



Homeland Security

Privacy Office, Mail Stop 0550

February 7, 2008

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 twentieth 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 telephonic calls with counsel representing the Department of Homeland Security in December 2007, you agreed to narrow the scope of your request. The Government proposed that plaintiff eliminate non-responsive material within email chains from the scope of the request. Plaintiff agreed that emails within an email chain containing no responsive material may be removed from the scope of the request, and further suggested that defendant may eliminate duplicative copies of emails that contain responsive material from the scope of the request.

As we advised you in our December 7th partial release letter, we have completed our search for responsive documents, and all responsive documents have been processed except for the documents being held at DHS for classification review and the classified documents that were referred outside the agency for releasability review.

We completed our review of 11 responsive documents, consisting of 61 pages, which were being held for possible classification. I have determined all of those documents are releasable in part. The releasable information is enclosed. The withheld information, which will be noted on the *Vaughn* index when

completed, consists of properly classified information and deliberative materials. I am withholding this information pursuant to Exemptions 1, and 5 of the FOIA, 5 U.S.C. §§ 552 (b)(1), and (b)(5).

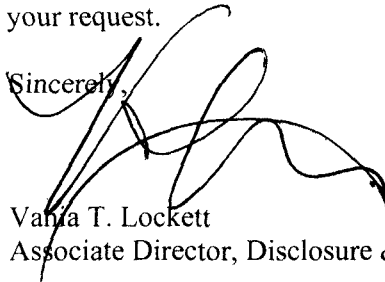
FOIA Exemption 1 provides that an agency may exempt from disclosure matters that are (A) specifically authorized under criteria established by an Executive Order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive Order. Portions of the withheld documents concern foreign government information relating to the national security and United States government programs and are classified under §§ 1.4(b), 1.4(c), 1.4(d), and 1.4(g) of Executive Order 12958, as amended.

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.

Our office continues to process your request insofar as it relates to the classified documents referred outside the agency and the remaining documents being held for DHS 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,



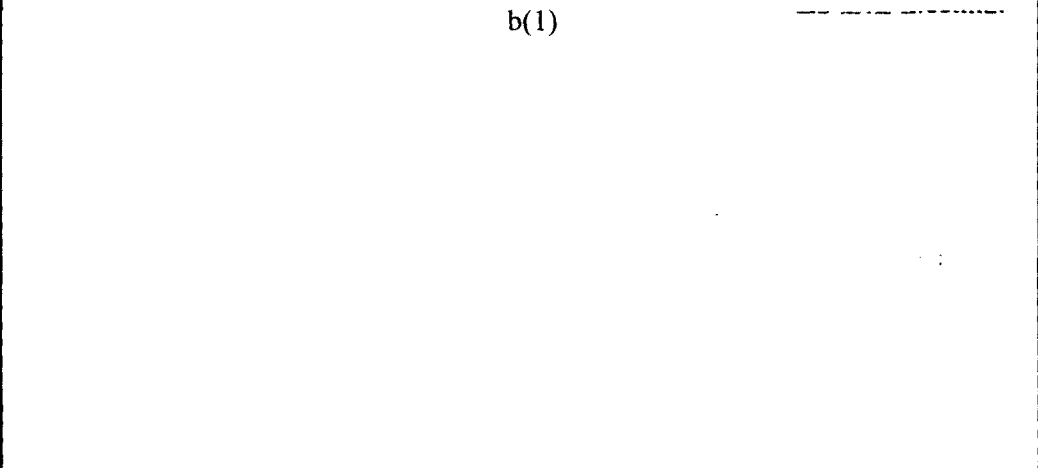
A handwritten signature in black ink, appearing to read 'Vanja T. Lockett', written over the word 'Sincerely,'.

Vanja T. Lockett
Associate Director, Disclosure & FOIA Operations

Enclosures: As stated, 61 pages

[Handwritten mark]

Prioritized Issues:

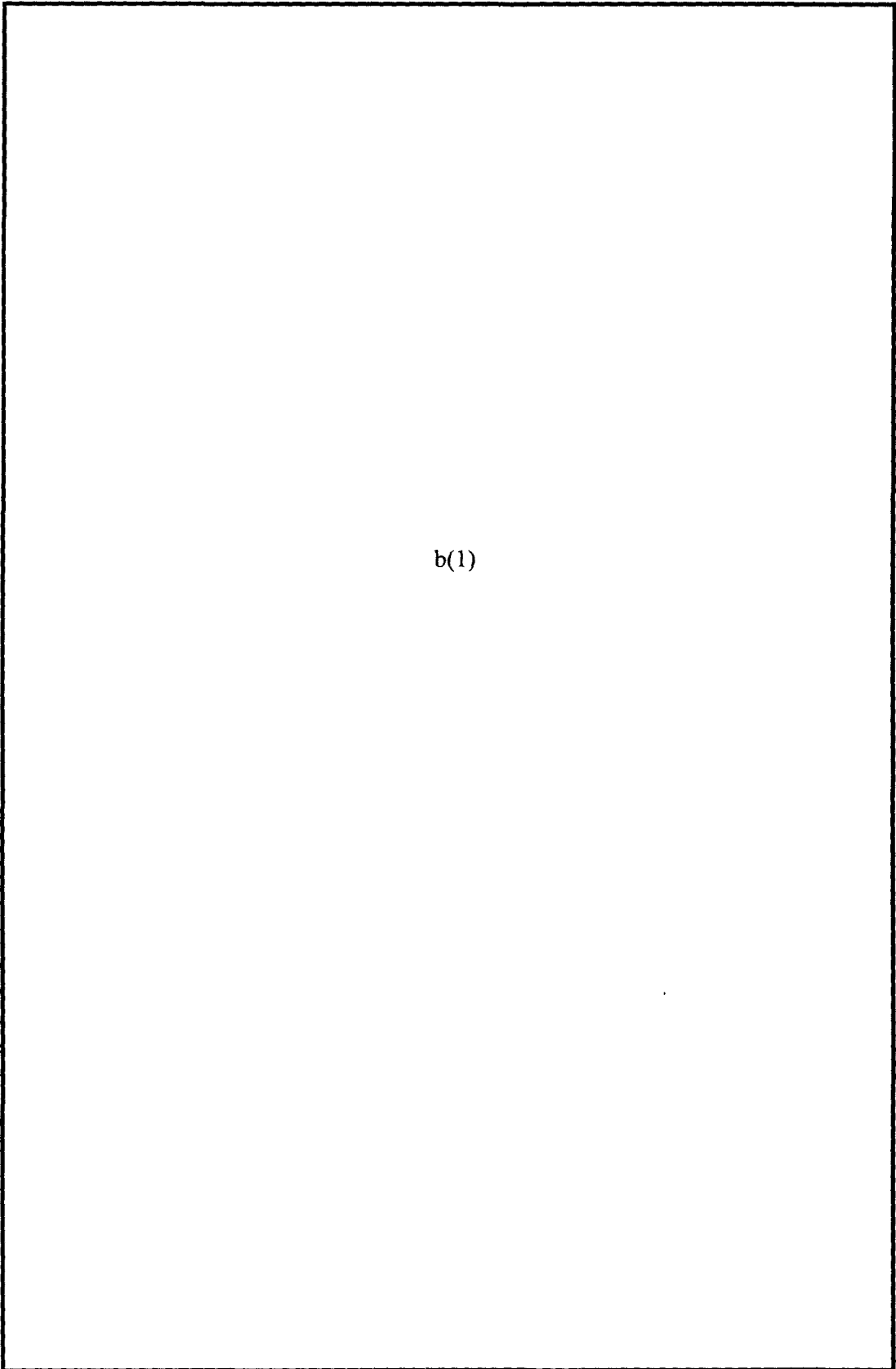
- 1. 
- 2. 
- 3. 

b(1)

Operationally, CBP has provided carriers 3 options for making PNR data available: 1.) Pull; 2.) Real-time push (data is transmitted upon creation or at 72 hours before the flight and any changes must be sent at the time they are made, or; 3.) A scheduled method under which carriers transmit PNR per a set schedule. Under this third option the carrier must provide CBP with a functional, automated means of obtaining PNR data outside of the scheduled pushes. Merely having a POC to call and request an independent push is insufficient.

[Handwritten mark]

~~SECRET~~



(S) 4.

b(1)

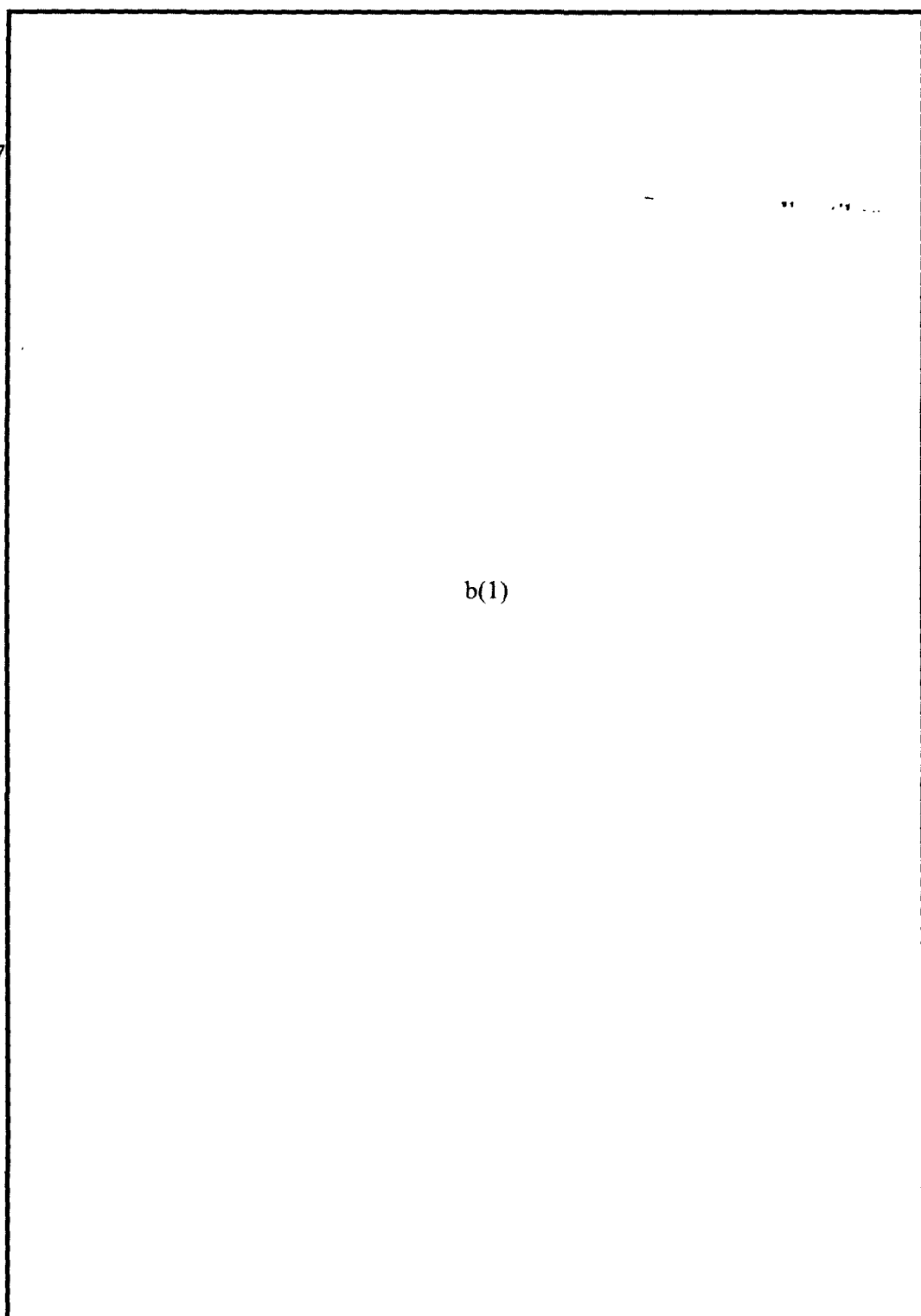
5.

6.

/

8.

(c) 7



8.

b(1)

9.

8.

Department of Homeland Security
US Immigration and Customs Enforcement
Discussion Document
US-EU PNR Dialogue

Purpose:

To provide talking points and background information on the Passenger Name Record (PNR) issue and related developments concerning law enforcement information sharing with the European Union (EU).

b(5)



Formatted: Bullets and Numbering
Deleted: the PNR agreement and
Formatted: Bullets and Numbering
Formatted: Bullets and Numbering
Formatted: Bullets and Numbering
Formatted: Bullets and Numbering
Formatted: Bullets and Numbering
Formatted: Indent: Left: 0.5",
Bulleted + Level: 2 + Aligned at:
0.75" + Tab after: 1" + Indent at:
1", Tabs: 0.75", List tab + Not at 1"

(u)

b(1)

b(5)



b(1)

The PNR Agreement was challenged by the European Parliament as insufficiently protective of EU privacy rights, and on May 19, 2006, the European Court of Justice (ECJ) struck down the Agreement.

The ECJ nullified the agreement on the procedural grounds that it was signed by the wrong EU legal authority, the one that deals with commercial issues rather than the one that deals with law enforcement and public security.

The EU notified the US that it will terminate the current Agreement on September 30, 2006 and has set a goal of establishing a new agreement by this date.

The future of our mission depends on reaching an agreement by this date.

Formatted: Indent: Left: 0.5"

Handwritten notes and signatures at the bottom right of the page.

(S)

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Formatted: Indent: Left: 0.5",
Tabs: 0.75", List tab + Not at 1"

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

[Redacted]

b(5)

[Redacted]

b(5)

[Redacted]

b(5)

[Redacted]

b(1)

Formatted: Indent: Left: 0",
Bulleted + Level: 1 - Aligned at:
0.25" + Tab after: 0.5" + Indent at:
0.5", Tabs: 0.25", List tab + Not at
0.5"

Formatted: Font: Not Italic

Formatted: No bullets or
numbering

Formatted: Bullets and Numbering

[Redacted]

b(5)

Formatted: Indent: left: 0.5",
Bulleted + Level: 2 + Aligned: at:
0.75" + Tab after: 1" + Indent at:
1", Tab: 0.75", List tab: Not at 1"

Deleted:

1
1
1

Background

Two converging events in Europe - the recent European Court of Justice decision on the legality of the EU-US PNR Agreement and a draft EU Framework Decision on Exchange of Criminal Data -- have major implications for US law enforcement and security.

The EU-US PNR Agreement. As noted, in May 2004, after substantial negotiations, the Department of Homeland Security entered into an agreement relating to the sharing of PNR information collected by air carriers flying to the United States from Europe. Central to the Agreement was a set of Undertakings made by Customs and Border Protection (CBP) regarding how it would treat the PNR data transmitted to it. Several of the limitations in those Undertakings significantly restrict US opportunities to use information for investigative and law enforcement purposes.

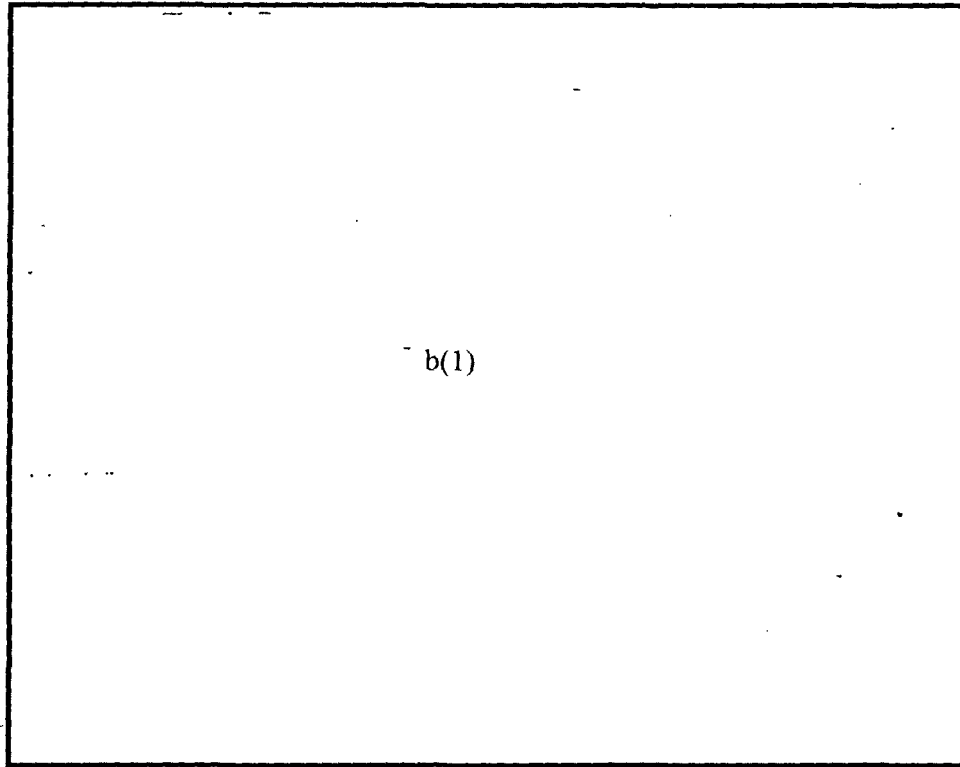
The most significant of these limitations, from the DHS perspective, are the following: (A) F
FOR OFFICIAL USE ONLY - NOT FOR DISTRIBUTION

[Redacted]

b(1)

[Redacted]

b(1)



(u) **The ECJ PNR Case.** The European Parliament (EP) filed two suits in the European Court of Justice (ECJ) challenging the information sharing arrangement.

(u) On May 30, 2006, the ECJ issued its opinion in the lawsuits. The opinion did not address the merits of the EU-US PNR Agreement or the role of the Parliament. Rather, the decision turned on the lack of competence of the Commission and Council to enter into the Agreement in the first instance. The EU had based its authority on the so-called "First Pillar," which allows the EU to regulate trade and commercial matters. The ECJ held (as the US had argued earlier) that the requirement that PNR data be sent to the US was a law enforcement and national security matter. Such transfers, the court held, were excluded from the data protection directive

(u) 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."

governing commercial data exports. If they are to be regulated, the court implied, it would have to be done under the "Third Pillar."

(U)

That is what the EU proposes to do. It has obtained authority from its Member States to erect substantially the same agreement on a new foundation. In order to meet the European Court of Justice deadline the Commission will seek to codify its position over the next couple of weeks and then will call for agreement on the new arrangement by September 30.

(U)

EU Proposals on Sharing Law Enforcement Information. The PNR negotiations will be closely intertwined with a broader effort to establish restrictive, EU-wide rules for information sharing in the area of law enforcement. Last October the EU put forward two draft documents that concern data sharing and protection in the law enforcement context. They consist of a draft Framework Directive of the European Parliament and Council on the retention of data and a proposed Council decision on the protection of personal data in criminal matters. [REDACTED]

[REDACTED]

b(5)

(U)

Article 15 of the draft Framework Directive, which would have the force of law within the European Union, lays out procedural rules for information sharing between individual EU member states.³

(S)

[REDACTED] b(1)

(U) (S)

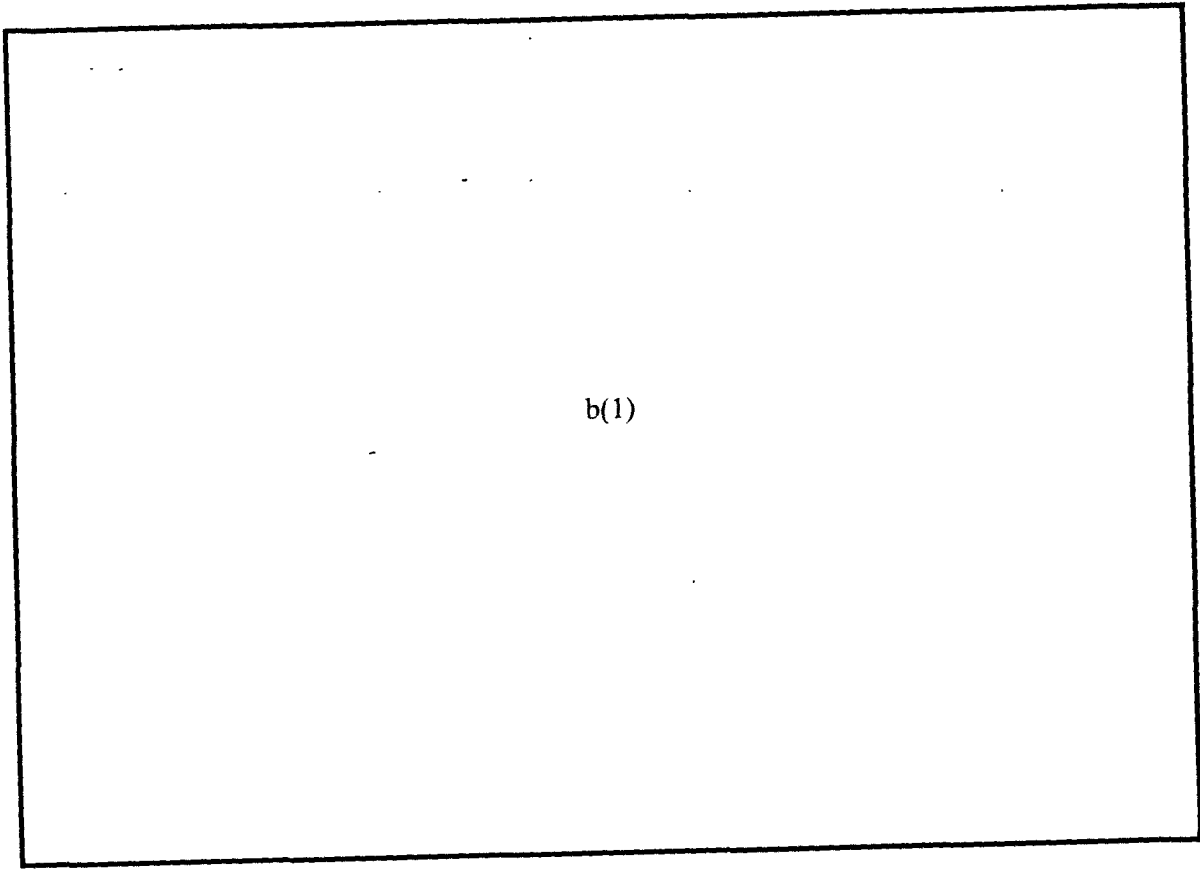
[REDACTED] b(1)

(U)

³ For example, the Draft Decision contains provisions on time limits for retention of shared data, ensuring the accuracy of shared data, logging and audit trails, as well as restrictions limiting further use of the data to the original purpose for which it was first transmitted. In effect, it borrows heavily from the PNR Agreement and the undertakings.

[REDACTED] b(1)

(c)



b(1)

SECRET

~~SECRET~~

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



Hi PNR
Se file

~~June 7, 2006~~
June 8, 2006

ACTION

MEMORANDUM FOR: Stewart Baker, Assistant Secretary for Policy (U)

THROUGH: Paul Rosenzweig, Acting Assistant Secretary for Policy Development and Counselor to the Assistant Secretary for Policy (U)

FROM: Michael Scardaville, Special Assistant and International Policy Advisor, PDEV (U)

SUBJECT: Assessment of the Commission's proposed resolution of the PNR situation and recommended short term actions (U)

Purpose (U)

(S)

b(1)

Background: The Commission's Proposal (U)

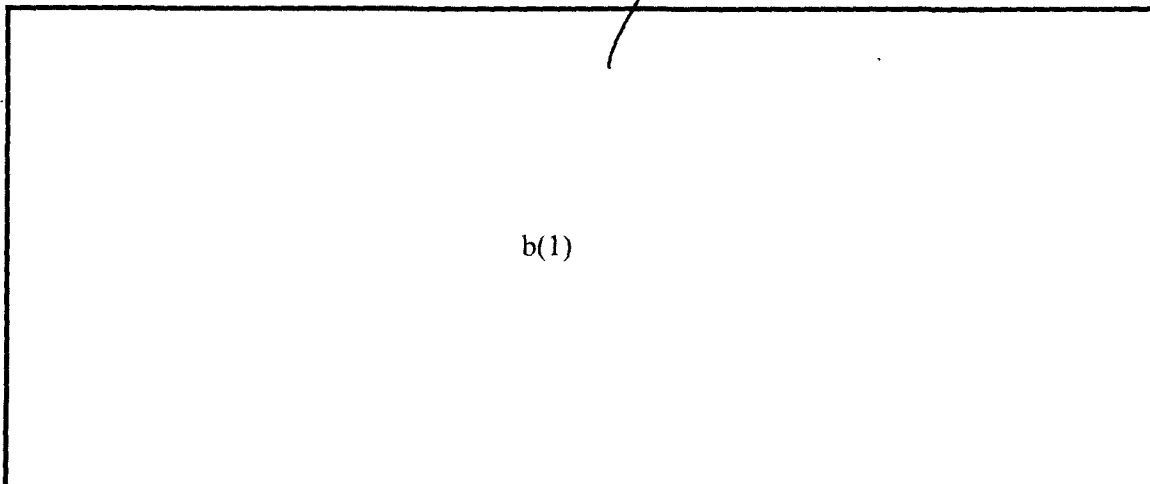
(U) As previously reported, over the course of the next couple of weeks the Commission will seek a decision from the European Council granting the Council Presidency (currently the Government of Austria but this position transfers to the Government of Finland on July 1), in close consultation with the Commission, authority to negotiate a new instrument with the United States on behalf of the European Union under Articles 24 and 38 of the Treaty on European Union. These same provisions were used in recent DOJ agreements with the EU on mutual legal assistance and cooperation with Europol and, as a result, their use has precedent in the area of law enforcement and security

(F61-mod)

~~SECRET~~

DERIVED FROM:
SCHNEIDER MFR
DECLASS: -

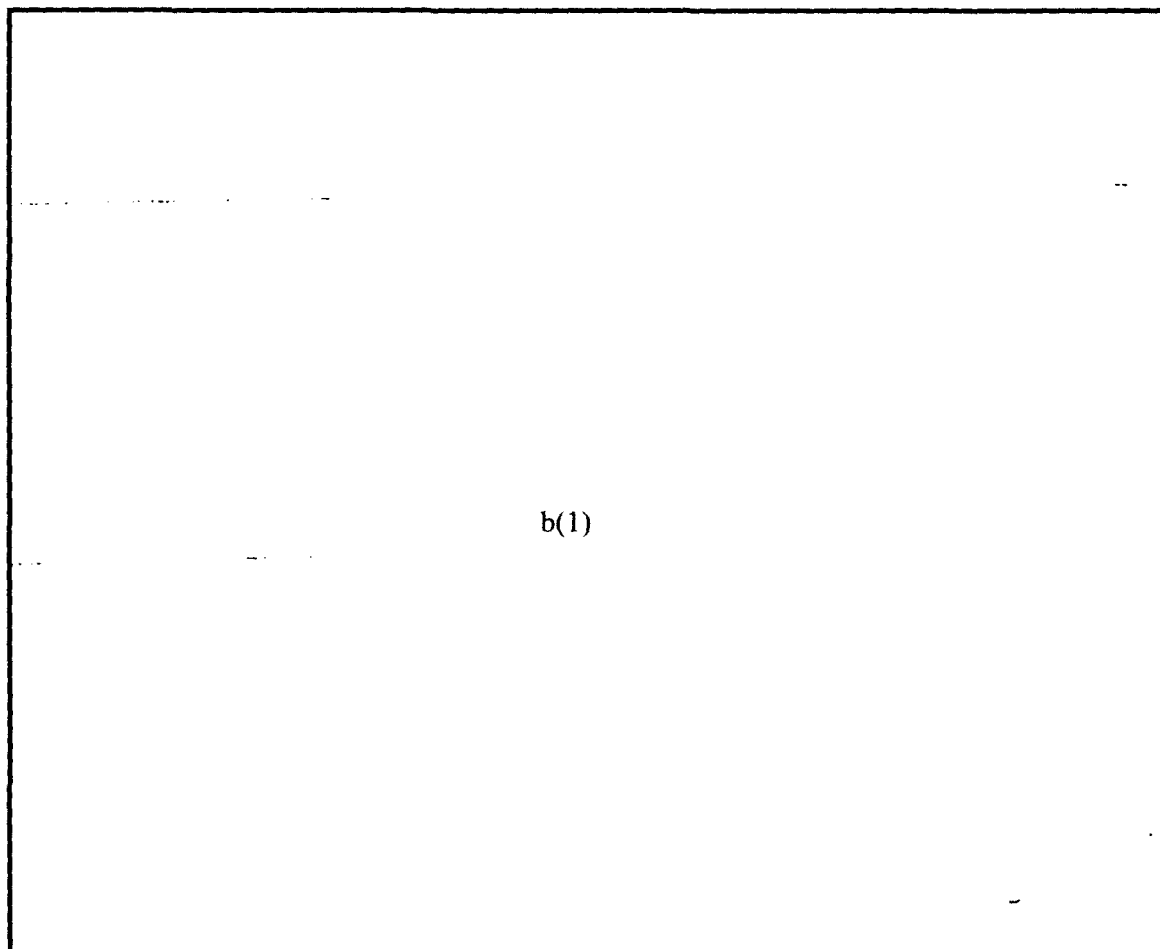
~~FOUO/NOFORN~~



b(1)

(U) Around the same time that the Council Decision is being finalized, but definitely by June 30, 2006, the Commission intends to notify DHS of its intent to terminate the agreement under the provisions of Article 7 of the Agreement. This is necessary to comply with the Court's decision to preserve the effect of the Commission's adequacy finding until September 30, 2006.

:/F61-mod)



(C)

b(1)

:/F61-mod)

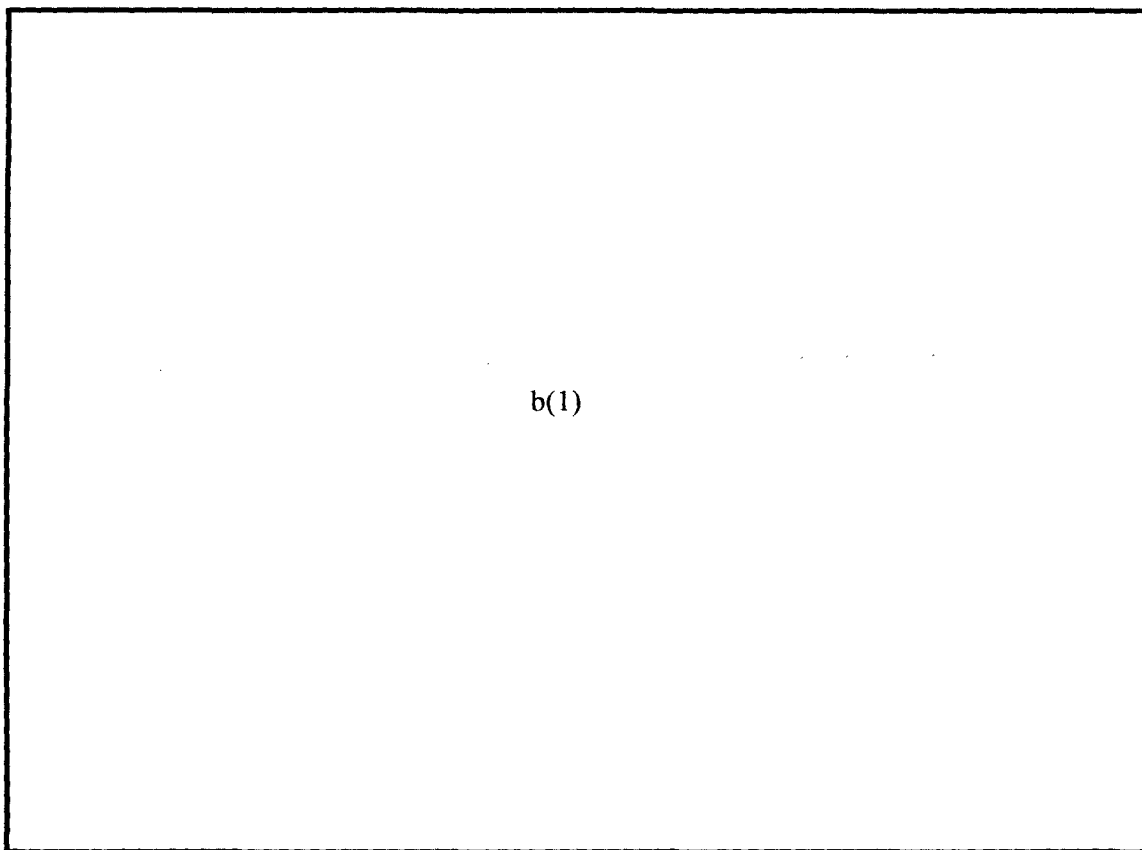


~~FOUO/NOFORN~~

Discussion (U)

(S) The Commission's Goal:

(S)



b(1)

(S)

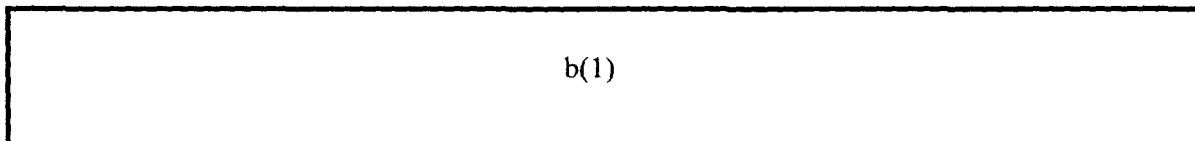
DHS Interests: (U)

(S)



b(5)

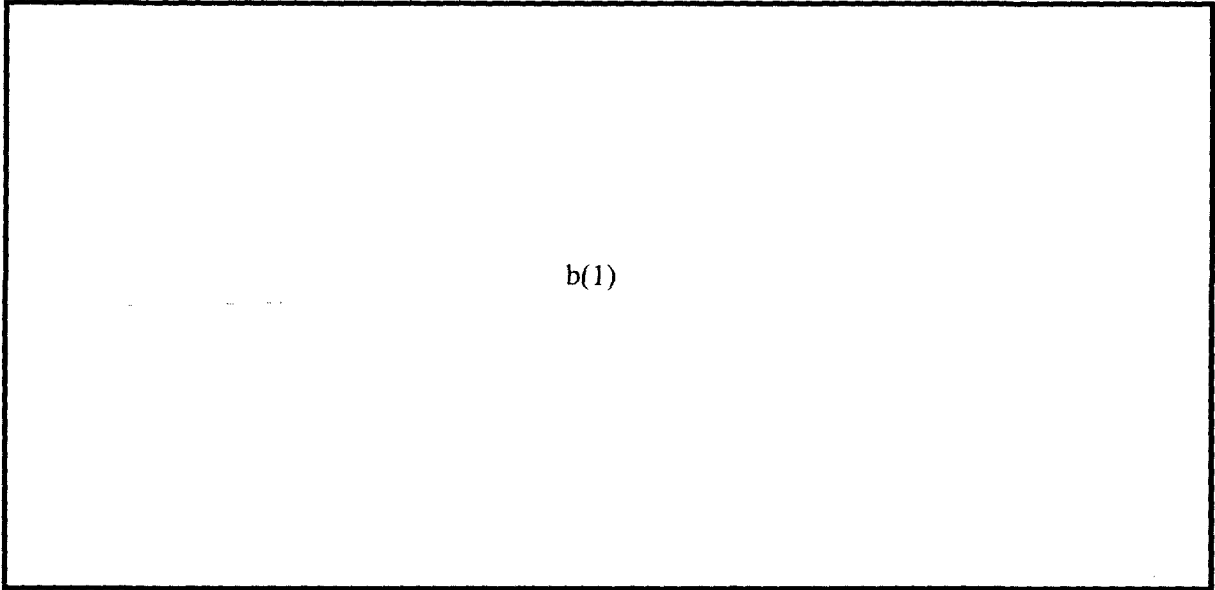
(S)



b(1)

[Handwritten mark]

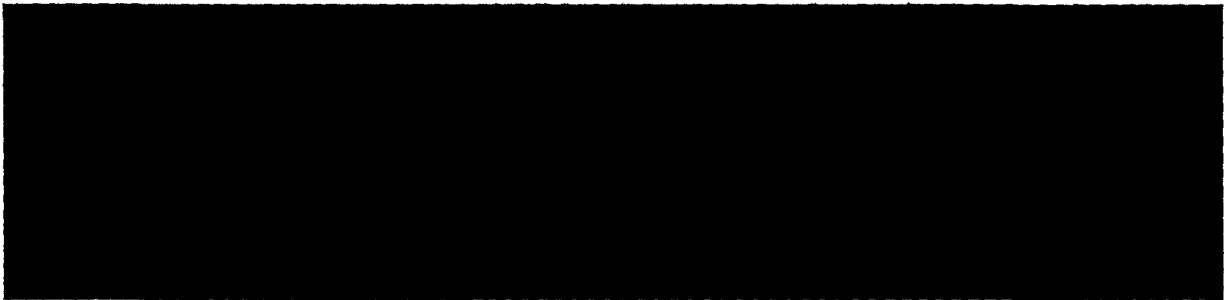
FOUO/NOFORN



b(1)

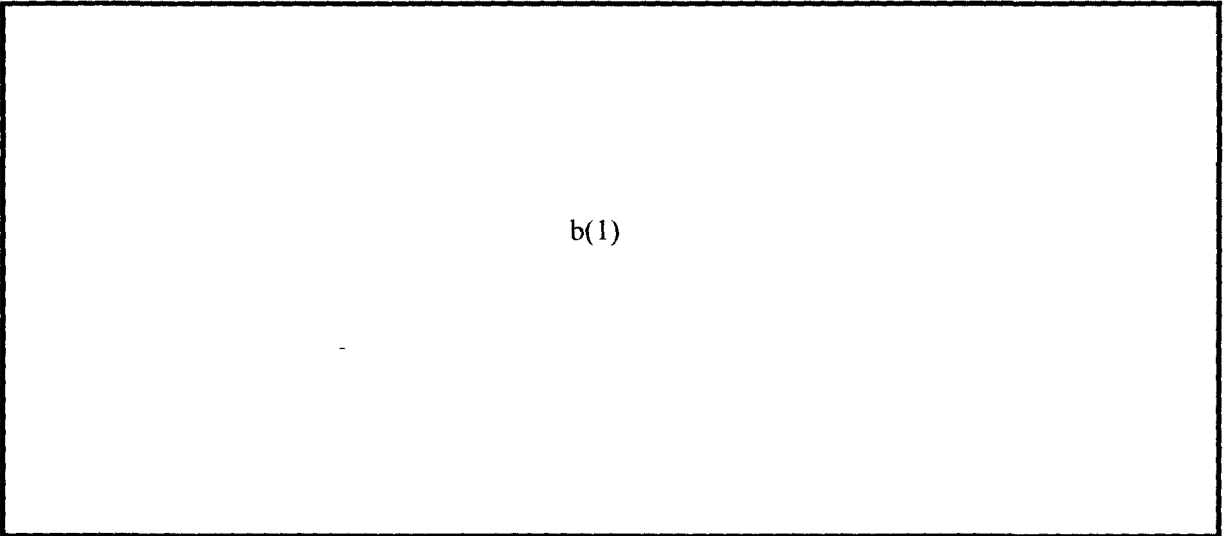
(c) (u)

Time Constraints: (S)



b(5)

(c)



b(1)

(c)

(c)

FOUO/NOFORN

~~SECRET~~ NOFORN

The Next Step: (u)

(F61-100)

b(1)

Critical Issues: (u)

(c) ~~(u)~~

(c)

(c)

(c)

(c)

b(1)

~~SECRET~~ NOFORN

~~SECRET~~
FOUO/NOFORN

(c) 2.
(c)

(c)

b(1)

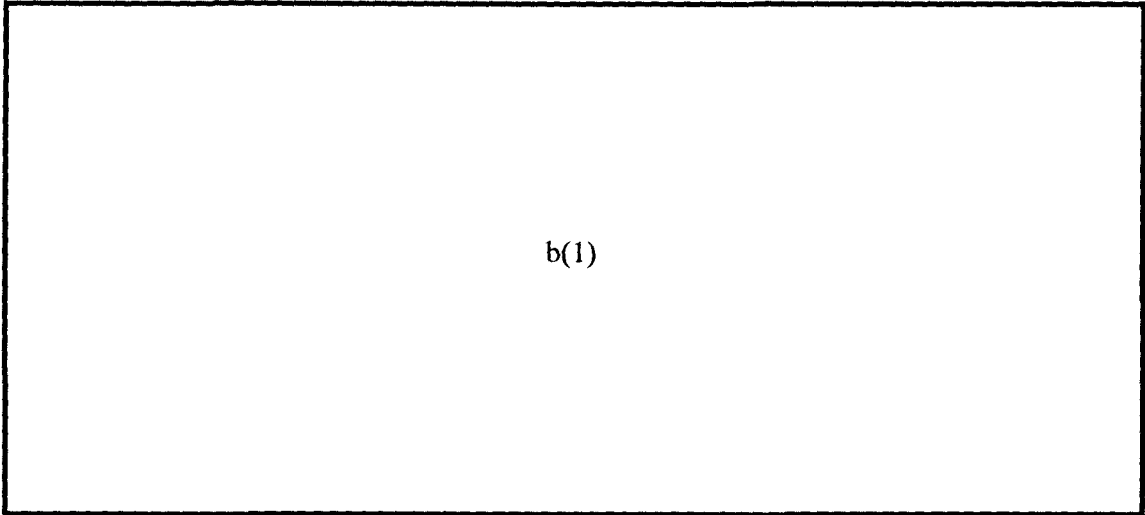
(c)

(c)

~~SECRET~~
FOUO/NOFORN

~~SECRET~~
FOUO/NOFORN

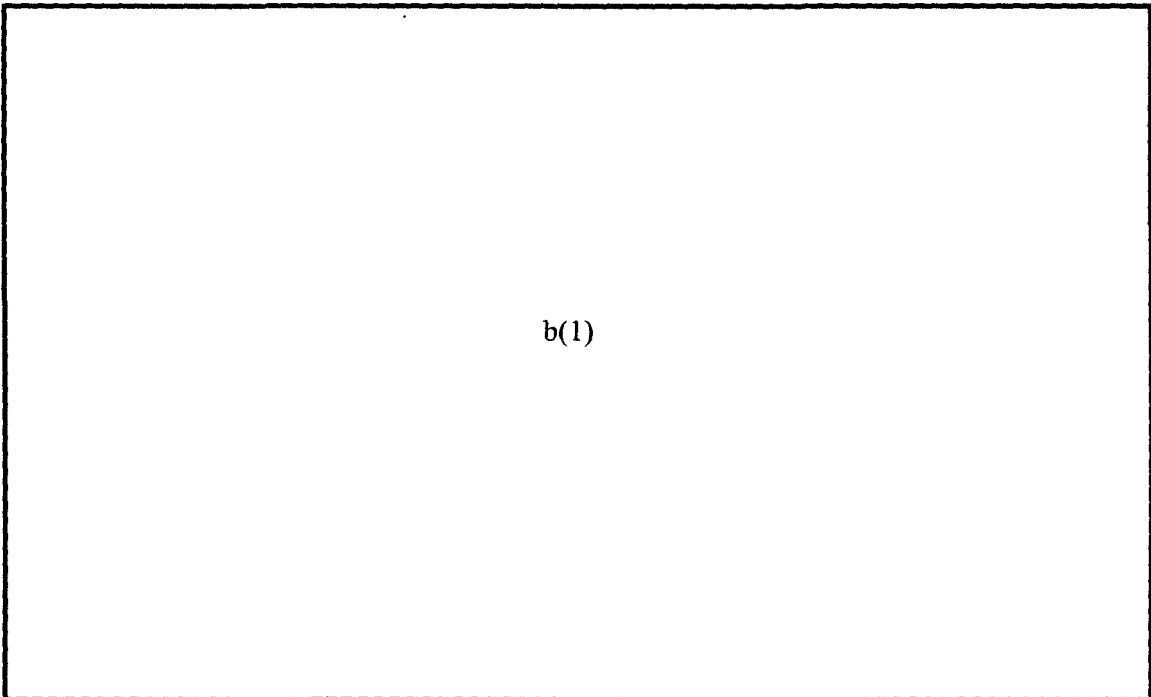
(c)



b(1)

Recommendations (u)

(c) 1.



(c)

b(1)

(c)

Approve _____ Disapprove _____
Modify _____ Needs more discussion _____

~~SECRET~~

~~CONFIDENTIAL~~

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



Homeland
Security

December 8, 2006

Deleted: June 12, 2006

Deleted: June 11, 2006

INFORMATION

MEMORANDUM FOR: Stewart Baker, Assistant Secretary for Policy

THROUGH: Paul Rosenzweig, Acting Assistant Secretary for Policy Development and Counselor to the Assistant Secretary for Policy

FROM: Michael Scardaville, Special Assistant and International Policy Advisor, PDEV

SUBJECT: Assessment of the Commission's proposed resolution of the PNR situation and recommended short term actions

Purpose

(S) (S)
(S) (S)
all (S)
#

b(1)

Background: The Commission's Proposal

(S)

b(1)

(S)

~~CONFIDENTIAL~~

Derived: Schneider MFE
Declass: 8 Dec 2021

FOUO/NOFORN

~~CONFIDENTIAL~~

(c)

entc

(c)

(c)

b(1)

(c)

(c)

FOUO/NOFORN

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

(c)

b(1)

Discussion

The Commission's Goal:

(c)

b(1)

(c)

DHS Interests:

(c)
(c)

b(1)

(u)

¹ 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 the Information Sharing Environment" (ISA)

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

(c)

b(1)

Time Constraints:

(c)

b(1)

(c)

(c)

Critical Issues:

(c)

b(1)

~~CONFIDENTIAL~~

FOUO/NOFORN

~~CONFIDENTIAL~~

(c)

(c)

(c)

(c)

(c)

b(1)

FOUO/NOFORN

~~CONFIDENTIAL~~

FOUO/NOFORN

~~CONFIDENTIAL~~

(P)

(C)

(C)

b(1)

(C)

(C)

b(1)

FOUO/NOFORN

~~CONFIDENTIAL~~



Homeland Security

June 12, 2007

Deleted: June 16, 2006

Memorandum

TO: [REDACTED] b(5)

FROM: [REDACTED] b(5)

RE: Passenger Name Records and Law Enforcement Information Sharing - Negotiations With The European Union

Purpose

To provide you with background information on the Passenger Name Record (PNR) issue and related developments concerning law enforcement information sharing with the European Union (EU) in preparation for a mid-July "un-DC."

Summary

Before September 11, the 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. This information - name, contact information, and the like - was drawn from information supplied to the airline as part of the reservation process. DHS uses the information to screen for no-fly violators and terrorist suspects before the plane takes off, protecting against midflight hijackings and bombings.

For flights between Europe and the U.S., the data must be [REDACTED] b(5) has long prohibited the export of personal data to countries whose legal protections are not "adequate" in the view of European data protection authorities. While the U.S. has many privacy laws, it does not have an overarching data protection regime that matches every aspect of European law. It has therefore been condemned as inadequate by European standards, and commercial data transfers to the U.S. have long been restricted. European airlines feared (with reason) that European data protection agencies would view the PNR transfers in the same light and would impose fines and other penalties on airlines that provided the PNR data to the U.S. Government.

Handwritten initials: JF, MJD

[REDACTED]

b(1)

Handwritten circled 'C' with an arrow pointing to the right.

The PNR Agreement was challenged by the European Parliament, which contended that the Agreement was insufficiently protective of EU privacy rights. On May 30 the European Court of Justice (ECJ) struck down the Agreement, not on substantive grounds but on procedural ones. Under EU law, commercial issues are within the competence of the EU and fall under the "First Pillar" authority – the authority that the EU had relied on in entering the Agreement. The ECJ held that the US wanted PNR data for law enforcement and public security reasons. Law enforcement and public security are not completely outside the EU's authority, but they fall within the "Third Pillar," where the authority of EU central institutions (the Commission, Parliament and Court of Justice) is more limited and more authority is left to the Member States.

Deleted: [REDACTED]
Deleted: [REDACTED] b(5)
Deleted: [REDACTED]

The EU now plans to seek authority from the Member States to renegotiate the PNR Agreement under the Third Pillar. The Commission has portrayed this as a technical change that would put the same agreement back in place, albeit under a different legal authority.

[REDACTED]

b(1)

Background

Two converging events in Europe – the recent European Court of Justice decision on the legality of the EC-US PNR Agreement and a draft EU Framework Decision on Exchange of Criminal Data -- have major implications for US law enforcement and security.

[REDACTED]

b(1)

The most significant of these limitations, from our perspective are the following: (u)

(c)
1.4(d)

(c)

(c)

(c)

[Redacted]

b(1)

(c)

[Redacted]

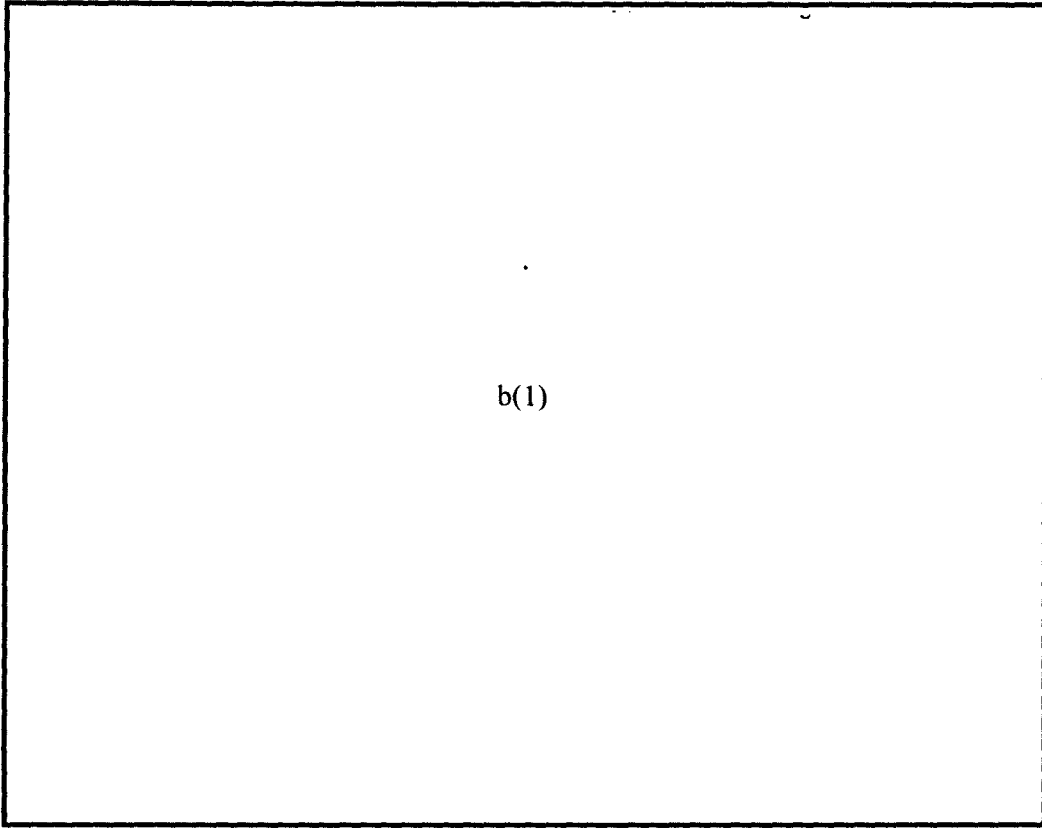
b(1)

Formatted: Space After: 5 pt
Deleted:

(u)

¹ PNR can also be used and transferred to address significant health risks under Paragraph 34. As noted below, despite this authorization the EU's Article 29 Working Party has concluded that CDC's plans to retain PNR data for health-related purposes violates EU law.

7



(S)

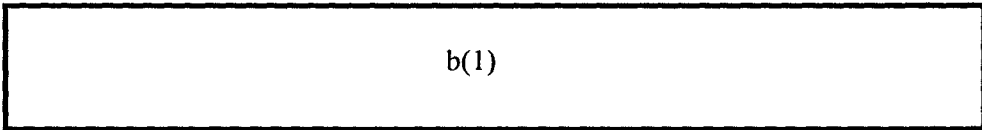
(C)
1.4(d)

b(1)

(S)

(U)

The ECJ PNR Case. The Agreement was no less controversial in Brussels. Disturbed over what it viewed as an attack on personal privacy and its own authority, the European Parliament (EP) filed two suits in the European Court of Justice (ECJ) challenging the information sharing arrangement.



b(1)

(C)
4(b)
(U)

³ 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."

~~SECRET~~

(4) That is what the EU proposes to do. It is seeking authority to erect substantially the same agreement on a new foundation. In order to meet the European Court of Justice deadline, the Commission will seek to codify its position over the next couple of weeks and then will call for agreement on the new arrangement by September 30.

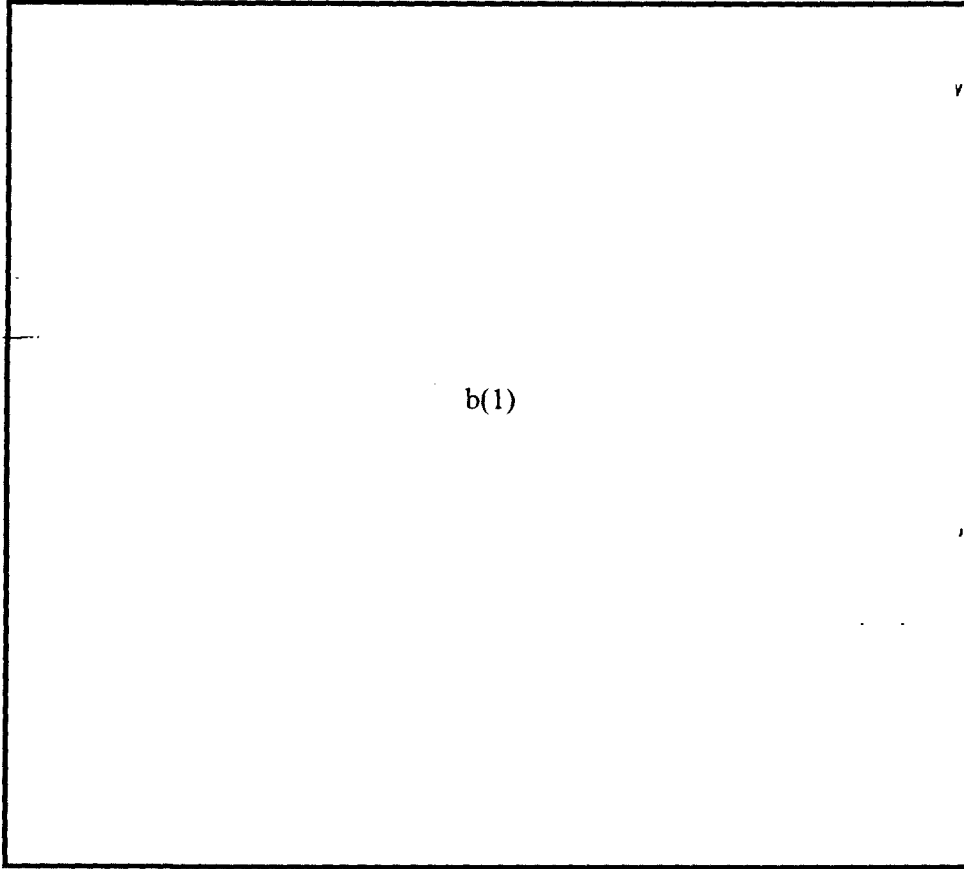
(5) [Redacted] b(1)

(4) **EU Proposals on Sharing Law Enforcement Information.** If that were all that is at stake, this would be an interesting diplomatic and legal problem for DHS. But it is not. The PNR negotiations will be closely intertwined with a broader effort [Redacted] b(5)
[Redacted] b(5) Last October the EU put forward three draft documents that concern data sharing and protection in the law enforcement context. They consist of a draft directive of the European Parliament and Council on the retention of data, a proposed Council decision on the protection of personal data in criminal matters, and [Redacted] b(5) a proposed Council decision on the exchange of law enforcement data between member states and third parties.

(Other) (Redacted) b(1)

(4) Acting under the First Pillar, the EU has also entered into a PNR sharing agreement with Canada. In light of the EU's determination that the US Undertakings provided "adequate" privacy protections, the EU-Canada agreement authorizes Canada to share PNR data received from the EU with the US. Even though the ECJ has struck down the EU-US agreement, the EU contends that its similar agreement with Canada remains in effect. Some Canadian government sources are concerned, however, that the absence of an "adequacy" finding (which is a First Pillar concept) may now have the effect of prohibiting US-Canada information sharing derived from EU-originated flights.

Deleted:



(C/Fgi-
Mod)

(S)

Deleted: the

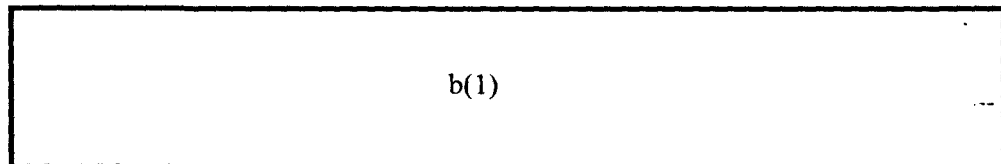
b(1)

(C/Fgi-
Mod)

(C/Fgi-Mod)

⁵ For example, the Draft Decision contains provisions on time limits for retention of shared data, ensuring the accuracy of shared data, logging and audit trails, as well as restrictions limiting further use of the data to the original purpose for which it was first transmitted. In effect, it borrows heavily from the PNR Agreement and the Undertakings.

(R)



b(1)

(e/Fgi-
Mod)

⁷ The adequacy finding granted to the U.S. was specific to the transfer of PNR data and only extended to its transmission to CBP. The May 30th decision of the ECJ also annuls this decision by the Commission on the grounds that the Commission did not have the legal authority to grant it

(a)

Handwritten signature or scribble at the bottom of the page.

(C/Fgi-Hod)

Communicable Diseases.

[Redacted] European reaction to another US initiative relating to avian flu. If air passengers are exposed to a pandemic strain of avian flu, the government will need to locate all of the passengers and crew, quickly. So the Centers for Disease Control has proposed a rule requiring airlines to retain PNR for up to 60 days for that purpose. The top data protection authorities of Europe, known as the "Article 29 Working Party," have now decided that this sort of data retention violates EU privacy directives. If given effect, the Working Party's opinion would place air carriers at legal jeopardy because of inconsistent legal regimes. It reflects a widespread EU view that privacy trumps even the critical public health interests of the United States.

b(5)
b(5)

Deleted:

Analysis & Recommendation

[Redacted]

b(1)

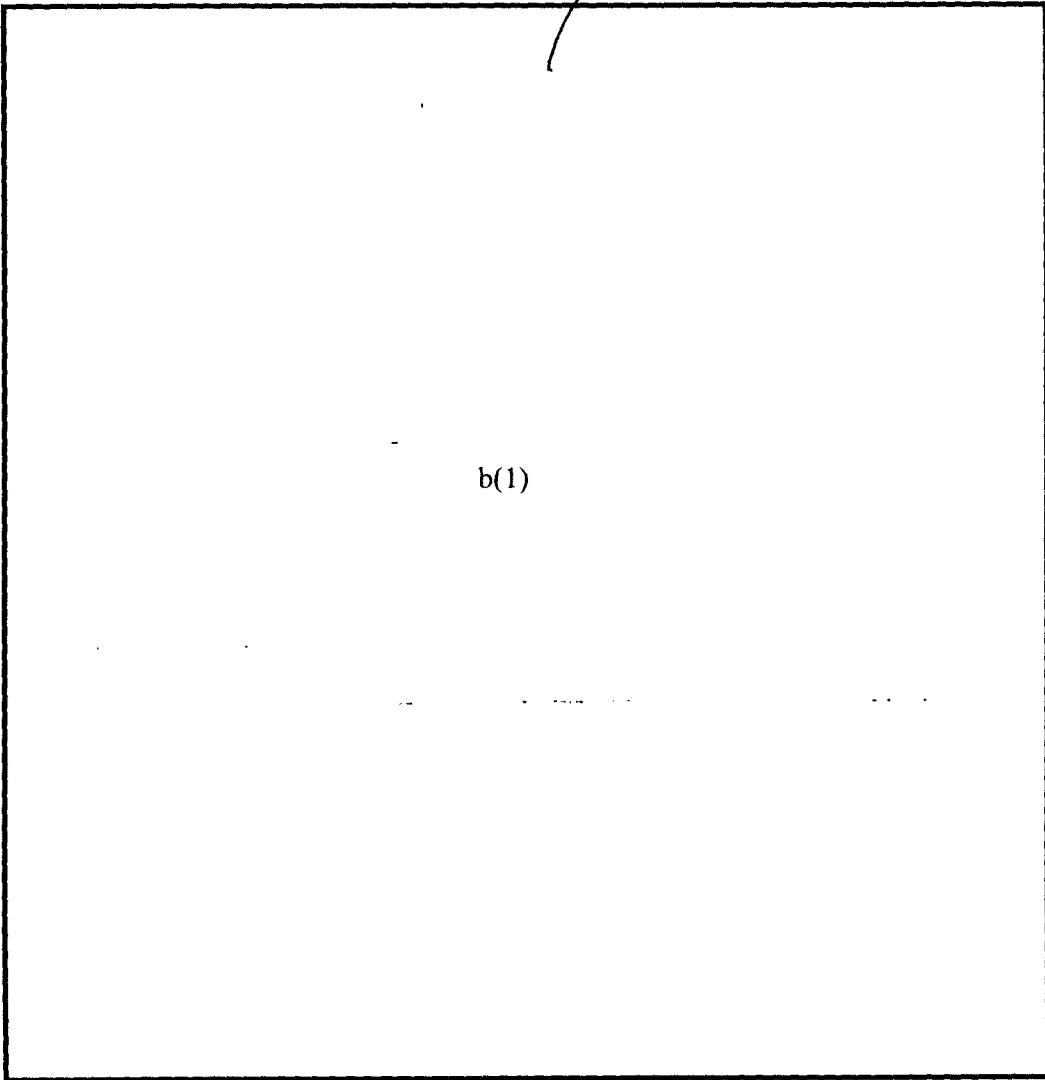
(S)
(S)
(S)

If adopted, the Draft Decision could conflict with a number of binding and non-binding information sharing arrangements that the United States has signed. For example, we have signed a 2003 Mutual Legal Assistance Agreement (MLAA) with the European Union and a 2001 information sharing agreement with Europol (the EU-level police agency); with respect to member states, we signed a 2003 MLAT with Germany, which builds on numerous other MLATs already in force with other EU member states. The United States also has many executive agreements and memoranda of understanding with member states under which critical information is currently being shared. Under EU law, directives supersede bilateral treaties and agreements and member states must conform their existing agreements with the directive.

(4)

Unlike in 2003, this risk is present now because the Court has conclusively ruled that the transfer of PNR data is a law enforcement matter. While European integration has been the greatest in areas associated with the Common Market, law enforcement and public security is a relatively new area of activity at the community level and many responsibilities still fall to the EU Member States. The ECJ firmly placed PNR in the area of law enforcement and public security, and as result, any actions taken in this area are likely to set precedents for further community involvement in other law enforcement matters.

(4)



(S)

(C) 1.4(d)

(S)

(C) 1.4(d)

Conclusion

The USG has a paramount interest in ensuring that law enforcement and border control information continues to flow to the United States. In creating the Information Sharing Environment we are working to break down walls that restrict the sharing of information between Federal agencies.

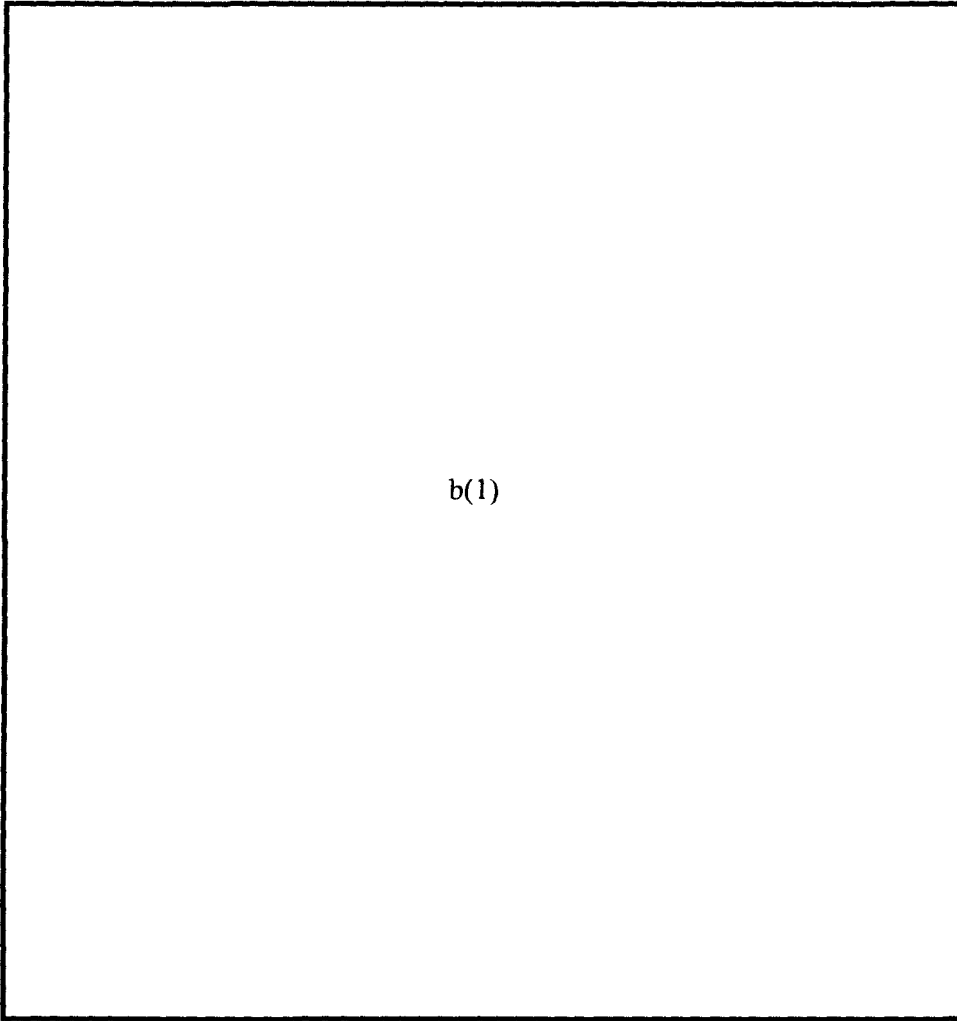
The PNR Agreement that the US signed with the EU in 2004 is an example of the old-style artificial limitation. We entered into the PNR Agreement based upon the EU's argument that the export of

(C)

(C)

(C) ↑ 1.4(d)

S/E



b(1)

(c)

(s)

(P) 4 (c)

/

~~CONFIDENTIAL~~

4712

DHS Priorities for Negotiation with the EU (U)

(U) With the expiration of the 2004 Agreement, there are several terms agreed to under the 2004 Agreement that DHS would like to revisit. Below are the specific changes DHS would like to pursue in a new agreement on the transfer of PNR data, in order of priority.

(c) • [Redacted] b(1)

(c) • [Redacted] b(1)

(c) • [Redacted] b(1)

(c) • [Redacted] b(1)

(c) • [Redacted] b(1)

(c) • [Redacted] b(1)

(c) • [Redacted] b(1)

~~CONFIDENTIAL~~

DERIVED: SCHNEIDER MFR
DECLASS: 9 AUG 2021

~~CONFIDENTIAL~~

(c)° [Redacted] b(1)

(c)• [Redacted] b(1)

(c)° [Redacted] b(1)

(c)• [Redacted] b(1)

(c)° [Redacted] b(1)

(c)• [Redacted] b(1)

(c)° [Redacted] b(1)

~~CONFIDENTIAL~~

UNCLASSIFIED

ELEMENTS OF A COOPERATIVE SYSTEM FOR COLLECTING AND USING PNR
DATA (U)

Collection and Use of Passenger Name Record (PNR)

- (U) 1. The Participants may collect PNR from air carriers' reservation and departure control systems located within the territory of another Participant for the purposes of preventing and combating terrorism and other crimes, as well as protecting the safety, health and security of airline passengers.
- (U) 2. Upon acquiring such data, the collecting agency or agencies of the Participants may share or otherwise provide access to other relevant authorities to accomplish the above purposes or as otherwise required by law.
- (U) 3. PNR data may be collected in a timeframe and a manner necessary for the purposes in paragraph 1 and may be retained as long as necessary for any purposes consistent with paragraph 1.

Protection of PNR Data

- (U) 4. Each Participant collecting, using and processing PNR should provide notice to airline passengers, directly or through air carriers. The notice should explain the nature of the information collected and the uses to which it is put without disclosing information that would compromise legitimate security interests.
- (U) 5. A Participant receiving PNR data should use its best efforts to maintain all such personal data in a manner that provides security and protections comparable to the security and protections provided to such information concerning its own citizens.
- (U) 6. Each Participant should promptly respond to questions from members of the public, regardless of nationality, regarding data protection or the accuracy of PNR data collected by that Participant.
- (U) 7. PNR data revealing race, political opinions, or religious or other beliefs, or concerning health and sexual life, should be used only upon a determination by a Participant that such data is particularly relevant to a purpose set forth in paragraph 1.
- (U) 8. The Participants should take appropriate action under their administrative, civil, or criminal laws in the event of misuse, alteration, or deletion of, or unauthorized access to, the data by their employees, agents or third parties.

International Cooperation

UNCLASSIFIED

UNCLASSIFIED

- (U) 9. No Participant should interfere with another Participant's access to PNR collected by a third state and shared pursuant to mutual arrangement consistent with the purposes detailed in paragraph 1.
- (U) 10. No Participant should interfere with an air carrier's ability to comply with rules, regulations or other orders governing access to PNR data that are issued by another Participant
- (U) 11. In the event that a Participant does not believe that another Participant is abiding by these Elements, the Participant should inform the other Participant of its intent to seek consultations. Restrictions on the collection, use and processing of data necessary for any of the purposes set forth in paragraph 1 should not be imposed in response to a perceived breach of these Elements if there is any significant possibility that the restrictions would increase the risk of a successful terrorist attack
- (U) 12. Participants should provide advance notice to each other of any action by a citizen or other entity (governmental or otherwise) that may challenge application of these Elements and should take all action to defend these Elements against challenge.

UNCLASSIFIED

~~CONFIDENTIAL~~
FOR OFFICIAL USE ONLY

Attachment 1: Detailed Assessment of Critical Issues (U)

(c) •

(c)

(c)

b(1)

(c) _____
[Redacted box] b(1)

FOR OFFICIAL USE ONLY

~~CONFIDENTIAL~~

DERIVED: SCHNEIDER MAR
DECLASSIFY 31 DEC 2021

~~CONFIDENTIAL~~

FOR OFFICIAL USE ONLY

(c)

(c)

(c)

b(1)

(c)

(c)

(c)

FOR OFFICIAL USE ONLY

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~
FOR OFFICIAL USE ONLY

(c) •

(c) •

b(1)

(c)

(c)

(c)
(c)

b(1)

FOR OFFICIAL USE ONLY

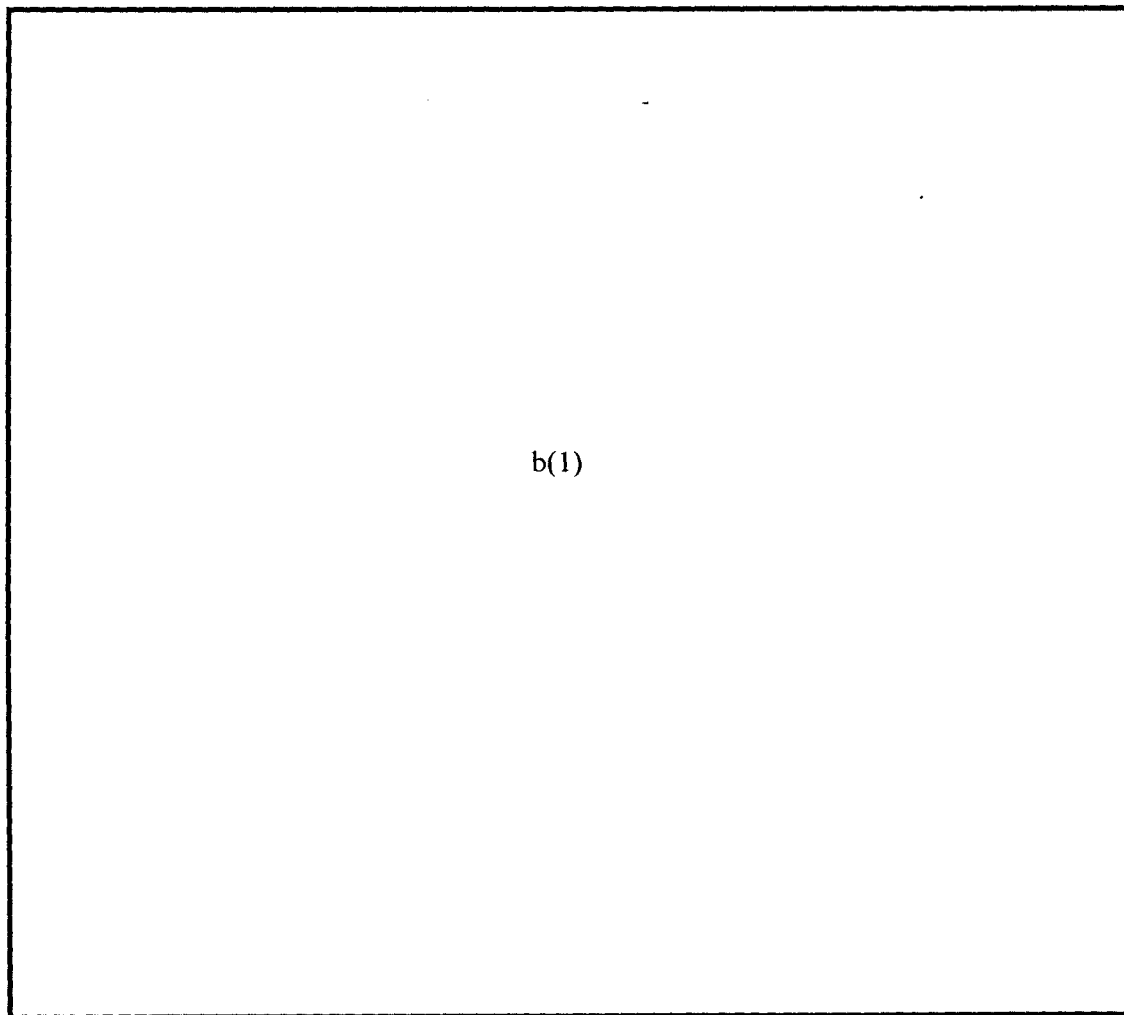
~~CONFIDENTIAL~~

~~CONFIDENTIAL~~
FOR OFFICIAL USE ONLY

(S)

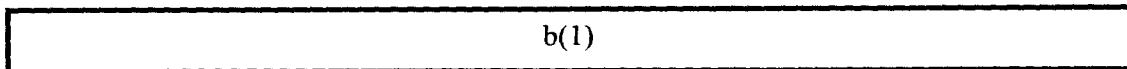
(C)

(S)



b(1)

(C)



b(1)

FOR OFFICIAL USE ONLY

~~CONFIDENTIAL~~

~~Confidential~~

(C)

(C)

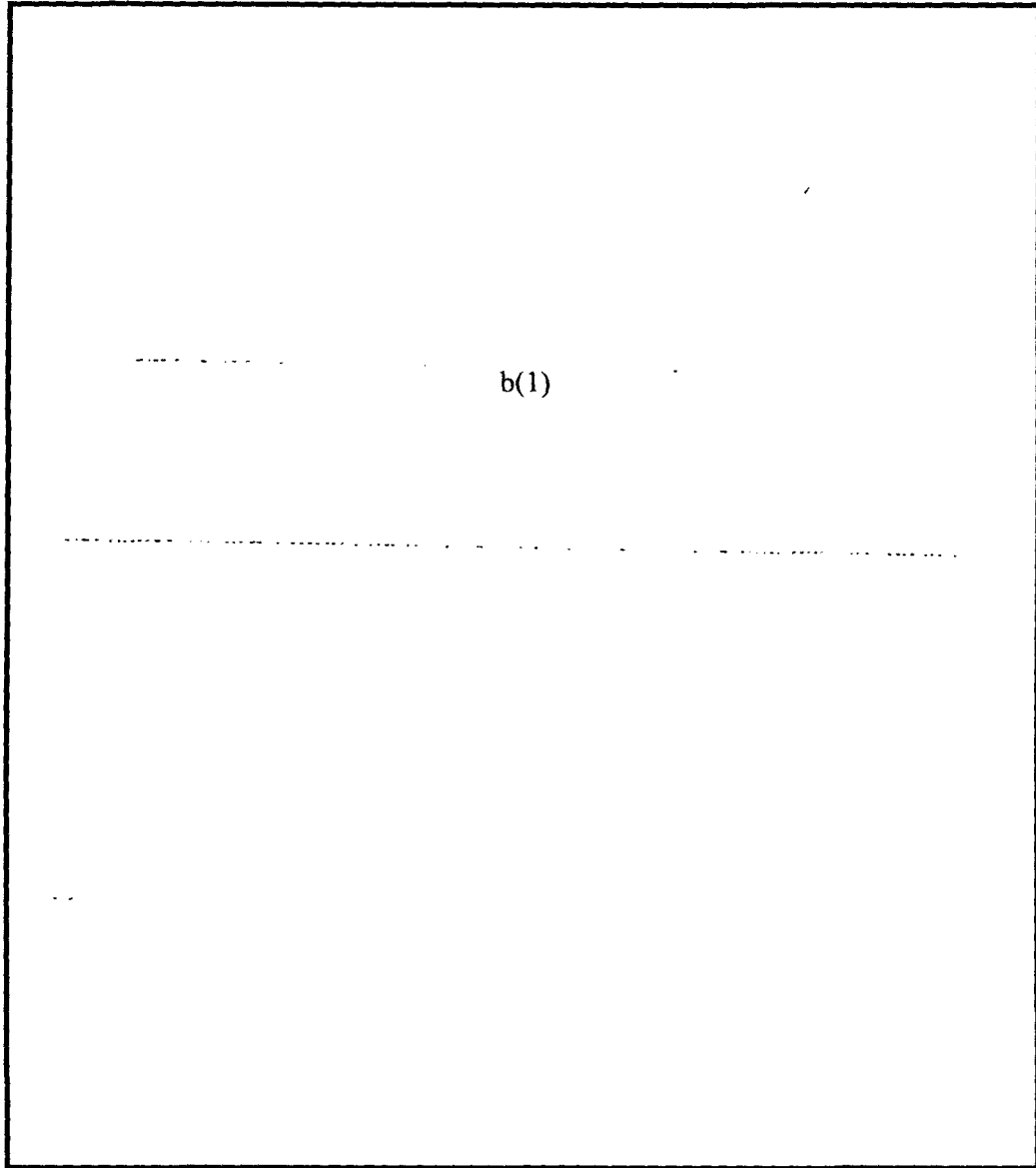
(C)

(C)

(C)

(C)

(C)



(u)

The USG is in the process of formulating its formal response to the EU proposal.

~~Confidential~~

[Handwritten scribbles]

[Handwritten scribbles]

[Redacted]

b(5)

[Redacted]

b(1)

[Handwritten scribbles]

[Redacted]

b(5)

[Redacted]

b(1)

[Redacted]

b(5)

[Redacted]

b(1)

[Handwritten scribbles]

[Redacted]

b(5)

[Redacted]

b(1)

[Redacted]

b(5)

[Redacted]

b(1)

[Redacted]

b(5)

[Redacted]

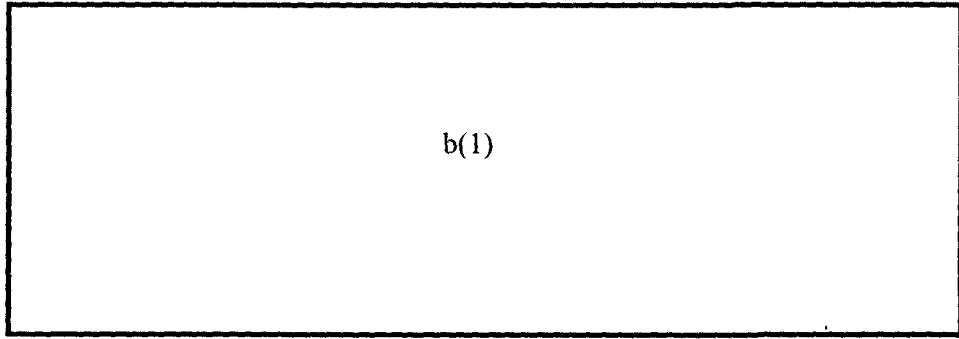
b(1)

[Redacted]

b(5)

~~Confidential~~

(c) •



~~Confidential~~



Homeland Security

June 26, 2006

Memorandum

TO: [REDACTED] b(5)

FROM: [REDACTED] b(5)

RE: Passenger Name Records and Law Enforcement Information Sharing - Negotiations With The European Union

Purpose

To provide you with background information on the Passenger Name Record (PNR) issue and related developments concerning law enforcement information sharing with the European Union (EU) in preparation for a mid-July "un-DC."

Summary

Before September 11, the 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. This information - name, contact information, and the like - was drawn from information supplied to the airline as part of the reservation process. DHS uses the information to screen for no-fly violators and terrorist suspects before the plane takes off, protecting against midflight hijackings and bombings.

For flights between Europe and the U.S., the data must be made available from Europe. EU law has long prohibited the commercial export of personal data to countries whose legal protections are not "adequate" in the view of European data protection authorities. While the U.S. has many privacy laws, it does not have an overarching data protection regime that corresponds to every aspect of European law. It has therefore been viewed as "inadequate" by European standards, and commercial data transfers to the U.S. have long been restricted. European airlines feared (with reason) that European data protection agencies would view the PNR transfers in the same light and would impose fines and other penalties on airlines that provided the PNR data to the U.S. Government.

To ease these fears, 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 is accompanied by a determination that US law is "adequate" by European standards as long as the US adheres to numerous detailed prescriptions worked out with EU negotiators (but unilaterally implemented by DHS).

[REDACTED] b(5)

Handwritten notes:
The EU...
...
...

[REDACTED]

b(5)

The PNR Agreement was also controversial in Europe. It was challenged by the European Parliament as insufficiently protective of EU privacy rights. On May 30 the European Court of Justice (ECJ) struck down the Agreement. But it chose a ground that was highly procedural – the equivalent under US law of the Supreme Court ducking a Fourth Amendment challenge by finding a law invalid because it exceeded Congress's Commerce Clause power. Under EU law, commercial issues fall within the jurisdiction of the EU as part of its "First Pillar" authority. This is the authority that the EU relied on in entering the Agreement. The ECJ, however, held that the US wanted PNR data for law enforcement and public security reasons. Law enforcement and public security are only partly within the EU's authority; they fall under the "Third Pillar," where the authority of EU central institutions (the Commission, Parliament and Court of Justice) is more limited and more authority is left to the Member States. Because the agreement was entered under the wrong authority, the Court ruled it invalid but delayed the effective date of its decision until September 30 in the hope that the jurisdictional problem could be quickly solved. To cure the problem, the EU plans to seek authority from the Member States to renegotiate the PNR Agreement under the Third Pillar. The Commission has portrayed this as a technical change that would put the same agreement back in place, albeit under a different legal authority.

b(1)

b(1)

b(1)

• BE can share PNR data with other law enforcement agencies, on a case-by-case basis, and only for the purpose of combating terrorism and serious transnational crimes.



Background

(U)

Two converging events in Europe – the recent European Court of Justice decision on the legality of the EC-US PNR Agreement and a draft EU Framework Decision on Exchange of Criminal Data -- have major implications for US law enforcement and security.

~~(S)~~
(C)
1.4(d)

b(1)

(U)

The most significant of these limitations, from our perspective are the following:

~~(S)~~
(C)
1.4(d)

b(1)

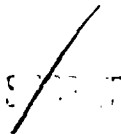
(e)

~~(S)~~

(C)

1.4(d)

b(1)



/

(e) [Redacted] b(1)

(e) [Redacted] b(1)

(e) [Redacted] b(1)

(c) 14(a)

(s)

(e)

(e)

[Redacted] b(1) →

/

(V) **The ECJ PNR Case.** The Agreement was no less controversial in Brussels. Disturbed over what it viewed as an attack on personal privacy and its own authority, the European Parliament (EP) filed two suits in the European Court of Justice (ECJ) challenging the information sharing arrangement.

(C)
1.4(b)
(4)
(U)

b(1)

(C)
1.4(d)

b(1)

(C) 1.4(b)(4)

ST



(c)

b(1)

(c)

b(1)

(c)

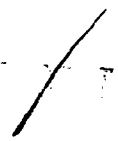
b(1)

(c)

2

(c)

b(1)



b(1)

b(5)

b(1)

If adopted, the Draft Decision could conflict with a number of binding and non-binding information sharing arrangements that the United States has signed. For example, we have signed a 2003 Mutual Legal Assistance Agreement (MLAA) with the European Union and a 2001 information sharing agreement with Europol (the EU-level police agency); with respect to member states, we signed a 2003 MLAA with Germany, which builds on numerous other MLAs already in force with other EU member states. The United States also has many executive agreements and memoranda of understanding with member states under which critical information is currently being shared. Under EU law, directives supersede bilateral treaties and agreements and member states must conform their existing agreements with the directive.

5/

(C)
1.4(d)

b(1)

(C)
1.4(d)

b(1)

(C)
1.4(a)

b(1)

(C)
1.4(a)

b(1)

(u)

¹² Conversely, Paragraph 34 of the Undertakings allows for the exchange of PNR for public health purposes and neither the Commission or the Article 29 Committee have challenged the DIIS-HHS MOU.

(u)

¹³ Unlike in 2003, this risk is present now because the Court has conclusively ruled that the transfer of PNR data is a law enforcement matter. While European integration has been the greatest in areas associated with the Common Market, law enforcement and public security is a relatively new area of activity at the community level and many responsibilities still fall to the EU Member States. The ECJ firmly placed PNR in the area of law enforcement and public security, and as result, any actions taken in this area are likely to set precedents for further community involvement in other law enforcement matters.

5/



(S)

b(1)

(S)

b(1)

Conclusion

(S)

The USG has a paramount interest in ensuring that law enforcement and border control information continues to flow to the United States. In creating the Information Sharing Environment we are working to break down walls that restrict the sharing of information between Federal agencies.

(S)

The PNR Agreement that the US signed with the EU in 2004 is an example of the old-style artificial limitation. We entered into the PNR Agreement based upon the EU's argument that the export of commercial information was subject to special restrictions under EU law. The European Court of Justice has now held that the information is law enforcement information, not commercial information, so that the rationale for the agreement has now dissolved.

(S)

b(1)



DISCUSSION DOCUMENT
Analysis of United States Interests in the U.S.-EU PNR dialogue
Department of Homeland Security

July 13, 2006

Purpose

To provide you with background information on the Passenger Name Record (PNR) issue and related developments concerning law enforcement information sharing with the European Union (EU) in preparation for a mid-July "un-DC."

Summary

Before September 11, the 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 uses the information to screen for no-fly violators and terrorist suspects prior to arrival, and even before the plane takes off¹, protecting against mid-flight hijackings and bombings.

For flights between Europe and the U.S., the data must be made available from European air carriers. EU law has long prohibited the commercial export of personal data to countries whose legal protections have not been deemed "adequate" in the view of European data protection authorities. While the U.S. has many privacy laws, it does not have an overarching data protection regime that corresponds to every aspect of European law. It has therefore been viewed as "inadequate" by European standards, and commercial data transfers to the U.S. have long been restricted by the lack of a broad adequacy finding. While the EU lacks similar requirements for the transfer of law enforcement information between the EU and third parties, a Framework Decision is currently being considered that would mirror the requirements applied in the commercial realm.

[Redacted]

b(5)

[Redacted]

b(1)

¹ CBP may automatically access 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 begin to be generated. In some cases, particularly 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.

(c)(1)
Not

(U)

b(1)

The PNR Agreement was also controversial in Europe. It was challenged by the European Parliament as insufficiently protective of EU privacy rights. On May 30 the European Court of Justice (ECJ) struck down the Agreement. But it chose a ground that was highly procedural – the equivalent under US law of the Supreme Court ducking a Fourth Amendment challenge by finding a law invalid because it exceeded Congress's Commerce Clause power. Under EU law, commercial issues fall within the jurisdiction of the EU as part of its "First Pillar" authority. This is the authority that the EU relied on in entering the Agreement. The ECJ, however, held that the US wanted PNR data for law enforcement and public security reasons. Law enforcement and public security are exempt from the EU's commercial data protection laws and are only partly within the EU's authority. Instead, they fall under the "Third Pillar," where the authority of EU central institutions (the Commission, Parliament and Court of Justice) is more limited and more authority is left to the Member States. This finding by the Court also eliminates the uncertainty that led to the signing of the agreement in the first place, specifically the fear that some Member States might bring action against air carriers under the commercial legal framework.

(U)

Because the agreement was entered under the wrong authority, the Court ruled it invalid but delayed the effective date of its decision until September 30 in the hope that the jurisdictional problem could be quickly solved. To cure the problem, the EU has obtained authority from the Member States to renegotiate the PNR Agreement under the Third Pillar. As required by the Agreement, the EU also notified 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. The USG received a proposed replacement text from the Finnish Presidency on July 19th, although Commission officials have indicated that this draft may not be final.³ Commission representatives have portrayed their proposal as a technical change that would put the same agreement back in place, albeit under a different legal authority.

(U)

b(1)

(U)

² 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. Broader access would allow other agencies to look for patterns in the travel of individuals not deemed to be high risk and to assess connections between passengers. ICE, for example, has expressed its frustration over losing access to this information.

(U)

³ Both the Departments of State and Homeland Security have a number of questions regarding the legal impact of a variety of wording choices, including references to the European Convention on Human Rights. Additional policy analysis is underway and our response will be driven by the decisions of the Deputies.

(S)

b(1)

(S)

b(1)

Background (U)

(U)

Two converging events in Europe – the recent European Court of Justice decision on the legality of the EU-US PNR Agreement and a draft EU Framework Decision on Exchange of Criminal Data -- have major implications for US law enforcement and security.

(U)

The EU-US PNR Agreement. As noted, in May 2004, after substantial negotiations, the Department of Homeland Security entered into an agreement relating to the sharing of PNR information collected by air carriers flying to the United States from Europe. The Agreement was intended to resolve a perceived conflict between EU law (which limits the sharing of personal information collected by commercial entities with governmental entities) and US law (which required the collection and dissemination of PNR data). Central to the Agreement was a set of Undertakings made by Customs and Border Protection (CBP) regarding how it would treat the PNR data transmitted to it.⁴ Several of the limitations in those Undertakings significantly restrict US opportunities to use information for investigative and law enforcement purposes.

(C)

b(1)

(C)

b(1)

(S)

b(1)

(V)

The ECJ PNR Case. The Agreement was no less controversial in Brussels. Disturbed over what it viewed as an attack on personal privacy and its own authority, the European Parliament (EP) filed two suits in the European Court of Justice (ECJ) challenging the information sharing arrangement.

(V)

On May 30, 2006, the ECJ issued its opinion in the lawsuits. The opinion did not address the merits of the EU-US PNR Agreement or the role of the Parliament. Rather, the decision turned on the lack of competence of the Commission and Council to enter into the Agreement in the first instance. The EU had based its authority on the so-called "First Pillar," which allows the EU to regulate trade and commercial matters. The ECJ held (as the US had argued earlier) that the requirement that PNR data be sent to the US was a law enforcement and national security matter. Such transfers, the court held, were excluded from the data protection directive governing commercial data exports. If they are to be regulated, the court implied, it would have to be done under the "Third Pillar."⁸

(V)

⁶ 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."

(C/S)
H/O

b(1)

(u)

⁸ Acting under the First Pillar, the EU has also entered into a PNR sharing agreement with Canada. In light of the EU's determination that the US Undertakings provided "adequate" privacy protections, the EU-Canada agreement authorizes Canada to share PNR data received from the EU with the US. Even though the ECJ has struck down the EU-US agreement, the EU contends that its similar agreement with Canada remains in effect. Some Canadian government

That is what the EU proposes to do. It has obtained authority from its Member States to erect substantially the same agreement on a new foundation. In order to meet the European Court of Justice deadline the Commission will seek to codify its position over the next couple of weeks and then will call for agreement on the new arrangement by September 30.

b(1)

EU Proposals on Sharing Law Enforcement Information. If that were all that is at stake, this would be an interesting diplomatic and legal problem for DHS. But it is not. The PNR negotiations will be closely intertwined with a broader effort to establish restrictive, EU-wide rules for information sharing in the area of law enforcement. Last October the EU put forward two draft documents that concern data sharing and protection in the law enforcement context. They consist of a draft Framework Directive of the European Parliament and Council on the retention of data and a proposed Council decision on the protection of personal data in criminal matters.

b(5)

b(1)

b(1)

sources are concerned, however, that the absence of an "adequacy" finding (which is a First Pillar concept) may now have the effect of *prohibiting* US-Canada information sharing derived from EU-originated flights.

* For example, the Draft Decision contains provisions on time limits for retention of shared data, ensuring the accuracy of shared data, logging and audit trails, as well as restrictions limiting further use of the data to the original purpose for which it was first transmitted. In effect, it borrows heavily from the PNR Agreement and the Undertakings.

b(1)

(C)(S)(g)(i)
Mod

b(1)

(C)(S)(g)(i)
Mod

Communicable Diseases. One indicator of the extent to which EU data protection authorities prioritize the expansion of such roles over public safety concerns can be found in the European reaction to another US initiative relating to avian flu. If air passengers are exposed to a pandemic strain of avian flu, the government will need to locate all of the passengers and crew, quickly. So the Centers for Disease Control has proposed a rule requiring airlines to retain PNR for up to 60 days for that purpose. The top data protection authorities of Europe, known as the "Article 29 Working Party," have now decided that this sort of data retention violates EU privacy directives. If given effect, the Working Party's opinion would place air carriers legal jeopardy because of inconsistent

(a)

b(1)

(C)(S)(g)(i)
Mod

(v)

¹¹ The adequacy finding granted to the U.S. was specific to the transfer of PNR data and only extended to its transmission to CBP. The May 30th decision of the ECJ also annuls this decision by the Commission on the grounds that the Commission did not have the legal authority to grant it

(v)

¹² If adopted without the offered exemptions, the Draft Decision could conflict with a number of binding and non-binding information sharing arrangements that the United States has signed. For example, we have signed a 2003 Mutual Legal Assistance Agreement (MLAT) with the European Union and a 2001 information sharing agreement with Europol (the EU-level police agency); with respect to member states, we signed a 2003 MLAT with Germany, which builds on numerous other MLATs already in force with other EU member states. The United States also has many executive agreements and memoranda of understanding with member states under which critical information is currently being shared. Under EU law, directives supersede bilateral treaties and agreements and member states must conform their existing agreements to the directive.

~~SECRET~~

For Official Use Only

legal régimes. It reflects a widespread EU view that privacy trumps even the critical public health interests of the United States.¹³

Analysis & Recommendation (u)

(C)

b(1)

(S)

b(1)

(C)

b(1)

(S)

b(1)

(u)

¹³ Conversely, Paragraph 34 of the Undertakings allows for the exchange of PNR for public health purposes and neither the Commission nor the Article 29 Committee have challenged the DHS-HHS MOU.

(u)

¹⁴ Unlike in 2003, this risk is present now because the Court has conclusively ruled that the transfer of PNR data is a law enforcement matter. While European integration has been the greatest in areas associated with the Common Market, law enforcement and public security is a relatively new area of activity at the community level and many responsibilities still fall to the EU Member States. The ECJ firmly placed PNR in the area of law enforcement and public security, and as result, any actions taken in this area are likely to set precedents for further community involvement in other law enforcement matters.

~~SECRET~~

~~SECRET~~

For Official Use Only

Conclusion (u)

(C)

b(1)

(S)

b(1)

(U)

The USG has a paramount interest in ensuring that law enforcement and border control information continues to flow to the United States. In creating the Information Sharing Environment we are working to break down walls that restrict the sharing of information between Federal agencies.

(U)

The PNR Agreement that the US signed with the EU in 2004 is an example of the old-style artificial limitation. We entered into the PNR Agreement based upon the EU's argument that the export of commercial information was subject to special restrictions under EU law. The European Court of Justice has now held that the information is law enforcement information, not commercial information, so that the rationale for the agreement has now dissolved.

(S)

b(1)

(U)

¹⁵ Excluding Canada and Mexico, flights originating in these five countries comprise nearly a quarter of all international flights arriving in the United States. In terms of global traffic, flights arriving from the UK rank third (after Canada and Mexico). Germany is 6th; France 9th; the Netherlands 10th; and Italy 17th.

~~SECRET~~

For Official Use Only

(c)

b(1)

Attachments

- (c) A. Excerpt from EU Data Protection Directive 95/46/EC (24 October 1995)
- (c) B. Excerpt from Draft Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matter (October 2005)

✓