



# Homeland Security

*Privacy Office*

December 28, 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 seventeenth 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 7<sup>th</sup> 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 7 responsive documents, consisting of 28 pages, which were being held for classification review. I have determined that 4 of those documents, consisting of 19 pages, are releasable in part, and 3 documents, consisting of 9 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 properly classified information, internal administrative trackings, deliberative material, legal opinions, attorney-client privileged information, law enforcement information, and homeland security information. I am withholding this information pursuant to Exemptions 1, 2, 5, and 7(E) of the FOIA, 5 USC §§ 552 (b)(1), (b)(2), (b)(5), and (b)(7)(E).

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 2(low) exempts from disclosure records that are related to internal matters of a relatively trivial nature, such as internal administrative trackings. 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.

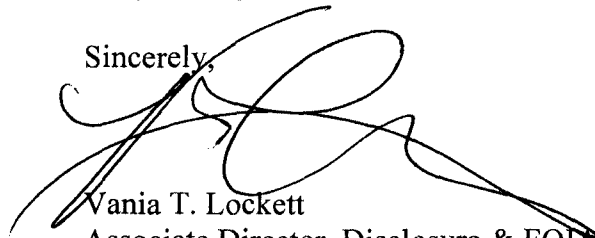
FOIA Exemption 5 protects from disclosure those inter- or intra-agency documents that are normally privileged in the civil discovery context. The deliberative process privilege protects the integrity of the deliberative or decision-making processes within the agency by exempting from mandatory disclosure 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.

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.

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 'Vania T. Lockett', written over the word 'Sincerely,'.

Vania T. Lockett  
Associate Director, Disclosure & FOIA Operations

Enclosures: As stated, 19 pages

UNCLASSIFIED

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



**Homeland  
Security**

Via Electronic Delivery (u)

[Mr. Jonathan Faull  
Director General  
European Commission  
Brussels, Belgium]

[Mr. Markus Laurent  
Deputy Director General  
Ministry of Foreign Affairs  
Helsinki, Finland]

(u) [Dear Jonathan and Markus:]

(u) This letter is intended to set forth our understandings with regard to the interpretation of a number of provisions of the Passenger Name Record (PNR) Undertakings issued on May 11, 2004 by the Department of Homeland Security (DHS) [

b5

] we look forward to further reviewing these and other issues in the context of future discussions toward a comprehensive, reciprocal agreement based on common principles.

Sharing and Disclosure of PNR (u)

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

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

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

UNCLASSIFIED

①

UNCLASSIFIED

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

(u) DHS will therefore facilitate the disclosure (without providing unconditional electronic access) of PNR data to U.S. government authorities exercising a counter-terrorism function that need PNR for the purpose of preventing or combating terrorism ~~E 65~~ (including threats, flights, individuals, and routes of concern) that they are examining or investigating. DHS will ensure that such authorities respect comparable standards of data protection to that applicable to DHS, in particular in relation to purpose limitation, data retention, further disclosure, awareness and training, security standards and sanctions for abuse, and procedures for information, complaints and rectification. Prior to commencing facilitated disclosure, each receiving authority will confirm in writing to DHS that it respects those standards. DHS will inform the EU in writing of the implementation of such facilitated disclosure and respect for the applicable standards before the expiry of the Agreement.

Early Access Period for PNR (u)

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

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

(u) DHS will move as soon as practicable to a push system for the transfer of PNR data in accordance with ~~E 65~~ Undertakings and will carry out no later than the end of 2006 the necessary tests for at least one system currently in development if DHS's technical requirements are satisfied by the design to be tested. Without derogating from ~~E 65~~ Undertakings and in order to avoid prejudging the possible future needs of the system any filters employed in a push system, and the design of the system itself, must permit any PNR data in the airline reservation or departure control systems to be pushed to DHS, in exceptional circumstances where augmented disclosure is strictly necessary to address a threat to the vital interests of the data subject or other persons.

UNCLASSIFIED

Data Retention (u)

- (u) Several important uses for PNR data help to identify potential terrorists: even data that is more than 3.5 years old can be crucial in identifying links among terrorism suspects. The Agreement [ b5 ] of whether and when to destroy PNR data collected [ b5 ] and questions [ b5 ] will be addressed by the United States and the European Union as part of future discussions.

The Joint Review (u)

- (u) Given the extensive joint analysis of the Undertakings conducted in September 2006 and the expiration of the agreement prior to the next Joint Review, the question of how and whether to conduct a joint review in 2007 will be addressed during the discussions regarding a future agreement.

Data Elements (u)

- (u) The frequent flyer field may offer addresses, telephone numbers, email addresses; all of these, as well as the frequent flyer number itself, may provide crucial evidence of links to terrorism. Similarly, information about the number of bags carried by a passenger may have value in a counterterrorism context. The Undertakings authorize DHS to add data elements to the 34 previously set forth in Attachment "A" of the Undertakings, if such data is necessary to fulfill the purposes set forth in paragraph 3.
- (u) With this letter the U.S. has consulted under Paragraph 7 with the EU in connection with item 11 of Attachment A regarding DHS's need to obtain the frequent flier number and any data element listed in Attachment A to the Undertakings wherever that element may be found.

Vital Interests of the Data Subject or Others (u)

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

Sincerely yours.

Stewart Baker  
Assistant Secretary for Policy

~~CONFIDENTIAL~~

[Sharing and] Disclosure of PNR (u)

(u) US: 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." Following this enactment, the President issued Executive Order 13388, directing that DHS and other agencies "promptly give access to the terrorism information to the head of each other agency that has counterterrorism functions."

(u) EU: Following the Intelligence Reform and Terrorism Prevention Act of 2004, the President issued Executive Order 13388, directing that DHS and other agencies "promptly give access to [...] terrorism information to the head of each other agency that has counterterrorism functions."

(u) [ b5 ]

(u) US E [ b5 ]

(c/fgi-mod) [ b1 ]  
(c/fgi-mod) [ b1 ]  
(c/fgi-mod) [ b1 ]  
(c/fgi-mod) [ b1 ]

[ ]  
[ ]  
[ ]

~~CONFIDENTIAL~~

Derived from: Schneider  
MFE  
Declass: 31 Dec 2016

~~CONFIDENTIAL~~

(c/fgi-MOD) [o]

b1

[

(u) US: C

[

b5

]

~~CONFIDENTIAL~~



~~CONFIDENTIAL~~

Sharing and Disclosure of PNR (u)

(u) US: 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." Following this enactment, the President issued Executive Order 13388, directing that DHS and other agencies ["promptly give access to . . . terrorism information to the head of each other agency that has counterterrorism functions" and establishing a mechanism for implementing the information sharing environment.]

(u) [ b5 ]

(u) US: [ b5 ]

(C) [ b1 ]

(C) [ b1 ]

(u) [ b5 ]

~~CONFIDENTIAL~~

Derived from: SCHMS, O&E  
MFC

Declass: 31 Dec 2016

~~SECRET~~  
FOR OFFICIAL USE ONLY

Attachment D

[ b2 ]

INFORMATION

MEMORANDUM FOR: Stewart Baker, Assistant Secretary for Policy (u)  
THROUGH: Paul Rosenzweig, Acting Assistant Secretary, PDEV and  
Councilor to the Assistant Secretary for Policy (u)  
FROM: PNR Working Group (u)  
SUBJECT: Summary of potential changes to seek in the PNR Undertakings (u)

Purpose (u)

(u) In anticipation of future negotiations with the EU on the PNR arrangement, below is an assessment of areas of the Undertakings DHS should seek to change in the US-EU PNR arrangement. [

[

b5

]

(c)

(c)

[

b1  
b5

]

Rex

Background (u)

~~FOR OFFICIAL USE ONLY~~

~~SECRET~~

(4)

CLASSIFIED BY: SCHNEIDER MFC

DECLASS :

11 DEC 2031

~~FOR OFFICIAL USE ONLY~~

(u)

[

b5  
b2H  
b7E

]

(u)

(C)

[

b1  
b5  
b2H  
b7E

]

(u)

[

b5  
b2H  
b7E

]

~~FOR OFFICIAL USE ONLY~~

~~CONFIDENTIAL~~

[

b5

]

Discussion (u)

(u)

[

b5  
b2H  
b7E

]

(u)

(c)

[

b1  
b5  
b2H  
b7E

]

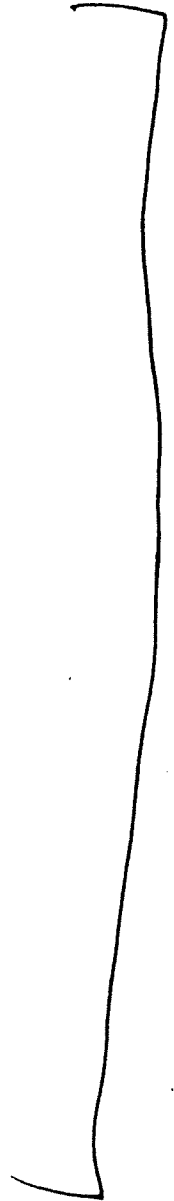
(c)

(c)

[ b5

]

(C)



b1  
b5  
b2H  
b7E

(S)

(S)

(S)

(Cat-  
Mod)

~~SECRET~~  
FOR OFFICIAL USE ONLY

(S) [

b1  
b5  
b2H  
b7E

]

**Attachments:**

1. Detailed Assessment of Critical Issues
2. List of Sensitive Terms

~~FOR OFFICIAL USE ONLY~~

~~SECRET~~

Attachment 1: Detailed Assessment of Critical Issues (U)

(U)

(U)

(C)

(S) (U)

b5  
b2H

b7E

b1  
b5  
b2H  
b7E

b1

FOR OFFICIAL ~~USE~~ ONLY

(u)

(u)

(u)

b5  
b2H  
b7E

(u)

(u)

(u)

(u)

FOR OFFICIAL ~~USE~~ ONLY



(C) (Eqj-10D).

[	b5	]
[	b1 b5 b2H b7E	]

(u).

(u)

b5  
b2H  
b7E

(C)

b1 b5 b2H b7E

[

b5

FOR OFFICIAL USE ONLY

(c) [

b1 b5 b2H b7E

]

(u) [

b5  
b2H  
b7E

]

(c) [

b1  
b5  
b2H  
b7E

]

(u) [

b5

]

FOR OFFICIAL USE ONLY

~~FOR OFFICIAL USE ONLY~~

Attachment 2

b1  
  
b2H  
b7E

C/FCI-MOD

~~CONFIDENTIAL~~

~~FOR OFFICIAL USE ONLY~~

~~CONFIDENTIAL~~

b1  
b2H  
b7E

(C/FOUO-MOD)

~~FOR OFFICIAL USE ONLY~~

~~CONFIDENTIAL~~

FOR OFFICIAL ~~USE~~ ONLY

~~CONFIDENTIAL~~

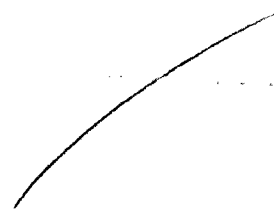
b1  
b2H  
b7E

FOR OFFICIAL ~~USE~~ ONLY

C/FGHMOD

~~CONFIDENTIAL~~

~~FOR OFFICIAL USE ONLY~~



b1  
b2H  
b7E

(C/CAI-MOD)

~~FOR OFFICIAL USE ONLY~~

~~CONFIDENTIAL~~