U.S. Department of Homeland Security
Washington, D.C. 20528

Homeland Security

Privacy Office

July 13, 2007

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

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

Dear Ms. Hofmann:

Pursuant to the order of the court, this is our fourth 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.

Continued searches of the DHS components produced an additional 6 documents consisting of 22 pages of records responsive to your request. Of those 6 documents, I have determined that 1 document totaling 3 pages is releasable in its entirety, and 5 documents totaling 19 pages are releasable in part. The withheld information, which will be noted on the *Vaughn* index when

completed, consists of names, telephone numbers, email addresses, drafts, recommendations, legal opinions, Law Enforcement information, and homeland security information. I am withholding this information pursuant to Exemptions 2, 5, 6, and 7(E) of the FOIA, 5 USC §§ 552 (b)(2), (b)(5), (b)(6), 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.

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

Sincerely,

Vania T. Lockett
Associate Director, Disclosure & FOIA Operations

Enclosures: 22 pages

b(6)

From: Scardaville, Michael b2
Sent: Wednesday, June 14, 2006 8:48 AM
To: Baker, Stewart; Scardaville, Michael
Cc: Rosenzweig, Paul
Subject: Re: PNR Sensitivie Data

They were negotiated with the EU after the agreement and Undertakings were concluded. Typically they would be included in the open fields of a PNR by a carrier or travel agent. These fields typically function as a free-form space for comments and directions not covered by other fields.

It is definitely an interesting collection of terms!

Sent from my BlackBerry Wireless Handheld

-----Original Message-----
From: Baker, Stewart
To: Scardaville, Michael
CC: Rosenzweig, Paul
Sent: Wed Jun 14 08:30:36 2006
Subject: RE: PNR Sensitivie Data

Where did we get the list of free-form terms we would not look for?
It's a weird assortment. Are these terms that actually appear in reservation systems?
Did the EU suggest them?

-----Original Message-----
From: Scardaville, Michael [mailto b2
Sent: Tuesday, June 13, 2006 1:09 PM
To: Baker, Stewart
Cc: Rosenzweig, Paul
Subject: PNR Sensitivie Data
Importance: High

Stewart,

Per your request, attached is a list of the sensitive data we have agreed not to access.

Mike b2

-----Original Message----- b6 b2
From:
Sent: Tuesday, June 13, 2006 12:00 PM
To: Scardaville, Michael
Subject: Re: pnr

Here is the sensitive data list that was agreed upon....

(See attached file: Sensitive Data Attachment.doc)

b6

OFFICE OF FIELD OPERATIONS
PASSENGER AUTOMATION PROJECTS OFFICE
WASHINGTON, DC 20229

b2

Doc #1

b6

From: Scardaville, Michael b2
Sent: Tuesday, June 13, 2006 1:09 PM
To: Baker, Stewart
Cc: Rosenzweig, Paul
Subject: PNR Sensitivie Data

Importance: High

Attachments: Sensitive Data Attachment.doc

Sensitive Data Attachment.doc ...

Stewart,

Per your request, attached is a list of the sensitive data we have agreed not to access.

Mike b2

-----C
From: b6 b2
Sent: Tuesday, June 13, 2006 12:00 PM
To: Scardaville, Michael
Subject: Re: pnr

Here is the sensitive data list that was agreed upon....

(See attached file: Sensitive Data Attachment.doc)

b6

OFFICE OF FIELD OPERATIONS
PASSENGER AUTOMATION PROJECTS OFFICE
WASHINGTON, DC 20229

b2

Attachment "C"

"Sensitive Data"

Codes

Description	Data Field type	Code

b7E
b2 high

b7E
b2 high

Terms

b7E
b2 high

b7E
b2 high

b7E
b2 high

[redacted]

* * * WARNING * * *

Access to Reservation/Departure Control System Data (PNR Data) is o
authorized for data which includes flights to, out of, or through the Un
Users of this system are not authorized to request or view any flight inf
flight list, or PNR Data without a NEXUS to the United States. System
usage is monitored. Violators will have their access suspended.

This system and data is for official use only and is Law Enforcement Se

To start ResMon, please indicate your agreement by clicking on the "I Agree" but

I Agree | I do NOT Agree

b7E
b2 high

Done

Doc #2

General Privacy Protections for Passenger Name Record (PNR) Data

PNR and General Privacy at the U.S. Border

- Although U.S. law permits CBP to access PNR data in an electronic format, most data elements contained in PNR data can be obtained by CBP upon examining a data subject's airline ticket and other travel documents pursuant to its normal border control authority, upon arrival of the passenger in the U.S. Electronic collection of PNR, however, substantially enhances CBP's ability to facilitate legitimate travelers and to conduct the necessary risk assessments, often prior to the boarding of passengers, thereby also increasing aviation security.

Computer System Security at CBP

- Authorized CBP personnel generally obtain access to PNR through the closed CBP intranet system which is encrypted end-to-end and the connection is controlled by the CBP National Data Center.

- PNR data stored in the CBP database is limited to "read only" access by authorized personnel, meaning that the substance of the data may be programmatically reformatted, but will not be substantively altered in any manner by CBP once accessed from an air carrier's reservation system.

- Details regarding access to information in CBP databases (such as who, where, when (date and time) and any revisions to the data) are automatically recorded and routinely audited by the Office of Internal Affairs to prevent unauthorized use of the system.

- Only certain officers, employees or information technology contractors (under CBP supervision) who have successfully completed a background investigation, have an active, password-protected account in the CBP computer system, and have a recognized official purpose for reviewing PNR data, may access PNR data through that system. Access by "contractors" to any PNR data contained in the CBP computer systems is for purposes of assisting in the maintenance or development of CBP's computer system.

- CBP officers, employees and contractors are required to complete security and data privacy training, including passage of a test, on a biennial basis. CBP system auditing is used to monitor and ensure compliance with all privacy and data security requirements.

- Unauthorized access by CBP personnel to air carrier reservation systems or the CBP computerized system which stores PNR is subject to strict disciplinary action (which may include termination of employment) and may

Doc # 3

result in criminal sanctions being imposed (fines, imprisonment of up to one year, or both) (see title 18, United States Code, section 1030).

- CBP policy and regulations also provide for stringent disciplinary action (which may include termination of employment) to be taken against any CBP employee who discloses information from CBP's computerized systems without official authorization (title 19, Code of Federal Regulations, section 103.34).

U.S. Laws Applicable to Treatment of PNR Data

- General Policy: CBP treats PNR information regarding persons of any nationality or country of residence as law enforcement sensitive, confidential personal information of the data subject, and confidential commercial information of the air carrier, and, therefore, would not make disclosures of such data to the public, except as necessary to enforce U.S. law (e.g., criminal prosecution) or as otherwise required by law (e.g., pursuant to a court order).

- Freedom of Information Act: Public disclosure of PNR data is generally governed by the Freedom of Information Act (FOIA) (title 5, United States Code, section 552) which permits any person (regardless of nationality or country of residence) access to a U.S. federal agency's records, except to the extent such records (or a portion thereof) are protected from public disclosure by an applicable exemption under the FOIA.

  - Among its exemptions, the FOIA permits an agency to withhold a record (or a portion thereof) from disclosure:

    - ✓ where the information is confidential commercial information;
    - ✓ where disclosure of the information would constitute a clearly unwarranted invasion of personal privacy;
    - ✓ where the information is compiled for law enforcement purposes, to the extent that disclosure may reasonably be expected to constitute an unwarranted invasion of personal privacy or could reasonably be expected to interfere with enforcement proceedings.

    (See title 5, United States Code (U.S.C.), sections 552(b)(4), (6), (7)(C).)

  - CBP regulations (title 19, Code of Federal Regulations (CFR), section 103.12), which govern the processing of requests for information (such as PNR data) pursuant to the FOIA, specifically provide that (subject to certain limited exceptions in the case of requests by the data subject) the disclosure requirements of the FOIA are not applicable to CBP records relating to:

- ✓ confidential commercial information;
- ✓ material involving personal privacy where the disclosure would constitute a clearly unwarranted invasion of personal privacy; and
- ✓ information compiled for law enforcement purposes, where disclosure could reasonably be expected to constitute an unwarranted invasion of personal privacy or could reasonably be expected to interfere with enforcement proceedings.

CBP invokes these exemptions uniformly based on the character of the data, without regard to the nationality or country of residence of the subject of the data.

- ➢ Under the FOIA, any person may request access to their personal information which may be held by CBP. The procedures for making FOIA requests for CBP records are contained in section 103.5 of title 19 of the U.S. Code of Federal Regulations. Decisions by CBP to withhold a record (or part thereof) may be administratively and judicially challenged. (See title 5 U.S.C. section 552(a)(4)(B) and 19 CFR sections 103.7-103.9).

- The Privacy Act: Provides certain protections for personal data held by U.S. government agencies regarding U.S. citizens and lawful permanent residents. (title 5 U.S.C. section 552a.)

- Criminal penalties
  - ➢ Unauthorized Access: see above.
  - ➢ Unauthorized Disclosures: Criminal penalties (including fines, imprisonment of up to one year, or both) may be assessed against any officer or employee of the United States for disclosing records/information (such as PNR) obtained in the course of his employment, where such disclosure is not authorized by law (see title 18 U.S.C. sections 641, 1030, 1905).

- Department of Homeland Security's (DHS) Chief Privacy Officer: The DHS Chief Privacy Officer is required by statute to ensure that personal information is used in a manner than complies with relevant laws (see section 222 of the Homeland Security Act of 2002 (Public Law 107-296, dated November 25, 2002)). The Chief Privacy Officer is independent of any directorate within the Department of Homeland Security (CBP is an agency within DHS). The determinations of the Chief Privacy Officer are binding on the Department and may not be overturned on political grounds.

b6

From: Rosenzweig, Paul b2
Sent: Sunday, June 11, 2006 7:16 PM
To: Baker, Stewart
Subject: Fw: Undertakings b5

Mike's thoughts

Sent from my BlackBerry Wireless Handheld

-----Original Message-----
From: Scardaville, Michael
To: Rosenzweig, Paul
Sent: Sun Jun 11 18:59:12 2006
Subject: Re: b5 Undertakings

I just read on BB and it looks accurate.

A few points though:
1.

b5

I originally put a footnote to this affect, so our leadership is fore warned about this (I'm not endorsing the position, but want to make sure you, SB and up don't unknowingly diverge with the WH)

b5

2. I don't know that all of these provisions would be viewed as onerous by the Euros - afterall its what they said they needed to comply with their law.

b5

. This is, however, just conjecture on my part.

Finally, The Data Integrity Project is Visit's effort to make a better estimate of visa overstays. One of the things they look for is wether the individual was encountered entering.

b5, b7E, b2(high)

I'll start working on a more comprehensive memo when I get in tommorow.

Sent from my BlackBerry Wireless Handheld

-----Original Message-----
From: Rosenzweig, Paul
To: Scardaville, Michael
Sent: Sun Jun 11 16:44:48 2006
Subject: Fw: b5 Undertakings

Pls check for accuracy. Note need for bigger memo for Moscow and rewust for list of sensetive data
---
Sent from my BlackBerry Wireless Handheld

-----Original Message-----
From: Baker, Stewart

Doc # 4

To: Rosenzweig, Paul
Sent: Sun Jun 11 16:39:01 2006
Subject: FW: b5 Undertakings

O <<060607 Summary of Undertakings Issues (CBP cc comments 6-9-06).rh.clean.doc>> b6 could you check my changes over to make sure they are accurate? This is a pretty good memory jogger, but it isn't an advocacy memo. We do need something for Moscow, so I'll take it, but perhaps a cleanedup version could go to the Embassy for me or the Secretary. And we need a deadpan but devastating summary of the provisions, building on the tone/style of what I've added. Also, I still have not seen a list of the "sensitive" data we aren't allowed to see.

-----Original Message---
From: Rosenzweig, Paul b2
Sent: Sunday, June 11, 2006 11:33 AM
To: Baker, Stewart
Subject: Fw: b5 Undertakings

Stewart

A good first cut. More soon

P

Sent from my BlackBerry Wireless Handheld

-----O: .ge-----
From: b6 b6
To: Rosenzweig, Paul
CC: b6
Sent: Fri Jun 09 15:48:58 2006
Subject: RE: b5 Undertakings

T <<060607 Summary of Undertakings Issues (CBP cc comments 6-9-06).rh.doc>> he attached (with redlines/comments and clean) includes comments from b6 :<060607 Summary of Undertakings Issues (CBP cc comments 6-9-06).rh.clean.doc>> in, b6 and me - the only ones I got. (Although the redlined version looks scary, much of it is from just moving existing text around rather than a wholesale rewrite). Please give me a call or let me know if you think we've inadverently moved this away from answering Stewart's question and/or have otherwise done violence to the intent.

Thanks,

-- b6

Senior Counsel

Department of Homeland Security

Office of the General Counsel

NAC-4, Washington, D.C. 20528

b2

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: Rosenzweig, Paul
Sent: Friday, June 09, 2006 3:39 PM
To: (b)(6)
Subject: RE: (b)(5) Undertakings

Stewart would like to see final this weekend. Can you get to me before COB?

P

Paul Rosenzweig

(b)(2)

From: (b)(6)
Sent: Friday, June 09, 2006 11:45 AM
To: Scardaville, Michael; Rosenzweig, Paul
Cc: (b)(6)

Subject: RE: (b)(5) Undertakings

Happy to be the collector of any and all comments if you can get them to me by 3:00 today.
Thx,

(b)(6)

Senior Counsel

Department of Homeland Security

Office of the General Counsel

NAC-4, Washington, D.C. 20528

(b)(7)

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: Scardaville, Michael
Sent: Thursday, June 08, 2006 8:15 PM
To: Rosenzweig, Paul

66

Subject: RE: 65 Undertakings

Paul,

Attached is a draft of the memo on the 65 Undertakings. As we discussed, this is a quick list based on what CBP, OGC and Privacy submitted in February and other conversations. When I return Monday, I'll begin working with all cc'd to produce a more comprehensive assessment.

Everyone else,

I'm out of the office tomorrow (Friday), but please let Paul and I know if you have significant edits or issues. If there are a lot, can somebody volunteer to combine them (I don't know when I'll be able to get to a computer) and send Paul a completed draft?

Stewart requested this for his own edification and would like it before he leaves for Europe Sunday. He isn't expecting this document to be the final word on this issue.

Thanks and see you Monday.

Mike

62

From: Rosenzweig, Paul
Sent: Thursday, June 08, 2006 4:17 PM
To: Scardaville, Michael
Subject: 65 Undertakings

Mike

I know your plate is groaning, esp w/ the need to update briefers for S1's trip. But S1 has also asked for a memo on " 65 the Undertakings ...."

Maybe tomorrow?

Sorry

P

Paul Rosenzweig

Counselor to the Asst. Secy. (Policy Directorate) and

Acting Assistant Secretary for Policy Development

Dept. of Homeland Security

Washington, DC 20528

Ph: 62

E:

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

Homeland Security

June 13, 2007

Deleted: June 11, 2006
Deleted: June 9, 2006

INFORMATION

MEMORANDUM FOR: Stewart Baker, Assistant Secretary for Policy

THROUGH: Paul Rosenzweig, Acting Assistant Secretary, PDEV and Councilor to the Assistant Secretary for Policy

FROM: Michael Scardaville, Special Assistant/International Policy Advisor

SUBJECT: Summary of potential changes to seek in the PNR Undertakings

Purpose

Per your request, below is a preliminary summary of areas of the Undertakings DHS may want to consider changing. I intend to work with CBP, OGC, TSA and Privacy to address these issues in more detail next week. My goal is provide you with a prioritized and justified list of changes to guide an eventual dialogue with the Europeans.

Background

b5

b5

In addition, some requirements, such as the audit standards, actually improved the overall operation of the program and others reflect existing policy (i.e., redress opportunities).

Discussion

Likely Top Priorities:

b5

Doc # 5

b5

Additional Issues:

b5
b7E
b2 high

b5
b7E
b2 high

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

Homeland Security

June 13, 2007

Deleted: June 9, 2006

INFORMATION

MEMORANDUM FOR: Stewart Baker, Assistant Secretary for Policy

THROUGH: Paul Rosenzweig, Acting Assistant Secretary, PDEV and Councilor to the Assistant Secretary for Policy

FROM: Michael Scardaville, Special Assistant/International Policy Advisor

SUBJECT: Summary of potential changes to seek in the PNR Undertakings

Purpose

Per your request, below is a preliminary summary of areas of the Undertakings DHS may want to consider changing. I intend to work with CBP, OGC, TSA and Privacy to address these issues in more detail next week. My goal is provide you with a prioritized and justified list of changes to guide an eventual dialogue with the Europeans.

Background

b5

In addition, some requirements, such as the audit standards, actually improved the overall operation of the program and others reflect existing policy (i.e., redress opportunities).

Discussion

Likely Top Priorities:

b5

b5

Doc # 6

b5
b7E
b2 high

b5

b6

b5

b5

PM 66

b5

b5