



Homeland Security

Privacy Office, Mail Stop 0550

March 19, 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 twenty-third 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 208 responsive documents, consisting of 1059 pages, which were being held for possible classification. I have determined that 1 document, consisting of 3 pages, is releasable in its entirety, 198 documents, consisting of 1008 pages, are releasable in part, and 9 documents, consisting of 48 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, names, telephone numbers, email addresses, deliberative material, legal opinions, law enforcement information, and homeland security information. I am withholding this information pursuant to Exemptions 1, 2, 5, 6, and 7(E) of the FOIA, 5 U.S.C. §§ 552 (b)(1), (b)(2), (b)(5), (b)(6), and (b)(7)(E).

We also completed our review of 2 responsive documents, consisting of 6 pages, that were referred to the Department of State (DOS) for releasability review. I have determined that those documents are withholdable in their entirety. The withheld information, which will be noted on the *Vaughn* index when completed, consists of predecisional and deliberative material. I am withholding this information pursuant to Exemption 5 of the FOIA, 5 U.S.C. § 552 (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 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.

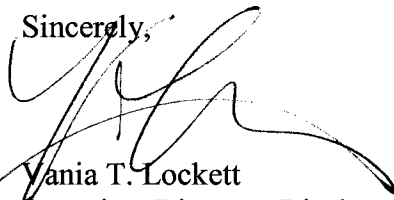
FOIA Exemption 6 exempts from disclosure records the release of which would cause a clearly unwarranted invasion of personal privacy. Weighed against the privacy interest of the individuals is the lack of public interest in the release of their personal information and the fact that the release adds 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 insofar as it relates to the remaining 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 'Y. Lockett', written over a horizontal line.

Yania T. Lockett
Associate Director, Disclosure & FOIA Operations

Enclosures: As stated, 1,011 pages

UNCLASSIFIED

May 14, 2007

Dear Member of the European Parliament:

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

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

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

One of these tools is Passenger Name Record (PNR) data, which is a limited set of information [b5] traveling between Europe and the United States. PNR data, used in combination with passenger manifest data, allows U.S. officers to check passenger names and other basic information against lists of known or suspected terrorists and criminals [b5]

Combined with other intelligence, we [b5] use PNR data to check for links that might reveal unknown terrorist connections, such as a traveler who has provided contact information overlapping with a known terrorist. It is our ability to identify these hidden links that has made PNR so valuable to our counterterrorism efforts and the reason it is imperative [b5]

Deleted: [b5]

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

- In June 2003, using PNR data and other [b5] one of our inspectors at Chicago's O'Hare airport pulled aside an individual for secondary inspection and questioning. When the secondary officers weren't satisfied with his answers they took his fingerprints and denied him entry to the United States. The next time we saw those fingerprints - or at least parts of them - they were on the steering wheel of a suicide vehicle that blew up and killed 132 people in Iraq.
- In January 2003, Customs and Border Protection (CBP) officers in Miami used PNR to disrupt an internal conspiracy within an airline that was smuggling

Deleted: [b5]

000364

1

UNCLASSIFIED

245

cocaine between Venezuela and Miami. A corrupt ticket counter agent would identify low risk travelers (typically families) and add an additional bag to their reservation after they departed the ticket counter. This bag would be filled with cocaine. Corrupt airline employees in Miami plotted to remove the added bags from circulation prior to inspection by CBP in Miami. [

[b5 b2 (High) b7E]

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

- In January 2006, CBP Officers

[b5]

CBP]

Officers contacted airline representatives in Korea and requested assistance in verifying the traveler's documents. With airline assistance, CBP determined the subject's travel document was a counterfeit Singapore passport. The subject was in possession of his Sri Lankan passport. The subject was also a positive match to the Transportation Security Administration's No Fly List and suspected of being an armed and dangerous terrorist. The subject was denied boarding for the flight. He was subsequently stopped on another date using the same method of PNR targeting. In the second incident, he attempted to travel to the U.S. using a counterfeit UK passport.

Deleted: [b5]

Deleted: [b5]

Deleted: [b5]

- In February 2006, CBP Officers used PNR data to identify a passenger with a high-risk for narcotics possession arriving from the Dominican Republic. The subject, a returning U.S. legal permanent resident, purchased his ticket using cash

[b5 b2 (High) b7E]

Upon arrival, the subject was selected for an enforcement exam. During an examination of the subject's personal effects, CBP Officers discovered two packages containing heroin. The subject was placed under arrest and turned over to Immigration and Customs Enforcement for prosecution.

Deleted: [b5]

Comment [m1]: [b5]

- At Boston Logan Airport in April 2006, CBP Officers used PNR data to identify two passengers whose travel patterns [b5]

] During the secondary interview process, one subject stated that he was traveling to the United States on business for a group that is suspected of having financial ties to Al Qaeda. The examination of the subject's baggage revealed images of armed men, one of which was labeled "Mujahadin." Both passengers were refused admission.

Comment [m2]: [b5]

Deleted: [b5]

Formatted: Highlight

000365

Unclassified

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

- In May 2006, CBP Officers used PNR data <

b5

> Upon arrival the subject applied for admission as a Jordanian citizen and was referred to secondary inspection for further examination. <

b5

> The subject admitted to being a former member of an organization which espoused political views and violent acts that include suicide bombings. The Joint Terrorism Task Force and Immigration and Customs Enforcement were contacted <

b5

These concrete examples illustrate the necessity of analyzing and sharing PNR data. But it is also important to note the strong privacy protections in place to safeguard this information. PNR data is protected under the U.S. Privacy Act and the Freedom of Information Act, among other laws, as well as the robust oversight provided through the U.S. Congress, American courts, and internal controls such as the Department of Homeland Security's privacy office, Inspector General, and Government Accountability Office. In addition, our policies ensure that records pertaining to foreign nationals are properly protected <

b5

b5

Deleted: []

Deleted: []

Deleted: []

Deleted: []

b5

Deleted: []

Deleted: []

Deleted: []

b5

Deleted: []

b5

One of the central lessons of the 9/11 attacks, and subsequent attacks in Europe and elsewhere, is that we must break down barriers to information sharing. That same lesson must extend to our use of PNR data. We must not take this valuable counter-terrorism

Unclassified

000366

tool away from [b 5] by limiting or restricting the kind of information sharing and analysis that has already proven effective.

~~Deleted: [b 5]~~

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

Sincerely,

Michael Chertoff
Secretary
U.S. Department of Homeland Security

Unclassified

000367

UNCLASSIFIED

May 14, 2007

Dear Member of the European Parliament:

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

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

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

One of these tools is Passenger Name Record (PNR) data, which is a limited set of information [b5] PNR data, used in combination with passenger manifest data, allows U.S. officers to check passenger names and other basic information against lists of known or suspected terrorists and criminals [b5]

Deleted: [b5]

Combined with other intelligence, we also use PNR data to check for links that might reveal unknown terrorist connections, such as a traveler who has provided contact information overlapping with a known terrorist. It is our ability to identify these hidden links that has made PNR so valuable to our counterterrorism efforts [b5]

Formatted: Not Highlight

Deleted: [b5]

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

- In June 2003, using PNR data and other [b5] one of our inspectors at Chicago's O'Hare airport pulled aside an individual for secondary inspection and questioning. When the secondary officers weren't satisfied with his answers they took his fingerprints and denied him entry to the United States. The next time we saw those fingerprints - or at least parts of them - they were on the steering wheel of a suicide vehicle that blew up and killed 132 people in Iraq.
- In January 2003, Customs and Border Protection (CBP) officers in Miami used PNR to disrupt an internal conspiracy within an airline that was smuggling

Deleted: [b5]

000368

246

UNCLASSIFIED

(2)

cocaine between Venezuela and Miami. A corrupt ticket counter agent would identify low risk travelers (typically families) and add an additional bag to their reservation after they departed the ticket counter. This bag would be filled with cocaine. Corrupt airline employees in Miami plotted to remove the added bags from circulation prior to inspection by CBP in Miami. [⊂]

⊃ b5 b2 (High) b7E

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

- In January 2006. CBP Officers [⊂]

b5

⊃ CBP

Officers contacted airline representatives in Korea and requested assistance in verifying the traveler's documents. With airline assistance, CBP determined the subject's travel document was a counterfeit Singapore passport. The subject was in possession of his Sri Lankan passport. [⊂] b5

⊃ The subject was a positive match to the Transportation Security Administration's No Fly List and suspected of being an armed and dangerous terrorist. The subject was denied boarding for the flight. He was subsequently stopped on another date using the same method of PNR targeting. In the second incident, he attempted to travel to the U.S. using a counterfeit UK passport.

- In February 2006. CBP Officers used PNR data to identify a passenger with a high-risk for narcotics possession arriving from the Dominican Republic. The subject, a returning U.S. legal permanent resident, purchased his ticket using cash [⊂]

b5 b2 (High) b7E

⊃ Upon arrival, the subject was selected for an enforcement exam. During an examination of the subject's personal effects, CBP Officers discovered two packages containing heroin. The subject was placed under arrest and turned over to Immigration and Customs Enforcement for prosecution.

- At Boston Logan Airport in April 2006. CBP Officers used PNR data to identify two passengers whose travel patterns [⊂]

b5

⊃ During the secondary interview process, one subject stated that he was traveling to the United States on business for a group that is suspected of having financial ties to Al Qaeda. The examination of the subject's baggage revealed images of armed men, one of which was labeled "Mujahadin." Both passengers were refused admission.

Deleted: [b5]

Deleted: [b5]

Deleted: [b5]

Deleted: [b5]

Deleted: [b5]

Comment [m1]: [b5]

Comment [m2]: [b5]

Deleted: [b5]

Formatted: Highlight

000369

Unclassified

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

Deleted: < b5 >

- In May 2006, CBP Officers used PNR data

b5

Upon arrival the subject applied for admission as a Jordanian citizen and was referred to secondary inspection for further examination.

Deleted:

Deleted:

Deleted:

Deleted:

Deleted:

The subject admitted to being a former member of an organization which espoused political views and violent acts that include suicide bombings. The Joint Terrorism Task Force and Immigration and Customs Enforcement were contacted

b5

b5

Deleted:

b5

Deleted:

Deleted:

Deleted:

These concrete examples illustrate the necessity of analyzing and sharing PNR data. But it is also important to note the strong privacy protections in place to safeguard this information. PNR data is protected under the U.S. Privacy Act and the Freedom of Information Act, among other laws, as well as the robust oversight provided through the U.S. Congress, American courts,

b5

b5

In addition, our policies ensure that records pertaining to foreign nationals are protected

b5

Deleted:

Deleted:

Deleted:

Deleted:

b5

Deleted:

Deleted:

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

Deleted: < b5 >

Unclassified

370
000310

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

Sincerely,

Michael Chertoff
Secretary
U.S. Department of Homeland Security

Unclassified

371
000321

DRAFT

/ FBI - mod

EU Federal Law Enforcement Counterparts

(2)

Country	Responsible ICE Attaché Office	Federal Counterpart(s)
United Kingdom	London	Strategic Organized Crime Agency (SOCA) Her Majesties Customs and Revenue (Customs) London Metropolitan Police UK Immigration Services
Germany	Frankfurt	German Customs (ZKA) German National Police (BKA) German Immigration Border Authority (BP) German State Criminal Authority (LKA)
France	Paris	French Customs French Judicial Police French National Police
Netherlands	Hague	Border Police (Marchesse) Dutch Customs Dutch Immigration
Italy	Rome	Guardia di Finanza (Customs and Internal Revenue agency) Carabinieri (narcotics, terrorism, cultural property cases) Polizia di Stato (Primary law enforcement in Italy, including immigration)
Spain	Madrid	Spanish National Police (SNP) Guardia Civil (another federal agency conducting criminal investigations) Spanish Customs
Belgium	Hague	Belgian National Police Belgian Immigration Belgian Customs
Denmark	Copenhagen	Danish National Police Danish tax authority
Luxembourg	Hague	Luxembourg National Police Luxembourg Immigration Luxembourg Customs
Poland	Frankfurt	Polish National Police Polish Border Guards Polish Customs
Portugal	Madrid	Portugese Immigration Portugese National Police
Austria	Vienna	Austrian National Police (BKA) Austrian Internal Security - illegal exports (BVT)
Greece	Athens	Hellenic Customs Hellenic National Police
Czech Republic	Vienna	Federal Police Czech Customs
Finland	Copenhagen	Finnish National Police Finnish Border Guards Finnish Customs
Hungary	Vienna	Hungarian Finance and Border Guard Hungarian National Police
Latvia	Frankfurt	Latvian Customs
Slovakia	Vienna	Slovakian National Police

/ / FSP - mod
000862

(3)

(C/PST-mul)

61

~~C/PST-mul~~

/PST-mul

998000

~~C/PST-mul~~
/PST-mul

(216-
1901)

61

600864

1901

1901

1901

Attachment A

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

July 13, 2006

Purpose (u)

(u) 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 (u)

(u) 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.

(u) 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. [b5]

ckj-
Mod

b1

000865

(u) 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.

(4)

Derived: Schneider
MRE
Declass: 13 July 2031

b1

(u) 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.

(c)

b1

(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)

b1

(S)

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

(c)

b1

000807

~~FOR OFFICIAL USE ONLY~~

significantly restrict US opportunities to use information for investigative and law enforcement purposes.

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

(c)¹.

b¹

(c)•

(c)•

(c)•

000868

~~FOR OFFICIAL USE ONLY~~

(c).

(e)

b1

(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.

(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

(u) 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."

(dfj-
MOD)

b1

000869

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

(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.

(S)¹

b1

(u) **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. [

← [

b5

]

(clg)
Med

b1

(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 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.

(u) ⁹ 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

(S):

b1

(C/Sj-
Mod)

(C/Sj-
Mod)

purpose for which it was first transmitted. In effect, it borrows heavily from the PNR Agreement and the Undertakings.

(C/Sj-
Mod)

b1

(u) 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

(u) 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,

(u) **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 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)

(s)

b1

(c)

(u) 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.

(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.

(S)

b1

Conclusion (u)

(a)

b1

(S)

(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)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.

(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)

b1

(C)

Attachments

- A. Excerpt from EU Data Protection Directive 95/46/EC (24 October 1995) (u)
- 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) (u)

Attachments:

A. DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 24 October 1995

Article 3

Scope

1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Directive shall not apply to the processing of personal data:

- in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,

Article 26

Derogations

1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases. Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:

- (a) the data subject has given his consent unambiguously to the proposed transfer; or
- (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or
- (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or
- (d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or
- (e) the transfer is necessary in order to protect the vital interests of the data subject; or
- ~~(f) the transfer is made from a register which according to laws or regulations is intended to~~

provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

2. Without prejudice to paragraph 1. a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights: such safeguards may in particular result from appropriate contractual clauses.

3. The Member State shall inform the Commission and the other Member States of the authorizations it grants pursuant to paragraph 2.

~~FOR OFFICIAL USE ONLY~~

If a Member State or the Commission objects on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals, the Commission shall take appropriate measures in accordance with the procedure laid down in Article 31 (2).

Member States shall take the necessary measures to comply with the Commission's decision.

4. Where the Commission decides, in accordance with the procedure referred to in Article 31 (2), that certain standard contractual clauses offer sufficient safeguards as required by paragraph 2, Member States shall take the necessary measures to comply with the Commission's decision.

CHAPTER IV TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

Article 25

Principles

1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.

4. Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.

~~5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.~~

6. The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.

Member States shall take the measures necessary to comply with the Commission's decision.

000876

~~FOR OFFICIAL USE ONLY~~

UNCLASS

B. Proposal for a COUNCIL FRAMEWORK DECISION on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters

Article 15

Transfer to competent authorities in third countries or to international bodies

1. Member States shall provide that personal data received from or made available by the competent authority of another Member State are not further transferred to competent authorities of third countries or to international bodies except if such transfer is in compliance with this Framework Decision and, in particular, all the following requirements are met.

(a) The transfer is provided for by law clearly obliging or authorising it.

(b) The transfer is necessary for the purpose the data concerned were transmitted or made available for or for the purpose of the prevention, investigation, detection or prosecution of criminal offences or for the purpose of the prevention of threats to public security or to a person, except where such considerations are overridden by the need to protect the interests or fundamental rights of the data subject.

(c) The competent authority of another Member State that has transmitted or made available the data concerned to the competent authority that intends to further transfer them has given its prior consent to their further transfer.

(d) An adequate level of data protection is ensured in the third country or by the international body to which the data concerned shall be transferred.

2. Member States shall ensure that the adequacy of the level of protection afforded by a third country or international body shall be assessed in the light of all the circumstances for each transfer or category of transfers. In particular, the assessment shall result from an examination of the following elements: the type of data, the purposes and duration of processing for which the data are transferred, the country of origin and the country of final destination, the general and sectoral rules of law applicable in the third country or body in question, the professional and security rules which are applicable there, as well as the existence of sufficient safeguards put in place by the recipient of the transfer.

3. The Member States and the Commission shall inform each other of cases where they consider that a third country or an international body does not ensure an adequate level of protection within the meaning of paragraph 2.

4. Where, under the procedure provided for in Article 16, it is established that a third country or international body does not ensure an adequate level of protection within the meaning of paragraph 2, Member States shall take the measures necessary to prevent any transfer of personal data to the third country or international body in question.

5. In accordance with the procedure referred to in Article 16, it may be established that a third country or international body ensures an adequate level of protection within the meaning of paragraph 2, by reason of its domestic law or of the international commitments it has entered into, for the protection of the private lives and basic freedoms and rights of individuals.

~~FOR OFFICIAL USE ONLY~~

6. Exceptionally, personal data received from the competent authority of another Member State may be further transferred to competent authorities of third countries or to international bodies in or by which an adequate level of data protection is not ensured if absolutely necessary in order to safeguard the essential interests of a Member State or for the prevention of imminent serious danger threatening public security or a specific person or persons.

000878

~~FOR OFFICIAL USE ONLY~~

UNCLASS

Attachment A

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

July 13, 2006

Purpose

(u) 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

(u) 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.

(u) 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. L

b5

b1

(u) ¹CBP 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

Derived: Schneider MFR
Subject: EU/PNR
Declass. 13 July 2031
000879 (382.1)

(5)

b1

(u) 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.

b1

(u) ³ 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) ⁴ 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)

b1

(S)

Background

(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

(S)

b1

FOR OFFICIAL USE ONLY

significantly restrict US opportunities to use information for investigative and law enforcement purposes.

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

(c) 1.

(c)

b1

(c)

(c)

Formatted: Font: Times New Roman, 12 pt

Formatted: Indent: Left: 0.75"

(c)

b1

Formatted: Bullets and Numbering

(c)

b1

FOR OFFICIAL USE ONLY

000882

(c)

(c)

b1

(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.

(u)

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)
M/S

b1

(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 governing commercial data exports. If they are to be regulated, the court implied, it would have to be done under the "Third Pillar."⁸

(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.

(S)

b1

(u) 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. ^c

E

b5

J

(u) (S)

b1

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 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 OFFICIAL USE ONLY~~

(S)

b1

(c)(1)
(mod)

(c)(1)
(mod)

(4)

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.

(c)(1)
(mod)

b1

(2)

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

~~FOR OFFICIAL USE ONLY~~

000825

(u)

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

Analysis & Recommendation

(c)

(s)

b1

(c)

(u)

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.

(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.

FOR OFFICIAL USE ONLY

(c)

(s)

b1

Conclusion

(c)

(s)

b1

(s)

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.

FOR OFFICIAL USE ONLY

600887

~~FOR OFFICIAL USE ONLY~~

- (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)

b1

(C)

Attachments

- A. Excerpt from EU Data Protection Directive 95/46/EC (24 October 1995) (u)
- 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) (u)

~~FOR OFFICIAL USE ONLY~~

000888

~~FOR OFFICIAL USE ONLY~~

Attachments:

**A. DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 24 October 1995**

Article 3

Scope

1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Directive shall not apply to the processing of personal data:

- in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,

Article 26

Derogations

1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:

- (a) the data subject has given his consent unambiguously to the proposed transfer: or
- (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or
- (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party: or
- (d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims: or
- (e) the transfer is necessary in order to protect the vital interests of the data subject; or
- (f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

2. Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.

3. The Member State shall inform the Commission and the other Member States of the authorizations it grants pursuant to paragraph 2.

~~FOR OFFICIAL USE ONLY~~

000889

UNCLASS

~~FOR OFFICIAL USE ONLY~~

If a Member State or the Commission objects on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals, the Commission shall take appropriate measures in accordance with the procedure laid down in Article 31 (2).

Member States shall take the necessary measures to comply with the Commission's decision.

4. Where the Commission decides, in accordance with the procedure referred to in Article 31 (2), that certain standard contractual clauses offer sufficient safeguards as required by paragraph 2, Member States shall take the necessary measures to comply with the Commission's decision.

CHAPTER IV TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

Article 25

Principles

1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.

4. Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.

5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.

6. The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.

Member States shall take the measures necessary to comply with the Commission's decision.

~~FOR OFFICIAL USE ONLY~~

000890

UNCLASS

~~FOR OFFICIAL USE ONLY~~

B. Proposal for a COUNCIL FRAMEWORK DECISION on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters

Article 15

Transfer to competent authorities in third countries or to international bodies

1. Member States shall provide that personal data received from or made available by the competent authority of another Member State are not further transferred to competent authorities of third countries or to international bodies except if such transfer is in compliance with this Framework Decision and, in particular, all the following requirements are met.

(a) The transfer is provided for by law clearly obliging or authorising it.

(b) The transfer is necessary for the purpose the data concerned were transmitted or made available for or for the purpose of the prevention, investigation, detection or prosecution of criminal offences or for the purpose of the prevention of threats to public security or to a person, except where such considerations are overridden by the need to protect the interests or fundamental rights of the data subject.

(c) The competent authority of another Member State that has transmitted or made available the data concerned to the competent authority that intends to further transfer them has given its prior consent to their further transfer.

(d) An adequate level of data protection is ensured in the third country or by the international body to which the data concerned shall be transferred.

2. Member States shall ensure that the adequacy of the level of protection afforded by a third country or international body shall be assessed in the light of all the circumstances for each transfer or category of transfers. In particular, the assessment shall result from an examination of the following elements: the type of data, the purposes and duration of processing for which the data are transferred, the country of origin and the country of final destination, the general and sectoral rules of law applicable in the third country or body in question, the professional and security rules which are applicable there, as well as the existence of sufficient safeguards put in place by the recipient of the transfer.

3. The Member States and the Commission shall inform each other of cases where they consider that a third country or an international body does not ensure an adequate level of protection within the meaning of paragraph 2.

4. Where, under the procedure provided for in Article 16, it is established that a third country or international body does not ensure an adequate level of protection within the meaning of paragraph 2, Member States shall take the measures necessary to prevent any transfer of personal data to the third country or international body in question.

5. In accordance with the procedure referred to in Article 16, it may be established that a third country or international body ensures an adequate level of protection within the meaning of paragraph 2, by reason of its domestic law or of the international commitments it has entered into, for the protection of the private lives and basic freedoms and rights of individuals.

~~FOR OFFICIAL USE ONLY~~

000891

UNCLASS

~~FOR OFFICIAL USE ONLY~~

6. Exceptionally, personal data received from the competent authority of another Member State may be further transferred to competent authorities of third countries or to international bodies in or by which an adequate level of data protection is not ensured if absolutely necessary in order to safeguard the essential interests of a Member State or for the prevention of imminent serious danger threatening public security or a specific person or persons.

~~FOR OFFICIAL USE ONLY~~

000892

UNCLASS

FOR OFFICIAL ~~USE~~ ONLY

Attachment C

Member State Positions known as of 7/20/06¹³

(S)

(S)

(S)

b1

¹³Note: DHS OIA has requested input from Economic Officers at other EU posts and is seeking for input.

FOR OFFICIAL ~~USE~~ ONLY

(6)

000893

FOR OFFICIAL ~~USE~~ ONLY

Attachment D

EU Views on Consent

(c)

(c)

b1

(c)

(c)

History of DHS Discussions with the EU on Consent and PNR

(c)

b1

FOR OFFICIAL ~~USE~~ ONLY

(7)

000294

FOR OFFICIAL ~~X~~ USE ONLY

(c)

b1

EU Position on Consent in other areas

(c)

b1

FOR OFFICIAL ~~X~~ USE ONLY

600895

FOR OFFICIAL USE ONLY

Attachment E

Issue: DHS' Response Options to European Court of Justice Decision
February 2006

(S)

(C)

(C)

b1

(C)

(C)

DHS' Optional Responses

(C)

b1

(C)

FOR OFFICIAL USE ONLY

000896

(S)

FOR OFFICIAL USE ONLY

(c)^D

(c)^v

(c)^v

(c)^v

(c)^v

b1

D

(c)

FOR OFFICIAL USE ONLY

600897

FOR OFFICIAL ~~USE~~ ONLY

(c) ²

(c) ²

b1

(c) ²

(c) ³⁾

(c) ²

FOR OFFICIAL ~~USE~~ ONLY

858300

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

July 27, 2006

Purpose

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

[b5]

Summary

- (u) 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.

- (u) 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. [b5]

(c/f; -)
mod

b1

000899

- (u) 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.

9

Derived: Schneider MCE
Declass: 27 July 2021

284.1

b1

(u) The PNR Agreement 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 procedural, not substantive: 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. 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.

(c)

b1

000900

(s) 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.

(S)

b1

(S)

(C)

Background

(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.³ Several of the limitations in those Undertakings significantly restrict US opportunities to use information for investigative and law enforcement purposes.~~

(U)

b1

000901

~~SECRET~~
FOR OFFICIAL USE ONLY

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

•
(c)

b1

•
(c)

•
(c)

•
(c)

(c)

b1

000902

~~SECRET~~
FOR OFFICIAL USE ONLY

(c)

b1

(c)

The ECJ PNR Case. 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.

(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 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. []

[

b5

]

(u)

⁵ 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."

000903

(C)

(S)

b1

(C/fgi-)
(mod)

(fgi-)
(mod)

(4)

⁶ 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.

(C/fgi-)
(mod)

b1

~~SECRET~~
FOR OFFICIAL USE ONLY

Conclusion

(c)

b1

(s)

00 0905

~~SECRET~~
FOR OFFICIAL USE ONLY

FOR OFFICIAL ~~USE~~ ONLY

Attachment A

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

July 13, 2006

Purpose (u)

(u) 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

(u) 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 off, protecting against mid-flight hijackings and bombings.

(u) 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. L 65 J

(u) (C) (S) Mod

b1

(u) 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.

FOR OFFICIAL ~~USE~~ ONLY

000911

Derived: Schneider
MFE

Declass: 12 July 2021

10

b1

(u) 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.

(c)

b1

(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.

000912

(S)

b1

(S)

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

(S)

b1

FOR OFFICIAL ~~USE~~ ONLY

significantly restrict US opportunities to use information for investigative and law enforcement purposes.

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

1.
(c)

(c)

b1

(c)

(c)

(c)

b1

FOR OFFICIAL ~~USE~~ ONLY

000914

(c)

(c)

b1

(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.

(u) _____
* 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-fpi-
Mod)

b1

(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 governing commercial data exports. If they are to be regulated, the court implied, it would have to be done under the "Third Pillar."⁸

(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.

(S)

b1

(u) **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. ←

b5

(C-fri)
Mod

b1

(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 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 OFFICIAL ~~USE~~ ONLY

(C/Fsi-
P2d)

(S)

02

b1

(C/Fsi-
MOD)

(C/Fsi-
MOD)

(4)

⁹ 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.

(C/Fsi-
MOD)

b1

(4)

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

FOR OFFICIAL ~~USE~~ ONLY

000917

b1

(S)

(u)

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 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)

(S)

b1

(c)

(u)

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.

(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.

FOR OFFICIAL ~~USE~~ ONLY

(c)

(S)^e

b1

Conclusion (u)

(c)

o.

(S)

b1

(u) ¹³ 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.

FOR OFFICIAL ~~USE~~ ONLY

000919

FOR OFFICIAL ~~USE~~ ONLY

- (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)

b1

(C)

Attachments

- A. Excerpt from EU Data Protection Directive 95/46/EC (24 October 1995) (u)
- 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) (u)

FOR OFFICIAL ~~USE~~ ONLY

000920

FOR OFFICIAL ~~USE~~ ONLY

Attachments:

A. DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 24 October 1995

Article 3

Scope

1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Directive shall not apply to the processing of personal data:

- in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law.

Article 26

Derogations

1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:

(a) the data subject has given his consent unambiguously to the proposed transfer; or

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or

(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or

(e) the transfer is necessary in order to protect the vital interests of the data subject; or

(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

2. Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.

3. The Member State shall inform the Commission and the other Member States of the authorizations it grants pursuant to paragraph 2.

FOR OFFICIAL ~~USE~~ ONLY

000921

UNCLASS

~~FOR OFFICIAL USE ONLY~~

If a Member State or the Commission objects on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals, the Commission shall take appropriate measures in accordance with the procedure laid down in Article 31 (2).

Member States shall take the necessary measures to comply with the Commission's decision.

4. Where the Commission decides, in accordance with the procedure referred to in Article 31 (2), that certain standard contractual clauses offer sufficient safeguards as required by paragraph 2, Member States shall take the necessary measures to comply with the Commission's decision.

CHAPTER IV TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

Article 25

Principles

1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.

4. Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.

5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.

6. The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.

Member States shall take the measures necessary to comply with the Commission's decision.

~~FOR OFFICIAL USE ONLY~~

000922

UNCLASS

FOR OFFICIAL ~~USE~~ ONLY

B. Proposal for a COUNCIL FRAMEWORK DECISION on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters

Article 15

Transfer to competent authorities in third countries or to international bodies

1. Member States shall provide that personal data received from or made available by the competent authority of another Member State are not further transferred to competent authorities of third countries or to international bodies except if such transfer is in compliance with this Framework Decision and, in particular, all the following requirements are met.

(a) The transfer is provided for by law clearly obliging or authorising it.

(b) The transfer is necessary for the purpose the data concerned were transmitted or made available for or for the purpose of the prevention, investigation, detection or prosecution of criminal offences or for the purpose of the prevention of threats to public security or to a person, except where such considerations are overridden by the need to protect the interests or fundamental rights of the data subject.

(c) The competent authority of another Member State that has transmitted or made available the data concerned to the competent authority that intends to further transfer them has given its prior consent to their further transfer.

(d) An adequate level of data protection is ensured in the third country or by the international body to which the data concerned shall be transferred.

2. Member States shall ensure that the adequacy of the level of protection afforded by a third country or international body shall be assessed in the light of all the circumstances for each transfer or category of transfers. In particular, the assessment shall result from an examination of the following elements: the type of data, the purposes and duration of processing for which the data are transferred, the country of origin and the country of final destination, the general and sectoral rules of law applicable in the third country or body in question, the professional and security rules which are applicable there, as well as the existence of sufficient safeguards put in place by the recipient of the transfer.

3. The Member States and the Commission shall inform each other of cases where they consider that a third country or an international body does not ensure an adequate level of protection within the meaning of paragraph 2.

4. Where, under the procedure provided for in Article 16, it is established that a third country or international body does not ensure an adequate level of protection within the meaning of paragraph 2, Member States shall take the measures necessary to prevent any transfer of personal data to the third country or international body in question.

~~5. In accordance with the procedure referred to in Article 16, it may be established that a third country or international body ensures an adequate level of protection within the meaning of paragraph 2, by reason of its domestic law or of the international commitments it has entered into, for the protection of the private lives and basic freedoms and rights of individuals.~~

FOR OFFICIAL ~~USE~~ ONLY

000923

UNCLASS

~~FOR OFFICIAL USE ONLY~~

6. Exceptionally, personal data received from the competent authority of another Member State may be further transferred to competent authorities of third countries or to international bodies in or by which an adequate level of data protection is not ensured if absolutely necessary in order to safeguard the essential interests of a Member State or for the prevention of imminent serious danger threatening public security or a specific person or persons.

~~FOR OFFICIAL USE ONLY~~

000924

UNCLASS

FOR OFFICIAL USE ONLY

~~Secret~~

DISCUSSION DOCUMENT

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

July 27, 2006

Purpose

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

(a) [b5]

Summary

(d) 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.

u 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. [b5]

(C/S) [initials]

b1

000925

(u) 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.

FOR OFFICIAL USE ONLY

~~Secret~~

Derived: Schneider MCE
Dolans: 27 July 2021

(11)

b1

(u)

The PNR Agreement 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 procedural, not substantive: 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. 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.

(c)

b1

(u)

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.

000926

(S)

b1

(S)

(C)

Background

(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.³ Several of the limitations in those Undertakings significantly restrict US opportunities to use information for investigative and law enforcement purposes.

(C)

b1

000927

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

(c)

b1

(c)

(c)

(c)

(c)

b1

000928

(c)

b1

(c)

(u) **The ECJ PNR Case.** 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.

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

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. []

(u)

[b5]

(u) ⁵ 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."

000929

(C)

(S)

2

b1

(C-Sci-Mod)
2

(S)
2

(4)

⁶ 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.

(C-Sci-Mod)

b1

~~Secret~~
FOR OFFICIAL USE ONLY

Conclusion

(c)

b1

(S)

FOR OFFICIAL USE ONLY

~~Secret~~

000931

Attachment C

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

July 13, 2006

Purpose (u)

- (u) 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 (u)

(u) 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.

(u) 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. <

b5

(c/fq/-
Mod)

b1

(u) 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.

000932

(12)

~~SECRET~~

Derived: Schneider MFR
Declass: PA
12 (Jul 2006)

FOR OFFICIAL USE ONLY

(C/fig)
mod

b1

(u) 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.

(c)

b1

(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.

FOR OFFICIAL USE ONLY

000933

~~SECRET~~
FOR OFFICIAL USE ONLY

(c)

(S)

b1

(S)

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.³ Several of the limitations in those Undertakings

(c)

b1

FOR OFFICIAL USE ONLY

~~SECRET~~

000934

~~FOR OFFICIAL USE ONLY~~

(v) significantly restrict US opportunities to use information for investigative and law enforcement purposes.

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

(c)^{1.}

2.

(c)

b1

(c)

(c)

(c)

b1

~~FOR OFFICIAL USE ONLY~~

000935

(C)

(C)

b1

(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.

(U) 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."

(S)
(M)

b1

~~SECRET~~

(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 governing commercial data exports. If they are to be regulated, the court implied, it would have to be done under the "Third Pillar."³

(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.

(S)

b1

(u) **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. c

L

b5

J

(ckg)
(M)

b1

(u) ³ 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.

~~FOR OFFICIAL USE ONLY~~

(c/fq)
(mod)

(S)

b1

(c/fq)
(mod)

(c/fq)
(mod)

(u) ¹⁰ 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.

(c/fq)
(mod)

b1

(u) 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

~~FOR OFFICIAL USE ONLY~~

000938

(S/Fg) (u)

b1

(u) **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 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)

b1

(S)

(c)

(u) 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.

(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-IHS 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.

(d)

(s)

b1

Conclusion (u)

(c)

b1

(s)

(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.

- (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)

b1

(c)

Attachments

- A. Excerpt from EU Data Protection Directive 95/46/EC (24 October 1995) (u)
- 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) (u)

~~SECRET~~

000941

FOR OFFICIAL USE ONLY

Attachments:

A. DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 24 October 1995

Article 3

Scope

1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Directive shall not apply to the processing of personal data:

- in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law.

Article 26

Derogations

1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:

(a) the data subject has given his consent unambiguously to the proposed transfer; or

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or

(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or

(e) the transfer is necessary in order to protect the vital interests of the data subject; or

(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

2. Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights, such safeguards may in particular result from appropriate contractual clauses.

3. The Member State shall inform the Commission and the other Member States of the authorizations it grants pursuant to paragraph 2.

FOR OFFICIAL USE ONLY

000942

UNCLASS

~~FOR OFFICIAL USE ONLY~~

If a Member State or the Commission objects on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals, the Commission shall take appropriate measures in accordance with the procedure laid down in Article 31 (2).

Member States shall take the necessary measures to comply with the Commission's decision.

4. Where the Commission decides, in accordance with the procedure referred to in Article 31 (2), that certain standard contractual clauses offer sufficient safeguards as required by paragraph 2, Member States shall take the necessary measures to comply with the Commission's decision.

CHAPTER IV TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

Article 25

Principles

1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.

4. Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.

5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.

6. The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.

Member States shall take the measures necessary to comply with the Commission's decision.

~~FOR OFFICIAL USE ONLY~~

000943

UNCLASS

~~FOR OFFICIAL USE ONLY~~

B. Proposal for a COUNCIL FRAMEWORK DECISION on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters

Article 15

Transfer to competent authorities in third countries or to international bodies

1. Member States shall provide that personal data received from or made available by the competent authority of another Member State are not further transferred to competent authorities of third countries or to international bodies except if such transfer is in compliance with this Framework Decision and, in particular, all the following requirements are met.
 - (a) The transfer is provided for by law clearly obliging or authorising it.
 - (b) The transfer is necessary for the purpose the data concerned were transmitted or made available for or for the purpose of the prevention, investigation, detection or prosecution of criminal offences or for the purpose of the prevention of threats to public security or to a person, except where such considerations are overridden by the need to protect the interests or fundamental rights of the data subject.
 - (c) The competent authority of another Member State that has transmitted or made available the data concerned to the competent authority that intends to further transfer them has given its prior consent to their further transfer.
 - (d) An adequate level of data protection is ensured in the third country or by the international body to which the data concerned shall be transferred.
2. Member States shall ensure that the adequacy of the level of protection afforded by a third country or international body shall be assessed in the light of all the circumstances for each transfer or category of transfers. In particular, the assessment shall result from an examination of the following elements: the type of data, the purposes and duration of processing for which the data are transferred, the country of origin and the country of final destination, the general and sectoral rules of law applicable in the third country or body in question, the professional and security rules which are applicable there, as well as the existence of sufficient safeguards put in place by the recipient of the transfer.
3. The Member States and the Commission shall inform each other of cases where they consider that a third country or an international body does not ensure an adequate level of protection within the meaning of paragraph 2.
4. Where, under the procedure provided for in Article 16, it is established that a third country or international body does not ensure an adequate level of protection within the meaning of paragraph 2, Member States shall take the measures necessary to prevent any transfer of personal data to the third country or international body in question.
5. In accordance with the procedure referred to in Article 16, it may be established that a third country or international body ensures an adequate level of protection within the meaning of paragraph 2, by reason of its domestic law or of the international commitments it has entered into, for the protection of the private lives and basic freedoms and rights of individuals.

~~FOR OFFICIAL USE ONLY~~

UNCLASS

000944

~~FOR OFFICIAL USE ONLY~~

6. Exceptionally, personal data received from the competent authority of another Member State may be further transferred to competent authorities of third countries or to international bodies in or by which an adequate level of data protection is not ensured if absolutely necessary in order to safeguard the essential interests of a Member State or for the prevention of imminent serious danger threatening public security or a specific person or persons.

~~FOR OFFICIAL USE ONLY~~

UNCLASS

000945

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

13

UNCLASSIFIED

001022

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 and crimes in cases (including threats, flights, individuals, and routes of concern) that they are examining or investigating. DHS will ensure that such authorities respect comparable standards of data protection to that applicable to DHS, in particular in relation to purpose limitation, data retention, further disclosure, awareness and training, security standards and sanctions for abuse, and procedures for information, complaints and rectification. Prior to commencing facilitated disclosure, each receiving authority will confirm in writing to DHS that it respects those standards. DHS will inform the EU in writing of the implementation of such facilitated disclosure and respect for the applicable standards before the 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 these 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 these 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

001023

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. <

b5

7

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

001024

UNCLASSIFIED

Options for PNR Negotiations with the EU

7/28/06

Background: C

b5

⊃ an international agreement was struck between DHS and the EU in 2004 governing CBP's access to PNR from the EU. The agreement was quickly challenged in court by the European Parliament. On 5/30/05 the European Court of Justice ruled that the EU inappropriately entered into this agreement on the grounds that the 1995 Directive did not apply C b5

⊃ On 7/3/06, the Finnish Presidency and the Commission terminated the agreement effective 9/30/06. The Finnish Presidency also received a mandate from the European Council to negotiate a replacement agreement by 9/30. The Commission presented the USG with a proposed text on 7/16.

(C)

(C)

b1

(C)

(C)

(C)

(14)

Law Enforcement Sensitive

001223

(18)

7/28/06

Options for PNR Negotiations with the EU
7/28/06

Background: [

b5

(S) an international agreement was struck between DHS and the EU in 2004 governing CBP's access to PNR from the EU. The agreement was quickly challenged in court by the European Parliament. On 5/30/05 the European Court of Justice ruled that the EU inappropriately entered into this agreement on the grounds that the 1995 Directive did not apply [

b5

]

On 7/3/06, the Finnish Presidency and the Commission terminated the agreement effective 9/30/06. The Finnish Presidency also received a mandate from the European Council to negotiate a replacement agreement by 9/30. The Commission presented the USG with a proposed text on 7/16.

(C)

b1

(C)

(C)

(C)

001228

(C)

Permit: Schneider MPA
Neelast: 7/20/06

Law Enforcement Sensitive

(B)

(16)

(c)

d/1-03
MVP

b1

(c)

(c)

(c)

(c)

(c)

(c)

(c)

001229

Law Enforcement Sensitive

Options for PNR Negotiations with the EU
7/28/06

(C)

(C)

b1

C/FST
MOD

(C)

(C)

(C)

C/FST MOD

(C)

(C)

(C)

001230

~~Law Enforcement Sensitive~~

Options for PNR Negotiations with the EU
7/28/06

(c)

(c)

(c)

b1

001231

~~Law Enforcement Sensitive~~

Options for PNR Negotiations with the EU

7/28/06

Background: \llcorner

b5

(u) \supset an international agreement was struck between DHS and the EU in 2004 governing CBP's access to PNR from the EU. The agreement was quickly challenged in court by the European Parliament. On 5/30/05 the European Court of Justice ruled that the EU inappropriately entered into this agreement on the grounds that the 1995 Directive did not apply \llcorner

b5

On 7/3/06, the Finnish Presidency and the Commission terminated the agreement effective 9/30/06. The Finnish Presidency also received a mandate from the European Council to negotiate a replacement agreement by 9/30. The Commission presented the USG with a proposed text on 7/16.

(c)

(c)

b1

(c)

(c)

(c)

001232

Permit: Schmidt MAN
Reddy 7/20/06

Law Enforcement Sensitive

(16)

275

Options for PNR Negotiations with the EU
7/28/06

(c)

(c)

C/PSJ
mvd

b1

(c)

(c) >

(c) >

(c)

(c)

(c)

(c)

001233

~~Law Enforcement Sensitive~~

Options for PNR Negotiations with the EU
7/28/06

(c)

(c)

C/POF
not

b1

(c)

(c)

(c)

C/POF not

(c)

(c)

(c)

001234

Options for PNR Negotiations with the EU
7/28/06

(c)

(c)

b1

001235

Law Enforcement ~~Sensitive~~

Options for PNR Negotiations with the EU
7/28/06

Background: [b5

(C) > an international agreement was struck between DHS and the EU in 2004 governing CBP's access to PNR from the EU. The agreement was quickly challenged in court by the European Parliament. On 5/30/05 the European Court of Justice ruled that the EU inappropriately entered into this agreement on the grounds that the 1995 Directive did not apply [

On 7/3/06, the Finnish Presidency and the Commission terminated the agreement effective 9/30/06. The Finnish Presidency also received a mandate from the European Council to negotiate a replacement agreement by 9/30. The Commission presented the USG with a proposed text on 7/16. b5

(C)

(C)

b1

(C)

(C)

001236

Derived: Schneider MAR Law Enforcement Sensitive
Re obs 7/20/06

(17)

(17)

Options for PNR Negotiations with the EU
7/28/06

(c)

(c)

C/PSA
red

(c)

b1

(c) >

(c) >

(c)

>

(c)

(c)

(c)

001237

~~Law Enforcement Sensitive~~

Options for PNR Negotiations with the EU
7/28/06

(c)

(c)

C/
PST - mod

(c)

bl

(c)

(c)

C/PST
mod

(c)

(c)

(c)

001238

~~Law Enforcement Sensitive~~

Options for PNR Negotiations with the EU
7/28/06

(c)

(c)

b1

001239

~~Law Enforcement Sensitive~~

Options for PNR Negotiations with the EU
7/28/06

(c) |

Deleted: []

(c) | F

Deleted: b5

Deleted: []

7/28/06
mrd

Deleted: []

Deleted: b1

Formatted: Indent: Left: 0.25",
Tabs: 0.5", List tab + Not at 0.75"

(c) |

b1

Deleted: []

Deleted: []

Deleted: []

(c) >

Deleted: []

(c) >

Deleted: b5

Deleted: []

Deleted: []

Deleted: []

(c) |

(c) >

(c) |

(c) | b1

Dr

(c) |

Deleted: []

Deleted: []

Deleted: b5

Deleted: []

Deleted: []

Deleted: []

(c) |

~~Law Enforcement Sensitive~~

001240

Options for PNR Negotiations with the EU
7/28/06

(a)

(c)

7/PSF
Mod

(c)

Deleted: [b5]

(c)

b1

Deleted: [redacted]

(c)

7/PSF mod

Deleted: [b5]

(c)

(c)

Deleted: /
Deleted: o

(c)

~~Law Enforcement Sensitive~~

001241

Options for PNR Negotiations with the EU
7/28/06

(c) >
(c) >

b1

Deleted: E b5 2

~~Law Enforcement Sensitive~~

001242

Options for PNR Negotiations with the EU
7/28/06

Background: b5

(u) an international agreement was struck between DHS and the EU in 2004 governing CBP's access to PNR from the EU. The agreement was quickly challenged in court by the European Parliament. On 5/30/05 the European Court of Justice ruled that the EU inappropriately entered into this agreement on the grounds that the 1995 Directive did not apply

b5 On 7/3/06, the Finnish Presidency and the Commission terminated the agreement effective 9/30/06. The Finnish Presidency also received a mandate from the European Council to negotiate a replacement agreement by 9/30. The Commission presented the USG with a proposed text on 7/16.

Deleted:
Deleted:

Deleted:
Deleted:

Deleted:
Deleted:
Deleted:
Deleted:
Deleted:
Deleted:

Deleted:

Deleted:
Deleted: [b5]
Deleted:

Deleted: [b5]
Deleted:

Deleted:

¹ European Parliament. Joint Motion for a Resolution on the interception of bank transfer data from the SWIFT system by the US secret services. 7/5/2006

Law Enforcement ~~Sensitive~~

Revised: Schneider MPX

Revised: 7/20/01

001250

19

Options for PNR Negotiations with the EU
7/28/06

(b)

(b)

Deleted

(b)

b1

Deleted

b5

2/25/06
Mull

Deleted

(b)

(b)

(b)

(b) b1

Deleted: [b5]

Deleted: 1

Deleted: [b5]

Deleted: 3

Deleted: M

(b)

² EDPS Press Release, May 30, 2006

Deleted

[b5]

Law Enforcement Sensitive

001251

Options for PNR Negotiations with the EU
7/28/06

Background: [

an international agreement was struck between DHS and the EU in 2004 governing CBP's access to PNR from the EU. The agreement was quickly challenged in court by the European Parliament. On 5/30/05 the European Court of Justice ruled that the EU inappropriately entered into this agreement on the grounds that the 1995 Directive did not apply [

On 7/3/06, the Finnish Presidency and the Commission terminated the agreement effective 9/30/06. The Finnish Presidency also received a mandate from the European Council to negotiate a replacement agreement by 9/30. The Commission presented the USG with a proposed text on 7/16.

Deleted: [b5]

(c) b1

Deleted:

(c) b1

Deleted:

Deleted:

Deleted:

[b5]

(c) b1

Deleted:

Deleted:

Deleted:

Deleted:

Deleted:

[b5]

Deleted: [b5]

Deleted: [b5]

~~Law Enforcement Sensitive~~

Derived: Schneider MPA

Revised: 7/20/21

001252

20

20

(c)
(c)
(c)
(c)

b1

9/26/06

(c)
(c)

(c) Deleted: b1
Deleted: S
Deleted: M
Deleted: D
(c) Deleted: b1
Deleted: nited States
(c) Deleted: b1
Deleted: W
Deleted: M
Deleted: M
Deleted: W
Deleted: S
Deleted: P
Deleted: N
Deleted: U
Deleted: C

Deleted: [b5]
Deleted: [b5]
Deleted: W
Deleted: W
Deleted: enure
Deleted: [b5]
Deleted: W
Deleted: S
Deleted: P
Deleted: :
Deleted: b1
Deleted: [b5]
Deleted: W
Deleted: M

~~Law Enforcement Sensitive~~

Options for PNR Negotiations with the EU
7/28/06

| @
@

bl

Deleted: S

Deleted: C

Deleted: C

Deleted: C b5 3

Deleted: C

Deleted: P

Deleted: M

| @
@

Deleted: W

Deleted: W

Law Enforcement Sensitive

001254

~~SECRET~~

(c)

Deleted: that

(c)

b1

Deleted: ed

(c)

Deleted: that

Deleted: and

Deleted: of

Deleted: the

Deleted: s

Deleted: a

Deleted: .

Formatted: Font: Italic

(c)

(u) issues:

(c)

b1

(c)

| [

b5

] |

~~SECRET~~

001256

(c)

(c)

(c)

(c)

(c)

(c)

b1

Deleted: those
 Deleted: would
 Deleted: d
 Comment (mf1): This doesn't make sense
 Deleted:
 Deleted: [b5]
 Deleted:
 Deleted: ¶
 Formatted: Indent: Left: 0.25", Tabs: 0.63", List tab + Not at 0.25"
 Formatted: Bullets and Numbering
 Formatted: Indent: Left: 0.58", Tabs: 0.88", List tab + 1.13", Left + Not at 0.55"
 Formatted: Indent: Left: 0.58", Tabs: 0.63", List tab + 0.88", List tab + Not at 0.55"
 Formatted: Indent: Left: 0.25", Tabs: 0.63", List tab - Not at 0.25"
 Comment (m2)
 [b5]
 Formatted: Indent: Left: 0.25", Space After: 0 pt, Outline numbered - Level: 1 + Numbering Style: 1, 2, 3, ... + Start at: 1 + Alignment: Left + Aligned at: 0" + Tab after: 0.25" + Indent at: 0.25", Tabs: 0.63", List tab + Not at 0.25"
 Deleted:
 [b5]
 Deleted: Since
 Deleted: us
 Deleted: as
 Deleted: As such,
 Deleted: re
 Deleted: that
 Deleted: are going to be
 Deleted: red
 Deleted: would
 Deleted: to
 Deleted: on
 Formatted: Not highlight

Deleted: [b5]
Deleted:

Formatted: Bullets and Numbering

Deleted: [b5]
Deleted:

Deleted: [b5]
Deleted: [b5]
Deleted:

Deleted: i
Deleted: w
Deleted: ed

Deleted: i
Formatted: Underline

Deleted: [b5]
Formatted: Font: Bold

Deleted: that

(c)

(c)

(c)

(c)

(c)

(c)

(c)

(c)

b1

(c)

(c)

(c)

b1

Deleted: for
Deleted:
Deleted: for
Deleted: for

Deleted:
Deleted:
Deleted:
Deleted:
Commer

Deleted:
Deleted:

b5

Comment [mrl4]:

Deleted:
Deleted:

L

(s)

(c)

(c)

The Article 29 Working Party [b5] noted, "The Working Party considers that information should be provided to passengers no later than the moment when the passenger gives their agreement to buy the ticket."

Even if the transfer of PNR data has become in practice a condition for traveling to the US, passengers are only aware of what that means in terms of the processing of their personal data if the information is given to them before they buy the ticket.

c b5

Deleted:

Deleted:

Deleted:

001259

(c)

Deleted: their
Deleted: a

Deleted: to

(c)

Deleted: [b5]
Deleted: [b5]

Deleted: has

(c)

b1

Deleted: [b5]
Deleted: [b5]

Deleted: n

Deleted: is

Deleted: [b5]

Deleted: to

Deleted: a

(c).

Deleted: e

(c)

(c).

Deleted: [b5]
Deleted: [b5]
Deleted: [b5]

(c)

Deleted: of the

10/1/77

Deleted: pressed

(c)

Deleted: [b5]
Deleted: c

|

b1

Deleted: issue

(c)

Deleted: [b5]

cc: Paul Rosenzweig, Counselor

001261