNR) data to the extent it is collected and contained in the air carrier's automated reservation/departure control systems ("reservation systems"). In 2002, the EU raised concerns that the statutory requirement conflicted with Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("European Data Protection Directive"). Most significantly, the European Data Protection Directive places burdens on private sector data controllers that limits their ability to share personal data across international borders with non-EU countries absent a demonstration that the receiving entity in a third country has adequate data protection standards.

In 2004, the United States government reached an arrangement with the European Commission (EC) which permitted airlines to legally provide access to passenger name record (PNR) data emanating from within the European Union (EU) to CBP. This access is subject to carefully negotiated limitations as set forth in a set of Undertakings issued by CBP offering detailed assurances on how the DHS component would collect, process, handle, protect, share and ensure oversight of PNR data received in connection with flights between the U.S. and EU. Compliance

FOR OFFICIAL USE ONLY

Drafted by: Michael Scardaville, Deputy Director of European and Multilateral Affairs,
PLCY/OIA

Contact: [

b 2

]

FOR OFFICIAL USE ONLY

with the Undertakings required significant system, policy and operational modifications by CBP and was accomplished on May 13, 2005.

The PNR Case. Shortly after the 2004 signing of the European Union agreement on CBP access to Passenger Name Record data, the European Parliament (EP), disturbed over what it viewed as an attack on personal privacy and its own authority, filed two suits in the European Court of Justice (ECJ) against the actions of the European Commission (EC) and the European Council for entering into the information sharing arrangement. The first suit challenged the authority of the EC and the European Council to enter into the International Agreement without the assent of the Parliament; the second challenged the merits of the arrangement itself—whether the Undertakings were adequate to meet the information privacy protections afforded under EU law to all individuals.

On May 30, 2006 the European Court of Justice (ECJ) annulled the decision of adequacy made by the European Commission, as well as the European Council's decision to enter into an international agreement with DHS on the use of Passenger Name Records. In issuing this finding, 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, consistent with the Advocate General's November 2005 opinion, the court found that the decisions of the Commission and Council were premised upon an inapplicable legal basis under European law. Instead of concluding the agreement under the data protection provisions of Article 95, the court deemed that the processing of PNR data is a law enforcement and public security issue, and as a result, is a shared competency between the European Union and Member States under the so called "third pillar."

The Court's ruling gave the European Commission until September 30, 2006 to establish a new community-wide arrangement to govern PNR access for flights to the United States. However, since the ECJ's decision removes the threat of fines and criminal penalties based on EU law, the immediate consequences for not striking a new arrangement are significantly diminished.

The Interim Agreement:

On October 19, 2006, the United States signed an interim agreement (already signed by the European Union) on the processing and transfer of passenger name record (PNR) data. This agreement was accompanied by a unilateral letter of interpretation of U.S. obligations with regard to such data that was negotiated by the parties and acknowledged by the EU. This new arrangement - which will expire on July 31, 2007 enables DHS to share information in ways that were not possible under the previous interpretation of the May 11, 2004 Undertakings, which formed the basis of the earlier U.S.-EU arrangement. It also codifies certain assumptions associated with the Undertakings including: carriers obligations in migrating to a system in which they transmit data to CBP, that a joint review is not necessary between the signing and the expiration of the agreement, access to additional data in the frequent flier field, and the use of sensitive information to protect the vital interests of the data subject. Nonetheless the agreement

FOR OFFICIAL USE ONLY

Drafted by: Michael Scardaville, Deputy Director of European and Multilateral Affairs,
PLCY/OIA

Contact: C

b2

2

FOR OFFICIAL USE ONLY

retains many of the deficiencies of the original 2004 agreement, including an overly short retention period, a facilitated but still disjointed regime for sharing PNR within the USG and does not allow for passenger participation through notice and consent. In addition, the detailed nature of the agreement, which is premised on EU oversight of DHS activities, limits the ability of the United States Government to adapt to changing requirements in combatin terrorism and crime. DHS is in the process of discussing potential replacements with the EU with a goal of concluding such talks before July 31, 2007.

Prescreening Systems of Other Governments:

Presently most nations do not collect PNR in order to prescreen travelers. Canada, however, does collect PNR and has an agreement with the EU similar to the 2004 U.S.-EU Agreement. In fact, the EU typically holds their agreement with Canada up as more of a model than their agreement with the United States. In addition, Canada shares PNR with the United States pursuant to the Shared Border Accord. Rumors persist that a number of European governments are pursuing PNR systems including the U.K., France, Spain, Italy and the EU but few details have been made available.

The use of APIS and Advance Passenger Processing (APP) data is more common. All 4CC member countries collect APIS or APP data in order to prescreen travelers. The United States has cooperative arrangements with Canada and Mexico to share this type of information.

FOR OFFICIAL USE ONLY

Drafted by: Michael Scardaville, Deputy Director of European and Multilateral Affairs,
PLCY/OIA

Contact: [

b2

]

Passenger Name Records and Other Issues

October 16, 2006

~~For Official Use Only~~

(52)

Outline for Brief

- PNR v. APIS
 - DHS uses
 - Possible Other Uses
- Key Points of New Agreement
- Follow on US-EU Negotiations
- PNR and Other Countries
- Other NSA-related Issues

~~For Official Use Only~~

APIS

- Manifest data:
 - Name
 - Passport
 - Nationality
- Collected by airlines and transmitted through AQQ NLT 15 min before pushback
- Checked against TSC lists
 - No Fly
 - Selectees

~~For Official Use Only~~

PNR Data fields

- 62 Data fields

High (b)(2)/(b)(7)(E) LE



- Collected since 1992
 - Originates with airlines and/or travel agents
 - Transmitted up to 72 hours before takeoff
 - Migrating from “pull” to “push” system
- Can be used for link and pattern analysis

For Official Use Only



Link Analysis Examples

High (b)(2)/(b)(7)(E) LE



For Office ~~Use~~ Only

New Agreement – Expanded Use

- Old Agreement from 2004
 - Limited to “case by case” analysis
 - Predication required
- New Agreement
 - “Case by case” expanded to include [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

high 62
67E

~~For Official Use Only~~

New Agreement – Limitations and Authorizations

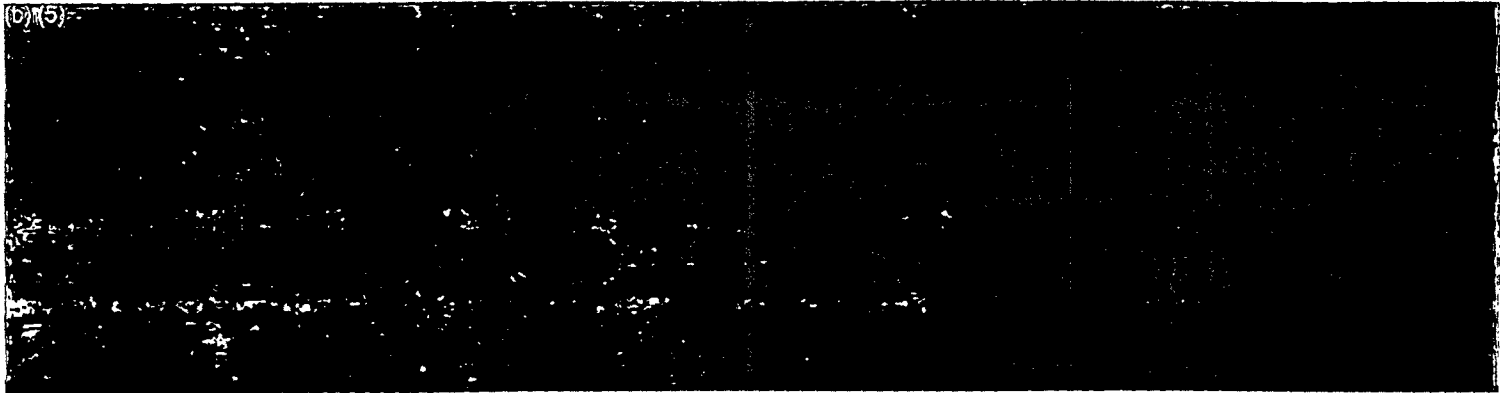
- Collection and use limitation: For terrorism and serious transnational crime only
- [REDACTED] } High (b)(7)
[REDACTED] } (b)(7)(E)
- Pre-72 hour access allowed with reason *UC*
- SORN/Privacy Act/Redress/FOIA – will apply at DHS origination level
- Highly sensitive data only upon specific need

For Official Use Only

Next Steps – US-EU

- Agreement expires July 2007

b5



b5


- [Redacted]
- [Redacted]

For Official Use Only

Other Countries

- Canada/Australia – Existing or pending EU agreements
- Non-EU countries
 - Now available for US-bound flights

High (b)(2)/(b)(7)(E) LE



For Official Use Only



65

Other [REDACTED] issues

65

[REDACTED]

High (b)(2)/(b)(7)(E) LE
[REDACTED]

[REDACTED]

High (b)(2)/(b)(7)(E)/(b)(5)
[REDACTED]

[REDACTED]

For Official Use Only

PNR EU Agreement: *What is CBP's position on the recently renegotiated PNR Agreement with the European Union and what does CBP believe are the material differences in the new agreement compared to the old PNR agreement? How does CBP anticipate that the new agreement will impact its various international aviation passenger-prescreening operations (including identity matching, risk targeting, IAP operations, etc.)? In addition what impact, if any, is expected from the new requirement that air carriers will have to "push" PNR data instead of CBP "pulling" the data?*

The new Passenger Name Record (PNR) agreement with the European Union is an interim agreement that will expire upon the date of any superseding agreement, but no later than July 31, 2007. The primary difference between the old and new agreement is the legal basis applied as the basis for the agreement under EU law. This change was necessary to comply with the May, 2006 ruling of the European Court of Justice, which found that the EU Data Protection Directive (95/46/EC) was not applicable to the transfer of PNR data to CBP because the transfer was for public security and law enforcement purposes.

Additionally, in connection with this interim agreement, the parties confirmed the ability of DHS to carry out its legal obligations by facilitating the disclosure of PNR to other U.S. government authorities that exercise counter-terrorism functions; such authorities will first need to assure DHS that they will protect the PNR data in a manner comparable to the way DHS protects such data (including security, training and accountability standards). CBP does not anticipate any significant impact on its international aviation passenger prescreening operations as a result of the interim agreement. Additionally, the new approach to disclosure of PNR will primarily benefit the other agencies that will now have access to this data to help support their counter-terrorism functions.

As part of the original PNR Undertakings, CBP stated that it would work with air carriers that wished to migrate to a "push" system, and during the past two years, CBP has been actively working with several EU carriers to implement such a system. CBP can support either a push or a pull method of obtaining PNR data. Currently, there are fifteen air carriers that push CBP PNR data; three of them are EU carriers. The push method has better and more modern technology for moving large amounts of data. It is also most cost efficient for CBP. The U.S. and EU understand that any push system employed by an air carrier must be consistent with CBP's operational needs.

Secretary

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



Homeland
Security

September 30, 2006

Erkki Tuomioja
Minister for Foreign Affairs
Republic of Finland
Helsinki, Finland

Franco Frattini
Vice President
European Commission
Brussels, Belgium

Dear Minister Tuomioja and Vice President Frattini:

As you know, the European Court of Justice has ordered that the Passenger Name Records (PNR) agreement between the United States and the European Union terminate tonight. We have been discussing a temporary interim PNR arrangement. Accordingly, I am pleased today to initial the attached agreement as a way forward. I do so with the following propositions in mind.

First, the right to decide which travelers are admitted through the borders of the United States is a fundamental attribute of our national sovereignty and a fundamental responsibility of my Department. I have no higher obligation than using this authority to protect our borders against those who would carry out acts of terrorism or serious transnational crime. As recent events have reminded us, trans-Atlantic air travel remains a particular focus for terrorist activity. Accordingly, there is an absolute need to assure that individuals seeking travel on U.S.-bound flights and admission to the United States are subject to appropriate security checks.

Second, the United States has full and plenary authority to require this information from travelers and air carriers. Such authority is contained in existing U.S. law and regulation. Moreover, each sovereign's interests in the control of its own borders is enshrined in the 1944 Chicago Convention on Civil Aviation, which gives each state party the right set the conditions and documentation requirements it deems necessary before admitting a traveler. Let me also be clear that the data we require relates to travelers voluntarily seeking admission to the United States.

Third, we appreciate European concerns that data protection provisions in Europe could be seen to impose inconsistent obligations on air carriers vis-à-vis U.S. PNR requirements. For that reason, we cooperated several years ago to develop an agreement for managing PNR data flows in ways that would not interfere with these European data protection provisions.

Fourth, we in fact signed such an agreement in May 2004. We find ourselves without that agreement, however, because European courts later determined that the European Commission lacked authority to commit to this agreement, so that it constituted an *ultra vires* act. This European Court ruling is, of course, absolutely an internal matter for European Union members, and we respect it.

Letter to Minister Tuomioja and Vice President Frattini
Page 2

Finally, in the spirit of cooperation – but also in light of our unwavering determination to secure our borders – we are prepared to sign the enclosed updated PNR agreement. As the enclosed initialed agreement shows, we are, in fact, prepared to continue the substance of the 2004 agreement, interpreted – as always envisioned – to reflect new U.S. legal imperatives on information sharing.

In July 2004, the 9-11 Commission issued its report on the attacks of September 11, 2001. The Report was highly critical of U.S. agencies' "systemic resistance to sharing information." Responding to this criticism, Congress enacted the Intelligence Reform and Terrorism Prevention Act of 2004, requiring the President to establish an information sharing environment "that facilitates the sharing of terrorism information." Congress called on the President to ensure to the greatest extent practicable that the environment "connects existing systems . . . and allows users to share information among agencies" and that it "ensures direct and continuous online electronic access to information."

Accordingly, we face additional obligations under U.S. legislation enacted since the signing of the 2004 agreement, and we must address these obligations in our PNR Undertakings in order to remain faithful to U.S. law. In fact, the original 2004 agreement specifically contemplated that our Undertakings must be consistent with U.S. law, including any new legislation.

With our agreement, I believe we will have assured the security of our traveling public while also protecting privacy.

Sincerely yours,



Michael Chertoff



Homeland Security

May 14, 2007

Dear Member of the European Parliament:

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

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

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

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

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

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

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

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

* On March 11, 2005, CBP arrested two individuals for smuggling drugs from London to Chicago. Their PNR information revealed the use of a common credit card. This credit card's reservation history identified a third traveler who had used the same card and listed a second credit card. Analysis of this new credit card number identified three additional travelers. Three of the four new travelers were arrested during subsequent travel for drug smuggling.

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

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

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

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

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

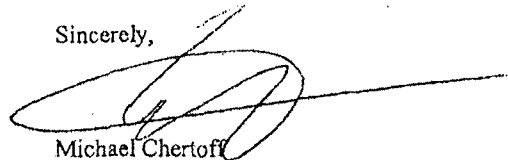
If such a system had been fully developed before 9/11, we might have been spared that tragedy. Consider this: two hijackers, Nawaq Alhamzi, appeared on a watchlist and would have been "flagged" when they purchased their tickets. Through analysis of their PNR data, we could have learned that three other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

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

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

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

Sincerely,

A handwritten signature in black ink, appearing to be "Michael Chertoff", written over a horizontal line. The signature is stylized and somewhat cursive.

Michael Chertoff