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

Homeland Security

[b2] Deleted: June 26, 2006

Memorandum

TO: [b5]

FROM: [b5]

RE: (U) Passenger Name Records and Law Enforcement Information Sharing – Negotiations With The European Union

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

(U) For flights between Europe and the U.S., the data must be made available from Europe by the airline. [b5] has long prohibited the export of personal data to countries whose legal protections are not "adequate" in the view of European data protection authorities. While the U.S. has many privacy laws, it does not have an overarching data protection regime that matches every aspect of European law. It has therefore been condemned as inadequate by European standards, and commercial data transfers to the U.S. have long been restricted. European airlines feared (with reason) that European data protection agencies would view the PNR transfers in the same light and would impose fines and other penalties on airlines that provided the PNR data to the U.S. Government. Deleted [b5]

(U) To ease these fears, in May 2004, the United States entered into an agreement with the EU regarding the transmission of PNR data from European air carriers to the USG. [b5] Deleted Deleted Deleted Deleted Deleted [b5]

Arrivals Schneider MPA
Depart: 12:20

(31)

(183)

[b5]

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

Deleted: [b5]
Deleted:
Deleted:

(C/PG MLA)

(C) b1

Deleted [b5]

(U) **Background**

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

(C) b1

(U) [1] CBP can share PNR data with other law enforcement agencies, on a case-by-case basis and only for the purpose of combating terrorism and serious transnational crimes.

(c) b1

(v) The most significant of these limitations. from our perspective are the following:

(c)

1 .

(c) b1

(c)

(c)

(c) b1

(C)

(C)

b1

(C)

(S)

Formatted: Not Highlight

(U) [3] PNR can also be used and transferred to address significant health risks under Paragraph 34. As noted below, despite this authorization the EU's Article 29 Working Party has concluded that CDC's plans to retain PNR data for health-related purposes violates EU law.

(U) [4] 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."

Formatted: Font: 11 pt

Formatted: Font: 11 pt

(C)

b1

(S) b1

(S) **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.

(S) b1

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

(C) b1 (C) b1

(U) Formatted: Not Highlight

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 [b5] Last October the EU put forward b5 draft documents that concern data sharing and protection in the law enforcement context. They consist of a draft directive of the European Parliament and Council on the retention of data and a proposed Council decision on the protection of personal data in criminal matters. [b5] as it would regulate the *exchange* of law enforcement data between member states and third parties.

Deleted: [b5]

Deleted: .

Deleted: .

Deleted: and - of

Deleted: [b5] on

Deleted: T

Deleted: [b5]

Deleted: added

b1

Deleted: .

Deleted: the

7 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.

b1

Communicable Diseases.

reaction to another US initiative relating to avian flu. If air passengers are exposed to a pandemic strain of avian flu, the government will need to locate all of the passengers and crew, quickly. So the Centers for Disease Control has proposed a rule requiring airlines to retain PNR for up to 60 days for that purpose. The top data protection authorities of Europe, known as the "Article 29 Working Party," have now decided that this sort of data retention violates EU privacy directives. If given effect, the Working Party's opinion would place air carriers at legal jeopardy because of inconsistent legal régimes. It reflects a widespread EU view that privacy trumps even the critical public health interests of the United States.[11]

Deleted:

Analysis & Recommendation

States are likely to extend these requirements to pure bilateral exchanges to avoid the perception that such exchanges are subject to a lower level of protection.

[9] 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

[10] If adopted, the Draft Decision could conflict with a number of binding and non-binding information sharing arrangements that the United States has signed. For example, we have signed a 2003 Mutual Legal Assistance Agreement (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 with the directive.

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

[12] 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)

1

b1

(C)

Formatted: Font: Not Italic

(C) b1

Conclusion

(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.

(C)

b1

(S)

[b2]

Deleted:
Deleted:

Memorandum

TO: J.D. Crouch, Assistant to the President and Deputy National Security Advisor

FROM: Michael Jackson, Deputy Secretary

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

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. [b5] 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 [b5] before the plane takes off, protecting against mid-flight hijackings and bombings.

Deleted: This

(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.

Deleted: e
Deleted: are
Deleted:

[b5]

(u) [redacted]

002411

Released from Schneider in FR
Declassify Sept 30 2022

European airlines feared (with reason) that European data protection agencies would view the PNR transfers as governed by the existing commercial privacy rules and would impose fines and other penalties on airlines that provided the PNR data to the U.S. Government. To ease these fears, in May 2004, the United States entered into an agreement with the EU regarding the transmission of PNR data from European air carriers to the USG. The Agreement is accompanied by a determination that [b5] "adequate" by European standards as long as the U.S. adheres to numerous detailed prescriptions worked out with EU negotiators (but unilaterally implemented by DHS).

(u) [b5]

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.

(u) [b5]

c/FGI-MOU

61

[b5]

[1] CBP can share PNR data with other law enforcement agencies, on a case-by-case basis and only for the purpose of combating terrorism and serious transnational crimes. However, this restriction prevents PNR information from being shared in bulk with the intelligence and law enforcement communities or providing those agencies direct access to such records. This broader access would allow other law enforcement agencies to further investigate patterns of individuals not deemed to be high risk or develop new leads through the additional assessment of connections between passengers. ICE, for example, has expressed its frustration over losing access to this information. [b5]

Deleted: [b5]
Deleted:
Deleted:
Deleted:
Deleted: [b5]
Deleted:
Deleted:
Deleted:
Deleted:
Deleted:
Deleted:
Deleted: [b5]
Deleted:
Deleted:
Deleted:
Deleted:
Deleted:
Formatted: Font: 11 pt
Deleted: under
Formatted: Font: 11 pt
Formatted: Font: 11 pt

Deleted:
Formatted: Not Highlight
Deleted:
Deleted:
Deleted:
Deleted:
Deleted:
Deleted:
Deleted:
Deleted:

Background

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

Deleted:

Deleted:
Deleted:

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

(c)

Deleted:
Deleted:

(c) b1

Deleted:
Deleted: < b 5 J
Deleted:

(c)

(c)

(c) (c)

(c) b1 b1

4

092414

(c)

Deleted: [b5]

(c)

b1

Deleted: c

(S)

(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."

Formatted: Tabs: 0.59", Left + 1.38", Left + 1.77", Left + 2.17", Left + 2.56", Left + 2.95", Left + 3.35", Left + 3.74", Left + 4.13", Left + 4.92", Left + 5.32", Left + 5.71", Left

Deleted: "

(GI-non)

b1

002415

(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

(c) b1

(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.

Deleted [b5]

Deleted: [b5]

(c) b1

(c) b1

(c)

(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 [b5] 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. This later proposal

(s) b1

(c);

(5)

Deleted: agreements

(c)

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

(u)

Communicable Diseases. [redacted]

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. [12]

Analysis & Recommendation

[redacted]

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

If adopted [redacted] 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 with the directive.

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

Deleted: b 5 D

Deleted:

Deleted:

Deleted: b 5 D

Deleted: b

Deleted:

Deleted: A

(S) b1

Conclusion

(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 EC 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.

(c) b1

(S)

Homeland Security

[b2]

Deleted:

Memorandum

TO: J.D. Crouch, Assistant to the President and Deputy National Security Advisor

FROM: Michael Jackson, Deputy Secretary

RE: (U) Passenger Name Records and Law Enforcement Information Sharing – Negotiations With The European Union

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. [b5] 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 [b5] before the plane takes off, protecting against mid-flight hijackings and bombings.

Deleted: This

(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 [

Deleted: c

Deleted: are

Deleted:

[b5]

[b1]

Derived from: Schneider MFR
Declassify on: 31 Dec. 2021

European airlines feared (with reason) that European data protection agencies would view the PNR transfers as being governed by the EU's commercial regulations and would impose fines and other penalties on airlines that provided the PNR data to the U.S. Government. To ease these fears, in May 2004, the United States entered into an agreement with the EU regarding the transmission of PNR data from European air carriers to the USG. The Agreement is accompanied by a determination that [b5] "adequate" by European standards as long as the US adheres to numerous detailed prescriptions worked out with EU negotiators (but unilaterally implemented by DHS). [b5]

(U)

Deleted: [b5]
Deleted:
Deleted:

Deleted [b5]

Deleted:

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 form 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. [b5]

(U)

Deleted:

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

(U)

Deleted: plans to seek

Formatted: Normal
Formatted: Font: 11 pt

(different mod)

b1

Formatted: Font: 11 pt

(C)

Formatted: Font: 11 pt

(U) renegotiate the PNR Agreement under the Third Pillar. [redacted] the Commission, [redacted] portrayed [redacted] as a technical change that would put the same agreement back in place, albeit under a different legal authority.

Deleted:
Formatted: Superscript
Deleted: T
Deleted: has
Deleted: a

(C)

(C) b1

Deleted: and use
Formatted: Not Highlight
Deleted: limiting
Deleted: is not

(C)

Deleted: b5 2

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.

Deleted: C

(C) b1

(b)(1)

b1

Deleted: the

Deleted: Agency

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

(c)

Deleted:

Deleted: which

(c)

b1

Deleted:

(c)

b1

Deleted: [65]

(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."

(U) [5] 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.

(a) b1

(b) That is what the EU proposes to do. It [redacted] authority [redacted] 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.

Deleted: [b5]

(c) (b) b1

Deleted: Made-in-Brussels

(c)

b1

(b) **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 [b5] last October the EC 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) b1

(s)

(J) [1] 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

(S)

Deleted: agreements

b1

(C)

(C)

c|FGI MOD

(U) ** 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) ** If adopted [redacted] 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 with the directive.

Communicable Diseases. European reaction to another U.S. 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

Deleted:
Deleted:
Deleted:
Deleted:

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

[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

(c)

(c)

b1

(c)

Conclusion

(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.

b1

10

Homeland Security

June 2[illegible], 2006

Memorandum

SECRET

TO: [b5]

FROM: [b5]

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

Purpose

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

Summary

Before September 11, the government knew very little about the people getting on planes bound for the United States. After the attacks, airlines were required to provide information about their U.S.-bound passengers. This information – name, contact information, and the like – was drawn from information supplied to the airline as part of the reservation process. DHS uses the information to screen for no-fly violators and terrorist suspects before the plane takes off, protecting against midflight hijackings and bombings.

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

To ease these fears, in May 2004, the United States entered into an agreement with the EU regarding the transmission of PNR data from European air carriers to the USG. The Agreement is accompanied by a determination that US law is "adequate" by European standards as long as the US adheres to numerous detailed prescriptions worked out with EU negotiators (but unilaterally implemented by DHS). [b5]

002542

186

E 65

The PNR Agreement is 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 EC 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 purposes. Law enforcement and public security are only partly within the EU's authority; they fall under the "Third Pillar," where the authority of EU central institutions (the Commission, Parliament and Court of Justice) is more limited and more authority is left to the Member States. Because the agreement was entered under the wrong authority, the ECJ ruled it invalid but delayed the effective date of its decision until September 30 in the hope that the jurisdictional problem could be quickly solved. To cure the problem, the EU plans to seek authority from the Member States to renegotiate the PNR Agreement under the Third Pillar. The Commission has portrayed this as a technical change that would put the same agreement back in place, albeit under a different legal authority.

(c)
1.4(d)

61

2
1.4(d)

(d)

[redacted]

002543

Background

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

b1

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

b1

b1

002544

b1

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

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."

b1

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 [illegible] the European Court of Justice (ECJ) challenging the information sharing arrangement.

b1

That is what the EU proposes to do. It is seeking authority to erect substantially the same agreement on a new foundation. In order to meet the European Court of Justice deadline, the Commission will

b1

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 U.S. Undertakings provided "adequate" privacy protections, the EU-Canada agreement authorizes Canada to share PNR data received from the EU with the U.S. Even though the ECJ has struck down the EU-U.S. 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 U.S.-Canada information sharing derived from EU-originated flights.

b1

seek to codify its position over the next couple of weeks and then will call for agreement on the new arrangement by September 30.

(c)

b1

b1

Communicable Diseases. b5 European reaction to another U.S initiative relating to avian flu. If all passengers are exposed to a pandemic

[b5]

b1

If adopted, the Draft Decision could conflict with a number of binding and non-binding information sharing arrangements that the United States has signed. For example, we have signed a 2003 Mutual Legal Assistance Agreement (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 with the directive.

strain. Even in 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 in 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."

Analysis & Recommendation

(C)
1.9(d)

(C)
1.4(d)

b1

(C)
1.4(a)

(C)
1.4(

(C)

(C)

Conversely, Paragraph 34 of the Undertakings allows for the exchange of PNR for public health purposes and neither the Commissioner of the Article 29 committee have challenged the DHS-HHS MOU.

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. It is possible that actions taken on PNR are likely to set precedents for further communication on law enforcement matters.

b1

Conclusion

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

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

b1

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

Homeland Security

[62]

Deleted: June 28, 2004

Memorandum

TO: [65]

FROM: [65]

RE: (U) Passenger Name Records and Law Enforcement Information Sharing – Negotiations With The European Union

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

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

(U) To ease these fears, in May 2004, the United States entered into an agreement with the EU regarding the transmission of PNR data from European air carriers to the USG. The Agreement is accompanied by a determination that [65] "adequate" by European standards as long as the US adheres to numerous detailed prescriptions worked out with EU negotiators (but unilaterally implemented by DHS). [65]

Deleted [65]

002551

Derived from: Schneider MFR
Declassify on: 31 Dec. 2031

(187)

b1

(C)

Background

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

(C) b1

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

(C) b1

(C)

(C)

(C)

b1

(C)

(C)

(S)

Deleted: w

Deleted: ;

Deleted: to

Deleted: [b5]

Deleted: T

Deleted: [b5]

Deleted: to

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

(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."

(S) b1

Formatted: Not Highlight
Deleted: [b5]
Deleted: is
Deleted: find

(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.

(S) b1

Deleted:

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

(S FGI NATO) b1

Formatted: Font: 11 pt
Formatted: Font: 11 pt

(U) 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.

(C)

(C)

b1

b1

(C)

(C)

(S)

Deleted: added

Deleted:

Deleted: the

(U) 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)

b1

(C)

Communicable Diseases. [redacted] b5 [redacted] European reaction to another US initiative relating to avian flu. If air passengers are exposed to a pandemic strain of avian flu, the government will need to locate all of the passengers and crew, quickly. So the Centers for Disease Control has proposed a rule requiring airlines to retain PNR for up to 60 days for

(U)

---

draft mod

b1

[10] 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)

[11] If adopted, the Draft Decision could conflict with a number of binding and non-binding information sharing arrangements that the United States has signed. For example, we have signed a 2003 Mutual Legal Assistance Agreement (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 with the directive.

(U)

that purpose. The top data protection authorities of Europe, known as the "Article 29 Working Party," have now decided that this sort of data retention violates EU privacy directives. If given effect, the Working Party's opinion would place air carriers at legal jeopardy because of inconsistent legal régimes. It reflects a widespread EU view that privacy trumps even the critical public health interests of the United States.[12]

Deleted:

Analysis & Recommendation

(C)

(C)

b1

(C)

(C)

(S)

(U)

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

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

(S) (C)↓ b1

(C) b1

(C)

Conclusion

(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.

(c[redacted])

(5)

b1

Page 2: [1] Deleted sb 6/26/2006 10:47:00 AM

Before September 11, the government knew very little about the people getting on planes bound for the United States. After the attacks, airlines were required to provide information about their U.S.-bound passengers. This information – name, contact information, and the like – was drawn from information supplied to the airline as part of the reservation process. DHS uses the information to screen for no-fly violators and terrorist suspects before the plane takes off, protecting against midflight hijackings and bombings.

(U)

For flights between Europe and the U.S., the data must be

Page 2: [2] Deleted sb 6/26/2006 10:48:00 AM

made available from Europe [b5] has long prohibited the export of personal data to countries whose legal protections are not "adequate" in the view of European data protection authorities. While the U.S. has many privacy laws, it does not have an overarching data protection regime that matches every aspect of European law. It has therefore been condemned as inadequate by European standards, and commercial data transfers to the U.S. have long been restricted. European airlines feared (with reason) that European data protection agencies would view the PNR transfers in the same light and would impose fines and other penalties on airlines that provided the PNR data to the U.S. Government.

(U)

[b5]

(U)

Page 2: [3] Deleted sb 6/26/2006 10:50:00 AM

[b5]

Page 2: [4] Deleted sb 6/26/2006 10:50:00 AM

(U) May 2004, the United States entered into an agreement with the EU regarding the transmission of PNR data from European air carriers to the USG.

Page 2: [5] Deleted sb 6/26/2006 10:50:00 AM

(C) b1

Page 2: [6] Deleted sb 6/26/2006 10:50:00 AM

(C) b1

Page 2: [7] Deleted sb

(C) b1

Page 2: [8] Deleted sb 6/26/2006 10:50:00 AM

(C) b1

Page 2: [9] Deleted sb 6/26/2006 10:50:00 AM

(C) b1

(U) [1] CBP can share PNR data with other law enforcement agencies, on a case-by-case basis and only for the purpose of combating terrorism and serious transnational crimes.

Page 2: [10] Deleted	sb	6/26/2006 10:50:00 AM
Page 2: [11] Deleted	sb	6/26/2006 10:50:00 AM
Page 2: [12] Deleted	sb	6/26/2006 10:52:00 AM

bl

bl

Derived: Schneider MPR
Declass 12/2021

413.1

[b2]

Memorandum

TO: J.D. Crouch, Assistant to the President and Deputy National Security Advisor

FROM: Michael Jackson, Deputy Secretary

RE: (U) Passenger Name Records and Law Enforcement Information Sharing – Negotiations With The European Union

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

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

(U) To ease these fears, in May 2004, the United States entered into an agreement with the EU regarding the transmission of PNR data from European air carriers to the USG. The Agreement is accompanied by a determination that CBP's use of PNR is "adequate" by European standards as long as the US adheres to numerous detailed prescriptions worked out with EU negotiators (but unilaterally implemented by DHS). [b5]

002563

186

[65]

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

(U)

(C)

b1

(C)

(C)

002564

(U) [1] CBP can share PNR data with other law enforcement agencies, on a case-by-case basis and only for the purpose of combating terrorism and serious transnational crimes.

(U) **Background**

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

(C) b1

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

- (C) b1
- (C)

2

(C) b1

(C)

(C)

b1

(C)

(C)

(S)

(C) [3] PNR can also be used and transferred to address significant health risks under Paragraph 34. As noted below, despite this authorization the EU's Article 29 Working Party has concluded that CDC's plans to retain PNR data for health-related purposes violates EU law.

(C) [4] 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) b1

(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.

(C) b1

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

(C) b1

C/FOR mtd b1

002567

(C) [6] 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.

(c)

(e) b1

(f)

(5.

002568

(4) [7] 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)

b1

(C)

Communicable Diseases. (C) b5

(U) 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

---

C/POP mcl

b1

(U) [9] 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

[10] If adopted, the Draft Decision could conflict with a number of binding and non-binding information sharing arrangements that the United States has signed. For example, we have signed a 2003 Mutual Legal Assistance Agreement (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 with the directive.

(U)

inconsistent legal régimes. It reflects a widespread EU view that privacy trumps even the critical public health interests of the United States. [11]

Analysis & Recommendation

(C)

(S)

b1

(C)

(S)

(U) [11] Conversely, Paragraph 34 of the Undertakings allows for the exchange of PNR for public health purposes and neither the Commission or the Article 29 Committee have challenged the DHS-HHS MOU.

(U) [12] 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)

(C) b1

(C)

Conclusion

(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.

(C) b1

002571

(c)

(5.)

b1

/

/

Homeland Security

July 5, 2006

Memorandum

TO: J.D. Crouch, Assistant to the President and Deputy National Security Advisor

FROM: Michael Jackson, Deputy Secretary

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

Purpose

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

Summary

Before September 11, the government knew very little about the people getting on planes bound for the United States. After the attacks, airlines were required to provide information about their U.S.-bound passengers. This information – name, contact information, and the like – was drawn from, [b5] information supplied to the airline as part of the reservation process. DHS uses the information to screen for no-fly violators and terrorist suspects [b5] before the plane takes off, protecting against mid-flight hijackings and bombings.

For flights between Europe and the U.S., the data must be made available from European air carriers. EU law has long prohibited the commercial export of personal data to countries whose legal protections have not been deemed "adequate" in the view of European data protection authorities. While the U.S. has many privacy laws, it does not have an overarching data protection regime that corresponds to every aspect of European law. It has therefore been viewed as "inadequate" by European standards, and commercial data transfers to the U.S. have long been restricted [

[b5]

]

Deleted:

Deleted:

Deleted:

b1

Derivative: Schneider NFR
Declassification: 5 July 2021

002573

In 2003, European airlines feared with reason that European data protection agencies would view the PNR transfers as being governed by EU's commercial privacy regime and would impose fines and other penalties on airlines that provided the PNR data to the U.S. Government. To ease those fears, in May 2004, the United States entered into an agreement with the EU regarding the transmission of PNR data from European air carriers to the USG. The Agreement is accompanied by a determination that [b5] "adequate" by European standards as long as the US adheres to numerous detailed prescriptions worked out with EU negotiators but unilaterally implemented by DHS. [

[b5]

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 [redacted] in the EU's commercial data protection laws, and are only partly within the EU's authority; they fall under the "Third Pillar," where the authority of EU central institutions like the Commission, Parliament and Court of Justice) is more limited and more authority is left to the Member States. [

[b5]

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 9/30/06 and has set a goal of establishing a new agreement by the September 30th expiration of the current arrangement. While DHS has not yet received a proposed replacement text from the Commission, they have portrayed their proposal as a technical change that would put the same agreement back in place, albeit under a different legal authority.

Deleted [b5]

[redacted] CBP can share PNR data with other law enforcement agencies on a case-by-case basis and only for the purpose of combating terrorism and serious transnational crimes.

[b5]

[b5]

002574

(C)

(C)
4(d)

b1

[b5]

Deleted:
Formatted:
Delete: [b5]
Deleted:

(C)
4(d)

[b5]

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.

Deleted:

(C)

b1

(C)

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

(C)

[b5]

(C) b1

(C)

(C)

(C) b1

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

(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."

Formatted: Para, Tabs: 0.59" Left + 1.36" Left + 1.77" Left + 2.17" Left + 2.56" Left + 2.95" Left + 3.35" Left + 3.74" Left + 4.13" Left + 4.92" Left + 5.32" Left + 5.71" Left

Deleted: 1

(C)

b1

/

(U) That is what the EU proposes to do. It [illegible] 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 ratify its position over the next couple of weeks and then will call for agreement on the new arrangement by September 30.

Deleted [65 J

Deleted [65 J

(S)

b1

(S)

(U) 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 U.S. 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.

/

(C)

(S) b1

(C)

(C)

(U) 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 NOFORN) b1

(U) 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

Communicable Diseases. (b5)

(U) European reaction to another U.S. 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 96 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.[5]

Analysis & Recommendation

(C) (b1)

(C)

Deleted: C
Deleted: El

(b5) (U) If adopted, the Draft Decision could conflict with a number of binding and non-binding information sharing arrangements that the United States has signed. For example, we have signed a 2003 Mutual Legal Assistance Agreement (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 with the directive.

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

(U) 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.

(c)

المصدر

(c)

b1

(s)

Formatted: Highlight

(c)

(c)

002581

Conclusion

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

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

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

Homeland Security

[62]

Deleted: June 30, 2006

Memorandum

TO: [65]

FROM: [65]

RE: (U) Passenger Name Records and Law Enforcement Information Sharing – Negotiations With The European Union

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

(U) For flights between Europe and the U.S., the data must be made available from Europe [65] has long prohibited the export of personal data to countries whose legal protections are not "adequate" in the view of European data protection authorities. While the U.S. has many privacy laws, it does not have an overarching data protection regime that matches every aspect of European law. It has therefore been condemned as inadequate by European standards, and commercial data transfers to the U.S. have long been restricted. European airlines feared (with reason) that European data protection agencies would view the PNR transfers in the same light and would impose fines and other penalties on airlines that provided the PNR data to the U.S. Government.

Deleted: scat

(U) To ease these fears, in May 2004, the United States entered into an agreement with the EU regarding the transmission of PNR data from European air carriers to the USG. The Agreement [[65]]

Deleted: [65]
Deleted:
Deleted:
Deleted: atc
Deleted: set by

DERIVED From: Schneider MFR
Declass on: 12 June 2029

Not 3

002583

[b5]

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

(U)

Deleted: [b5]
Deleted:
Deleted:

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

(U)

(C) b1

Deleted [b5]

Background

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

(U)

(C) b1

(U) [1] CBP can share PNR data with other law enforcement agencies on a case-by-case basis and only for the purpose of combating terrorism and serious transnational crimes.

002584

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

(c)

(c) b1

(c)

(c) b1

002585

(c)

(c) b1

(S)

Formatted: Not Highlight

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

(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/s) b1

Formatted: Font: 11 pt

Formatted: Font: 11 pt

002586

(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.

(S) b1

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

(S) b1

(S) b1

(U) 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.

Formatted: Not Highlight

Deleted: three

Deleted:

Deleted:

Deleted: end - of

Deleted: [65 J

Deleted: T

Deleted: [65 J

Deleted: added

Deleted:

Deleted: the

(C)

(C)

b1

(S)

(C)

(U) 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.

(4 FGI) MEO

b1

002585

(C) b1

Communicable Diseases. (U) reaction to another US initiative relating to avian flu. If air passengers are exposed to a pandemic strain of avian flu, the government will need to locate all of the passengers and crew, quickly. So the Centers for Disease Control has proposed a rule requiring airlines to retain PNR for up to 60 days for that purpose. The top data protection authorities of Europe, known as the "Article 29 Working Party," have now decided that this sort of data retention violates EU privacy directives. If given effect, the Working Party's opinion would place air carriers at legal jeopardy because of inconsistent legal régimes. It reflects a widespread EU view that privacy trumps even the critical public health interests of the United States.[11]

Deleted:

Analysis & Recommendation

(C) b1

(U) [9] 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) [10] If adopted, the Draft Decision could conflict with a number of binding and non-binding information sharing arrangements that the United States has signed. For example, we have signed a 2003 Mutual Legal Assistance Agreement (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 with the directive.

(U) [11] Conversely, Paragraph 34 of the Undertakings allows for the exchange of PNR for public health purposes and neither the Commission or the Article 29 Committee have challenged the DHS-HHS MOU.

(c)

(c)

b1

(c)

(s)

(u)

[12] 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.

002590

Formatted: Font: Not Bold

(C)

b1

Conclusion

(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.

(C)

b1

(S)

002591

[b2]

Deleted: [illegible]

Memorandum

TO: [b5]

FROM: [b5]

RE: (U) Passenger Name Records and Law Enforcement Information Sharing – Negotiations With The European Union

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) [redacted]

(U) [redacted]

(U) [redacted] CBP's use of PNR [redacted]

Deleted: [b5]

[b5]

Derived From: Schneier-MFR
Declassify On: [redacted]
June 2021

002592

(191)

E b5]

(U) "First Pillar" authority the authority that the EU relied on in entering the Agreement. The ECJ [b5] held that the U.S. wanted PNR data for law enforcement and public security reasons. Law enforcement and public security are the EU's authority they fall 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.

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

(C) b1

(C)

(U) CBP can share PNR data with other law enforcement agencies, on a case-by-case basis and only for the purpose of combating terrorism and serious trans-national crimes

(C) b1

Deleted: [b5]

002593

(c) (b)1

Background

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

(c) (b)1

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

(c)

(b)1

(c)

002594

(C)

(C)

b1

(C)

(C)

(S)

Deleted:
Deleted:
Deleted:
Deleted:
Deleted: 7
Deleted:
Deleted: to

[b5]

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

(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."

b1

Formatted:
Deleted:
Deleted: [b5]
Deleted:

(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.

(C) b1

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

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

Formatted:
Formatted:

dFGAT
3/10/05

b1

(U) 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 EC-US agreement, the EU contends that its similar agreement with Canada remains in effect. Some Canadian government sources are concerned, however, that the absence of an "adequacy" finding (which is a First Pillar concept) may now have the effect of *prohibiting* US-Canada information sharing derived from EU-originated flights.

Deleted:

Deleted: [b5]
Formatted:
Formatted:

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

b1

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

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.

Deleted:
Deleted:
Deleted:
Deleted:

Deleted:
Deleted:

Deleted: [b5
Deleted:
Deleted:]

b1

(C)

(C)

b5 (W)

Communicable Diseases. C b5

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

b1

(FOR MOD.

(U)

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) If adopted, the Draft Decision could conflict with a number of binding and non-binding information sharing arrangements that the United States has signed. For example, we have signed a 2003 Mutual Legal Assistance Agreement (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 with the directive.

002598

[illegible] for that purpose. The top data protection authorities in EU 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.

Deleted:

Deleted:

Analysis & Recommendation

(b)(5)

(b)(1)

(b)(5)

(2) Conversely, Paragraph 34 of the Undertakings allows for the exchange of PNR for public health purposes and neither the Commission or the Article 29 Committee have challenged the DHS HHS MOU.

(b)(5) 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.

Formatted:
Deleted:
Deleted:
Deleted:
Deleted:
Deleted:

(S) b1 b5

(S) Deleted: b5
Formatted:
Deleted: b5

(S) b1

Conclusion

(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 U.S 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

(5) b1

Deleted
Deleted
Deleted [b5]

Page 2: [1] Deleted sb 6/26/2006 10:47:00 AM

Before September 11, the government knew very little about the people getting on planes bound for the United States. After the attacks, airlines were required to provide information about their U.S.-bound passengers. This information – name, contact information, and the like – was drawn from information supplied to the airline as part of the reservation process. DHS uses the information to screen for no-fly violators and terrorist suspects before the plane takes off, protecting against midflight hijackings and bombings.

For flights between Europe and the U.S., the data must be

Page 2: [2] Deleted sb 6/26/2006 10:48:00 AM

[b5] has long prohibited the export of personal data to countries whose legal protections are not "adequate" in the view of European data protection authorities. While the U.S. has many privacy laws, it does not have an overarching data protection regime that matches every aspect of European law. It has therefore been condemned as inadequate by European standards, and commercial data transfers to the U.S. have long been restricted. European airlines feared (with reason) that European data protection agencies would view the PNR transfers in the same light and would impose fines and other penalties on airlines that provided the PNR data to the U.S. Government.

[b5]

Page 2: [3] Deleted sb 6/26/2006 10:50:00 AM

[b5]

Page 2: [4] Deleted sb 6/26/2006 10:50:00 AM

May 2004, the United States entered into an agreement with the EU regarding the transmission of PNR data from European air carriers to the USG.

Page 2: [5] Deleted sb 6/26/2006 10:50:00 AM

b1

Page 2: [6] Deleted sb 6/26/2006 10:50:00 AM

b1

Page 2: [7] Deleted sb 6/26/2006 10:50:00 AM

b1

Page 2: [8] Deleted sb 6/26/2006 10:50:00 AM

b1

Page 2: [9] Deleted sb 6/26/2006 10:50:00 AM

b1

Page 2: [10] Deleted		sb	6/26/2006 10:50:00 AM
Page 2: [11] Deleted	b1	sb	6/26/2006 10:50:00 AM
Page 2: [12] Deleted	b1	sb	6/26/2006 10:52:00 AM

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

Homeland Security

(b2)

Memorandum

TO: J.D. Crouch, Assistant to the President and Deputy National Security Advisor

FROM: Michael Jackson, Deputy Secretary

RE: (U) Passenger Name Records and Law Enforcement Information Sharing – Negotiations With The European Union

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

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

(U) To ease these fears, in May 2004, the United States entered into an agreement with the EU regarding the transmission of PNR data from European air carriers to the USG. The Agreement is accompanied by a determination that CBP's use of PNR is "adequate" by European standards as long as the US adheres to numerous detailed prescriptions worked out with EU negotiators (but unilaterally implemented by DHS). (b5)

Derived From: Schneider MFR
Declass on: 21 Sept 2022

002623

(592.1)

(93)

(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 only partly within the EU's authority; they fall under the "Third Pillar," where the authority of EU central institutions (the Commission, Parliament and Court of Justice) is more limited and more authority is left to the Member States. Because the agreement was entered under the wrong authority, the Court ruled it invalid but delayed the effective date of its decision until September 30 in the hope that the jurisdictional problem could be quickly solved. To cure the problem, the EU plans to seek authority from the Member States to renegotiate the PNR Agreement under the Third Pillar. The Commission has portrayed this as a technical change that would put the same agreement back in place, albeit under a different legal authority.

(U) [1] CBP can share PNR data with other law enforcement agencies, on a case-by-case basis and only for the purpose of combating terrorism and serious transnational crimes.

b1

Background

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

(C b1

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

- (C)

b1

-

(C

(C)[2] b1

002625

(C)

(C) b1

(C)

(C)

(S

(U) [3] PNR can also be used and transferred to address significant health risks under Paragraph 34. As noted below, despite this authorization the EU's Article 29 Working Party has concluded that CDC's plans to retain PNR data for health-related purposes violates EU law.

(U) [4] 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."

EC

b1

(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.

(S) b1

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

(S) b1

(S)[5] b1

[5] 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. (U) 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.

(C) b1

(C)

(S

[7] For example, the Draft Decision contains provisions on time limits for retention of shared data, ensuring the (U) 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

b1

(C;

Communicable Diseases. [

b5

(U)] 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

c/FGI MOD

b1

[9] 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 (U) grounds that the Commission did not have the legal authority to grant it

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

inconsistent legal régimes. It reflects a widespread EU view that privacy trumps even the critical public health interests of the United States. [11]

Analysis & Recommendation

(C)

(C) b1

(C)

(S)

(U) [11] Conversely. Paragraph 34 of the Undertakings allows for the exchange of PNR for public health purposes and neither the Commission or the Article 29 Committee have challenged the DHS-HHS MOU.

(U) [12] 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.

(C)

b1

(C

Conclusion

(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.

(C

b1

002631

(s) b1

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

Homeland Security

[b2]

Memorandum

TO: [b5]

FROM: [b5]

RE: (U) Passenger Name Records and Law Enforcement Information Sharing – Negotiations With The European Union

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

[b5]

(U) United States entered into an agreement with the EU, regarding the transmission of PNR data from European air carriers to the USG. [b5]

[b5]

[b5]

(U) Justice (ECJ) struck down the Agreement, not on substantive grounds but on procedural ones. Under EU law, commercial issues are within the competence of the EU and fall under the "First Pillar" authority – the authority that the EU had relied on in entering the Agreement. [b5]

[b5]

(U) The EU now [b5] seek authority from the Member States to renegotiate the PNR Agreement under the Third Pillar. [b5] have portrayed this as a technical change that would put the same agreement back in place, albeit under a different legal authority.

(U) b1

DERIVED FROM: Schneider Memo
Declass on: 21 Sept 2022

002633

190

193

b1

Background

1

(c)

b1

(c)

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

(c)

b1

(c)

b1

(S)

(S)

b1

(S)

(S)

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

(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 the Information Sharing Environment."

(C)

b1

(C)

'C|FGI'
MOD.

(U) Negotiations will, therefore, soon begin in earnest, against a September 30 deadline. There is need, therefore, for the early finalization of a USG negotiating position.

(U) [4] Acting under the First Pillar, the EU has also entered into a PNR sharing agreement with Canada. In light of the EU's determination that the US Undertakings provide "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. Canada is concerned, however, that any new EU-US agreement will come without an "adequacy" finding (since those are a First Pillar concept) and thus that the continued EU-Canada agreement will now have the effect of *prohibiting* US-Canada information sharing derived from EU-originated flights.

(C)

(C)

b1

(S)

(S)

(C)

(U) 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 mirrors, in many ways, existing use and sharing limitations in the PNR Agreement and the Undertakings

FGI MOD

b1

(c) b1

(c)

(a) **Communicable Diseases.** One final piece of the puzzle bears brief mention. The USG, through the Centers for Disease Control, has published a draft NPRM relating to the retention of PNR data for potential use in the control of communicable diseases. The regulation would authorize the retention of such data for up to 60 days in order to enable CDC to contact international air travelers who are subsequently determined to have been exposed to a communicable disease such as SARS or Avian Flu.

(c) b1

(b) The adequacy finding granted to the U.S. is specific to the transfer of PNR data and only extends to its transmission to CBP.

(d) If adopted, the Draft Decision could conflict with a number of binding and non-binding information sharing arrangements that the United States has signed. For example, we have signed a 2003 Mutual Legal Assistance Agreement (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 with the directive.

Analysis & Recommendation

(C)

(C

(C

(C

(C

(S)

(U) 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.

(C) b1

(C)

Conclusion

(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 it involved the exchange of commercial information that requires special protections under EU law. The European Court of Justice has now held that the information is law enforcement information, not commercial information.

(C) b1

(S)

Department of Homeland Security
Washington, DC 20528

Homeland Security

[62]

Memorandum

TO: [65]

FROM: [65]

RE: (U) Passenger Name Records and Law Enforcement Information Sharing – Negotiations With The European Union

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

(U) For flights between Europe and the U.S., the data must be [65] has long prohibited the export of personal data to countries whose legal protections are not "adequate" in the view of European data protection authorities. While the U.S. has many privacy laws, it does not have an overarching data protection regime that matches every aspect of European law. It has therefore been condemned as inadequate by European standards, and commercial data transfers to the U.S. have long been restricted. European airlines feared (with reason) that European data protection agencies would view the PNR transfers in the same light and would impose fines and other penalties on airlines that provided the PNR data to the U.S. Government.

(U) To ease these fears, in May 2004, the United States entered into an agreement with the EU regarding the transmission of PNR data from European air carriers to the USG. The Agreement [65] 'adequate" by European standards as long as the US adheres to numerous detailed prescriptions [65]

Deleted: [65]

Delete

Derived: Schneider MPR
Declas: 12/2021

32

002641

194

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

- (c)
- (c) b1
- (c)
- (c)

(c) b1

(v) [2] PNR can also be used and transferred to address significant health risks under Paragraph 34. As noted below, despite this authorization the EU's Article 29 Working Party has concluded that CDC's plans to retain PNR data for health-related purposes violates EU law.

(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) b1

(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."

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

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.

(S)

b1

(C)

(C)

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

[6]

b1

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

Communicable Diseases.

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

Analysis & Recommendation

If adopted, the Draft Decision could conflict with a number of binding and non-binding information sharing arrangements that the United States has signed. For example, we have signed a 2003 Mutual Legal Assistance Agreement (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 with the directive.

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

Conclusion

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

the 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.

(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.

(C) b1

(S)

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

Homeland Security

July 5, 2006~~June 26, 2006~~

Memorandum

TO: [b5]

FROM: [b5]

RE: (U) Passenger Name Records and Law Enforcement ~~Information~~ Sharing – Negotiations With The European Union

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

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

(U) To ease these fears, in May 2004, the United States entered into an agreement with the EU regarding the transmission of PNR data from European air carriers to the USG. The Agreement is accompanied by a determination that [b5] 'adequate" by European standards as long as the US adheres to numerous detailed prescriptions worked out with EU negotiators (but unilaterally implemented by DHS). [b5]

DERIVED FROM: SCHNEIDER MFR
DECLASS ON: 5 July 2021

002650

(293)

(195)

/

[65]

(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 only partly within the EU's authority; they fall under the "Third Pillar," where the authority of EU central institutions (the Commission, Parliament and Court of Justice) is more limited and more authority is left to the Member States. Because the agreement was entered under the wrong authority, the Court ruled it invalid but delayed the effective date of its decision until September 30 in the hope that the jurisdictional problem could be quickly solved. To cure the problem, the EU plans to seek authority from the Member States to renegotiate the PNR Agreement under the Third Pillar. The Commission has portrayed this as a technical change that would put the same agreement back in place, albeit under a different legal authority.

(C)

(C) b1

(C)

(S) [1] CBP can share PNR data with other law enforcement agencies on a case-by-case basis and only for the purpose of combating terrorism and serious transnational crimes.

/

b1

Background

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

(c) b1

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

(c) b1

(c)

(c) b1

(c)

(c) b1

(c)

(c)

(S)

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

(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."

(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.

(C) b1

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

(S) b1

(C) b1

(U) 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.

(C)

b1

(C)

(S)

(U) 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) b1

(C

Communicable Diseases. b5

(U) > 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

(FBI MOD) b1

(U) [9] 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) [10] If adopted, the Draft Decision could conflict with a number of binding and non-binding information sharing arrangements that the United States has signed. For example, we have signed a 2003 Mutual Legal Assistance Agreement (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 with the directive.

inconsistent legal régimes. It reflects a widespread EU view that privacy trumps even the critical public health interests of the United States.[1]

Analysis & Recommendation

(C)

(C)

b1

(C)

(S)

(U) [1] Conversely, Paragraph 34 of the Undertakings allows for the exchange of PNR for public health purposes and neither the Commission or the Article 29 Committee have challenged the DHS-HHS MOU.

(U) [2] 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.

(C) b1

(C)

Conclusion

(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.

(C) b1

(C) b1

Conclusion

(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.

(C)

(S) b1

Washington, DC 20528

[redacted]

Memorandum

TO: J.D. Crouch, Assistant to the President and Deputy National Security Advisor

FROM: Michael Jackson, Deputy Secretary

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

Purpose

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

Summary

Before September 11 the government knew very little about the people getting on planes bound for the United States. After the attacks, airlines were required to provide information about their U.S.-bound passengers. This information – name, contact information, and the like – was drawn from information supplied to the airline as part of the reservation process. DHS uses the information to screen for no-fly violators and terrorist suspects before the plane takes off, protecting against mid-flight hijackings and bombings.

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

To ease these fears, in May 2004, the United States entered into an agreement with the EU regarding the transmission of PNR data from European air carriers to the USG. The Agreement is accompanied by a determination that CBP's use of PNR is "adequate" by European standards as long as the US adheres to numerous detailed prescriptions worked out with EU negotiators (but unilaterally implemented by DHS). [redacted]

Declassify Advertise MFR
Declass 12/2027

002672

19e

30

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 EC relied on in entering the Agreement. The ECJ, however, held that the US wanted PNR data for law enforcement and public security reasons. Law enforcement and public security are only partly within the EU's authority; they fall under the "Third Pillar," where the authority of EU central institutions (the Commission, Parliament and Court of Justice) is more limited and more authority is left to the Member States. Because the agreement was entered under the wrong authority, the Court ruled it invalid but delayed the effective date of its decision until September 30 in the hope that the jurisdictional problem could be quickly solved. To cure the problem, the EU plans to seek authority from the Member States to renegotiate the PNR Agreement under the Third Pillar. The Commission has portrayed this as a technical change that would put the same agreement back in place, albeit under a different legal authority.

[1] CBP can share PNR data with other law enforcement agencies on a case-by-case basis and only for the purpose of combating terrorism and serious transnational crimes.

Background

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

(C) b1

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

- (C) b1
- (C)

(C) b1

---

[2]

(c)

(c) b1

(c)

(c)

(c)

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

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

(S) b1

(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) b1

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

(U) b1

(U/FOUO)

(U) [6] 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.

(c)

(c) b1

(c)

(5)

(c) [7] 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)

b1

(C)

Communicable Diseases.

b5

(U) 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

C/FOR mvd

b1

(U) [9] 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

(C) [10] If adopted, the Draft Decision could conflict with a number of binding and non-binding information sharing arrangements that the United States has signed. For example, we have signed a 2003 Mutual Legal Assistance Agreement (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 with the directive.

inconsistent legal régimes. It reflects a widespread EU view that privacy trumps even the critical public health interests of the United States. [11]

Analysis & Recommendation

(C)

(C)

(C) b1

(S)

(C) [11] Conversely. Paragraph 34 of the Undertakings allows for the exchange of PNR for public health purposes and neither the Commission or the Article 29 Committee have challenged the DHS-HHS MOU.

(C) [12] 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)

(C) b1

(C)

Conclusion

(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.

(C) b1

002680

(C)

(S)

b1

002681

S2 C/E

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

Homeland Security

[b2]

Deleted: June 2, 2004

Memorandum

TO: [b5]

FROM: [b5]

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

Purpose

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

Summary

Before September 11, the government knew very little about the people getting on planes bound for the United States. After the attacks, airlines were required to provide information about their U.S.-bound passengers. This information – name, contact information, and the like – was drawn from information supplied to the airline as part of the reservation process. DHS uses the information to screen for no-fly violators and terrorist suspects before the plane takes off, protecting against midflight hijackings and bombings.

For flights between Europe and the U.S., the data must be made available from Europe [b5] has long prohibited the export of personal data to countries whose legal protections are not "adequate" in the view of European data protection authorities. While the U.S. has many privacy laws, it does not have an overarching data protection regime that matches every aspect of European law. It has therefore been condemned as inadequate by European standards, and commercial data transfers to the U.S. have long been restricted. European airlines feared (with reason) that European data protection agencies would view the PNR transfers in the same light and would impose fines and other penalties on airlines that provided the PNR data to the U.S. Government.

Deleted: west

To ease these fears, in May 2004, the United States entered into an agreement with the EU regarding the transmission of PNR data from European air carriers to the USG. The Agreement [b5]

Deleted
Deleted
Deleted
Deleted: ate
Deleted: ed

[b5]

002749

197

[b5]

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

Deleted:
Deleted:
Deleted: [b5]

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

b1

Background

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

(g) b1

[illegible]

2

002750

b1

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

b1

b1

Formatted: Not Highlight

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

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."

Formatted: Font: 11 pt

Formatted: Font: 11 pt

b1

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.

b1

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

b1

Comment [m1]: 65

Deleted:

Formatted: Not Highlight

Formatted: Not Highlight

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* U.S-Canada information sharing derived from EU-originated flights.

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 [b5]

] Last October the EU put forward [b5] draft documents that concern data sharing and protection in the law enforcement context. They consist of a draft directive of the European Parliament and Council on the retention of data [b5] proposed Council decision on the protection of personal data in criminal matters [

b5]

Deleted: [b5]

Deleted:

Deleted:

Deleted: and - of

Deleted: [b5]

Deleted: T

Deleted: [b5]

b1

Deleted: added

Deleted:

Deleted: the

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.

b1

~~Communicable Diseases.~~

European reaction to another US initiative relating to avian flu. ~~If air passengers are exposed to a pandemic~~ strain of avian flu, the government will need to locate all of the passengers and crew, quickly. So the Centers for Disease Control has proposed a rule requiring airlines to retain PNR for up to 60 days for that purpose. The top data protection authorities of Europe, known as the "Article 29 Working Party," have now decided that this sort of data retention violates EU privacy directives. If given effect, the Working Party's opinion would place air carriers at legal jeopardy because of inconsistent legal regimes. It reflects a widespread EU view that privacy trumps even the critical public health interests of the United States.[9]

Deleted:

Analysis & Recommendation

[9] 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.

[10] If adopted, the Draft Decision could conflict with a number of binding and non-binding information sharing arrangements that the United States has signed. For example, we have signed a 2003 Mutual Legal Assistance Agreement (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 with the directive.

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

b1

(S)

(S)

[12] 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. (U)

002756

Formatted: Font: Not Italic

b1

Conclusion

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

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

b1

b1

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

Homeland Security

[b2]

Deleted: July 6, 2006

Memorandum

TO: J.D. Crouch, Assistant to the President and Deputy National Security Advisor

FROM: Michael Jackson, Deputy Secretary

RE: (U) Passenger Name Records and Law Enforcement Information Sharing – Negotiations With The European Union

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 [b5] before the plane takes off[1], 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 [b5]

[b5]

[1] (U) CBP may automatically access PNR data from European carriers up to 72 hours in advance of a flight. During this predeparture 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.

Jared Schneider MFR
Declass: 12/2021

002818

33

198

In 2003, European airlines feared (with reason) that European data protection agencies would view the PNR transfers as being governed by the existing commercial requirements and would impose fines and other penalties on airlines that provided the PNR data to the U.S. Government. To ease these fears, in May 2004, the United States entered into an agreement with the EU regarding the transmission of PNR data from European air carriers to the USG. The Agreement is accompanied by a determination that [b5] "adequate" by European standards as long as the US adheres to numerous detailed prescriptions worked out with EU negotiators (but unilaterally implemented by DHS). [

b5

]

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. [

b5

]

(C) b1

[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.

(C)

b1

(C)

(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.

(C) b1

(C)

(C) b1

(S)

(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."

C/POF MUD b1

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.

b1

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.

b1

EU Proposals on Sharing Law Enforcement Information. If that were all that is at stake, this would be an interesting diplomatic and legal problem for DHS. But it is not. The PNR negotiations will be closely intertwined with a broader effort [redacted] 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. This later proposal

[7] 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.

sharing with other government agencies). This will mean additional restrictions for US agencies sharing data with Europe.[10]

(C) b1

Communicable Diseases. [b5]

~~reaction to another US initiative relating to avian flu. If air passengers are exposed to a pandemic~~ European

(U) 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.[12]

Analysis & Recommendation

(C) b1

(U) [10] 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

[11] If adopted [b5] the Draft Decision could conflict with a number of binding and

(U) 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 with the directive.

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

[12] 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.

(C) b1

Conclusion

(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.

(C) b1

(C)

UNCLASSIFIED

R1F

Secretary

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

Homeland Security

May 14, 2007

Dear Member of the European Parliament:

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

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

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

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

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

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

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

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

000361

199

UNCLASSIFIED

244

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

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

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

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

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

---

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

Unclassified

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

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

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

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

Sincerely,

Michael Chertoff

Unclassified