SECRET

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

Homeland Security

101.1

(b2)

INFORMATION

MEMORANDUM FOR: Stewart Baker

THROUGH: Marisa Lino, Senior Advisor, PLCY/OIA

FROM: Michael Scardaville, Deputy Director for European Affairs

SUBJECT: Key Issues for the May 3, 2007 PNR VTC (u)

Overview: (u)

(c)

(b1)

(c)

1.
2.
3.
4.

(c)

001992

Derived From Schneider MFR
Declassify August 27, 2022

(22)

SECRET

(c)

(c)

(c)

(c)

(u) Issues:

(c)

(c)

(c)

(c)

(c)

(c)

Comment [m1]: b5

b1

(c)

(c)

Comment [m2]: b5

(c)

Comment [m3]: b5

(c)

(c)

001264

(c)°

(c)

(c).

(c)

(c)

61

(c)

(c).

(c)

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

(5)

(c)•

(c)

61

(c)

(c)

(c)•

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

(c)

(c).

(c)

(c)

b1

(c)

cc: Paul Rosenzweig, Counselor

~~SECRET~~

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

Homeland Security

111.1

[62]

Deleted: May 2, 2007

INFORMATION

MEMORANDUM FOR: Stewart Baker

THROUGH: Marisa Lino, Senior Advisor, PLCY/OIA

FROM: Michael Scardaville, Deputy Director for European Affairs

(u) SUBJECT: Key Issues for the May 3, 2007 PNR VTC

(u) Overview:

(c)

b1

(c)

1.

2.

3.

4.

Deleted: .
Deleted:
Deleted:
Deleted:
Deleted:
Deleted:
Deleted: _
Deleted: the
Deleted: that
Deleted: ay
Deleted: that
Formatted: Indent: Left: 0.5", First line: 0", Tabs: 0.5", List tab + Not at 1.25"
Deleted: that
Formatted: No bullets or numbering
Formatted: Indent: Left: 0.5", Hanging: 0.5", Tabs: 1", List tab + Not at 1.25"
Formatted: No bullets or numbering
Formatted: Indent: Left: 0.5", Hanging: 0.5", Tabs: 1", List tab + Not at 1.25"
Formatted: Bullets and Numbering
Deleted: that
Deleted: ¶
Formatted: No bullets or numbering
Formatted: Indent: Left: 0.5", Hanging: 0.5", Tabs: 1", List tab + Not at 1.25"

65

001268

(23)

Derived from Schneider MFR
Declassify August 30, 2022

~~SECRET~~

(c)

(c)

(c)

(c)

(c)

(u) Issues:

(c)

(c)

(c)

Deleted: that

Deleted: ed

Deleted: that

Deleted: and

Deleted: of

Deleted: the

Deleted: s

Deleted: a

Deleted: '

Formatted: Font: Italic

Deleted: those

Deleted: would

Deleted: d

Comment [mr11]: This doesn't make sense.

b1

b1

DECLASS

(c)

(c)

(c)

(c)

(c)

(c)

b1

Deleted: ¶

Comment [m2]:
[b5]

Deleted: Since t

Deleted: us

Deleted: as

Deleted: As such, i

Deleted: re

Deleted: that

Deleted: are going to be

Deleted: ied

Deleted: would

Deleted: to

Deleted: on

Formatted: Not Highlight

Comment:
[b5]

Deleted: so long as it was

Deleted: who have

Comment [m4]:
[b5]

Deleted: w

Deleted: additional

(c)

(c)

(c)

(c)

(c)

(c)

(c)

(c)

(c)

Deleted: i

Deleted: w

Deleted: ed

Deleted: '

Formatted: Underline

Deleted: In addition

Formatted: Font: Bold

Deleted: that

Deleted: for

Deleted:

Deleted: for

Deleted: their

Deleted: notice

Deleted: . f

Deleted:

Deleted:

[65]

Comment [mrl5]: [b5]
Deleted: '

(S)

Comment [mrl6]: [b5]
Deleted: [b5]

(C)

(C)

b1

Deleted: their
Deleted: at

(C)

Deleted: to

Deleted: [b5]
Deleted: do
Deleted: has
Deleted: [b5]

(C)

Deleted: it
Deleted: [b5]
Deleted: on
Deleted: to
Deleted: e

¹ The Article 29 Working Party [b5] noted, "The Working Party considers that information should be provided to passengers no later than the moment when the passenger gives their agreement to buy the ticket. . . . Even if the transfer of PNR data has become in practice a condition for traveling to the US, passengers are only aware of what that means in terms of the processing of their personal data if the information is given to them before they buy the ticket." [b5]

Deleted:
Deleted: r
Deleted: "

(c)

(c)

(c)

(c)

(c)

(c)

b1

Deleted: i

Deleted:
Deleted
Deleted [65]

Deleted: of the

Deleted: pressed

Deleted: [65]

Deleted: issue

b1

Deleted [b5]

cc: Paul Rosenzweig, Counselor

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

Homeland Security

147.1

(b)(2)

Deleted: May 2, 2007

INFORMATION

MEMORANDUM FOR: Stewart Baker

THROUGH: Marisa Lino, Senior Advisor, PLCY/OIA

FROM: Michael Scardaville, Deputy Director for European Affairs

(u) SUBJECT: Key Issues for the May 3, 2007 PNR VTC

(u) Overview:

(c)

b1

(c)

001275

Derived from Schneider MFR
Declassify Aug. 27, 2022

(24)

(c)
(c)

(c)

(c)

b1

(u) Issues:
(c)
(c)

b1

(c)

(c)

(c) b1

(c).

(c)

(c) °

(c)°

(c)°

b1

(c)°

(c)°

(c)

(c)·

(c)

(c)

E 65

J

001273

(c)

(c)

(c)

61

(s)

(c)

[1] The Article 29 Working Party [c 65] noted, "The Working Party considers that information should be provided to passengers no later than the moment when the passenger gives their agreement to buy the ticket. . . . Even if the transfer of PNR data has become in practice a condition for traveling to the US, passengers are only aware of what that means in terms of the processing of their personal data if the information is given to them before they buy the ticket."

[c 65]

(c)

(c)

(c)

b1

(c).

(c)

(c).

(c)

(c)

b1

(c)

cc: Paul Rosenzweig, Counselor

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

Homeland Security

148.1

[62]

Deleted: May 2, 2007

INFORMATION

MEMORANDUM FOR: Stewart Baker

THROUGH: Marisa Lino, Senior Advisor, PLCY/OIA

FROM: Michael Scardaville, Deputy Director for European Affairs

(U) SUBJECT: Key Issues for the May 3, 2007 PNR VTC

(U) Overview:

(C)

(C)

b1

b5

Deleted:
Deleted:
Deleted:
Deleted:
Deleted:
Deleted:
Deleted:
Deleted:
Deleted:
Deleted:
Deleted:
Formatted: Indent: Left: 0", First line: 0", Tabs: 0.5", List tab
Deleted: that
Formatted: No bullets or numbering
Formatted: Indent: Left: 0.5", Hanging: 0.5", Tabs: 1", List tab
Formatted: No bullets or numbering
Deleted: [65]
Formatted: Indent: Left: 0.5", Hanging: 0.5", Tabs: 1", List tab
Formatted: Bullets and Numbering
Deleted: that
Deleted: the
Deleted: ¶
Deleted: ¶
Formatted: No bullets or numbering, Tabs: 1.25", List tab
Formatted: Indent: Left: 0.5", Hanging: 0.5", Tabs: 1", List tab

001282

(25)

Derived from Schneider MFR
Declassify Aug. 30, 2022

(c)

(c)

(c)

b1

(c)

(c)

(u) Issues:

(c)

(c)

b1

(c)

Deleted: that

Deleted: ed

Deleted: that

Deleted: and

Deleted: of

Deleted: non-

Comment [RR1]: c 65 ~7

Deleted: the

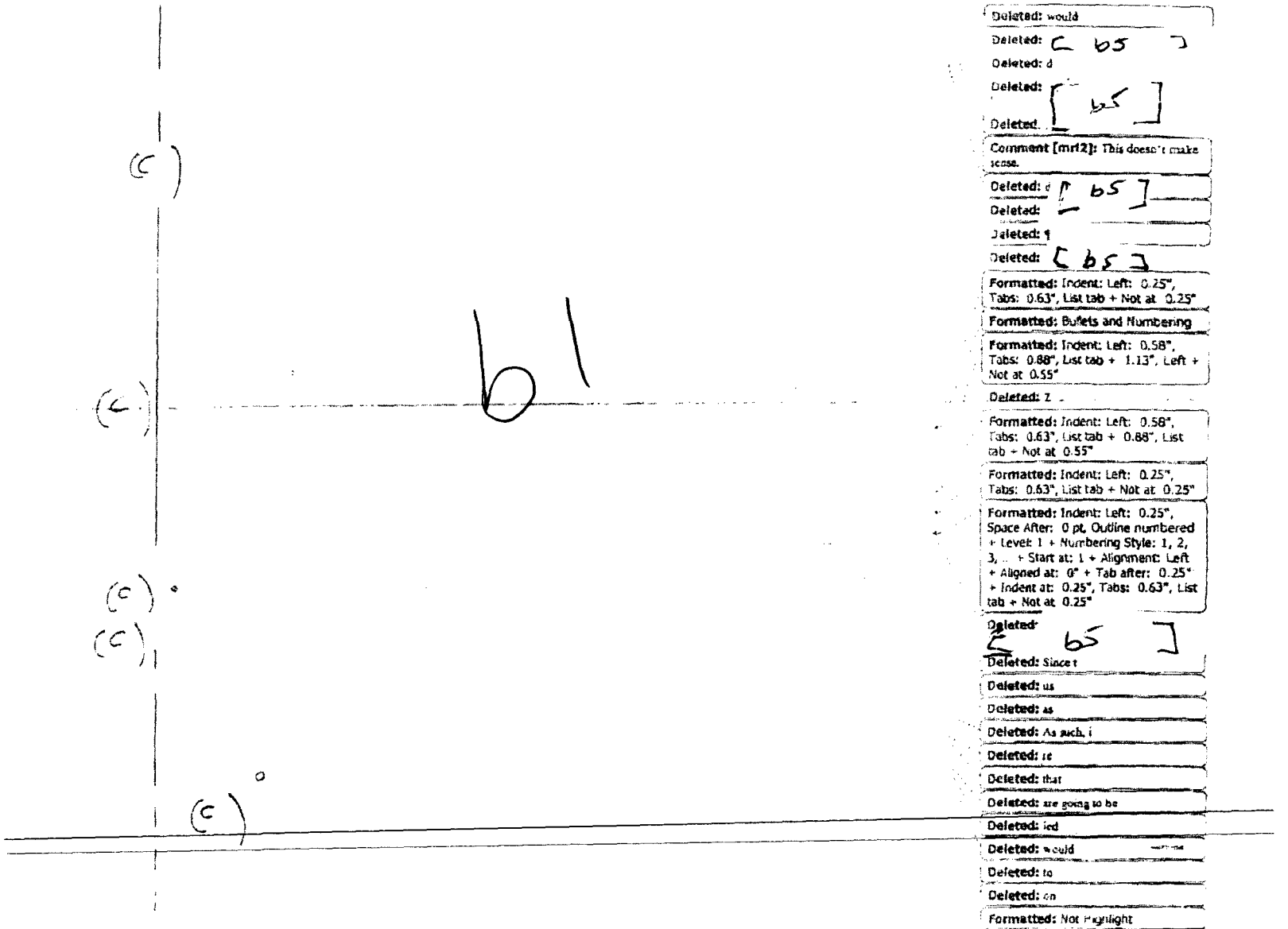
Deleted: s

Deleted: a

Deleted: '

Formatted: Font: Italic

Deleted: those



Deleted: would

Deleted: [b5]

Deleted: d

Deleted: [b5]

Deleted:

Comment [mrl2]: This doesn't make sense.

Deleted: d [b5]

Deleted:

Deleted: ¶

Deleted: [b5]

Formatted: Indent: Left: 0.25", Tabs: 0.63", List tab + Not at 0.25"

Formatted: Bullets and Numbering

Formatted: Indent: Left: 0.58", Tabs: 0.88", List tab + 1.13", Left + Not at 0.55"

Deleted: 2

Formatted: Indent: Left: 0.58", Tabs: 0.63", List tab + 0.88", List tab + Not at 0.55"

Formatted: Indent: Left: 0.25", Tabs: 0.63", List tab + Not at 0.25"

Formatted: Indent: Left: 0.25", Space After: 0 pt, Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0" + Tab after: 0.25" + Indent at: 0.25", Tabs: 0.63", List tab + Not at 0.25"

Deleted: [b5]

Deleted: Since t

Deleted: us

Deleted: as

Deleted: As such, i

Deleted: ie

Deleted: that

Deleted: are going to be

Deleted: ied

Deleted: would

Deleted: to

Deleted: on

Formatted: Not Highlight

Deleted: [b5]

Deleted: .

Formatted: Bullets and Numbering

Deleted

Deleted

Deleted:

Deleted:

Deleted:

Deleted:

Deleted: :

Deleted: w

Deleted: ed

Deleted: '

Formatted: Underline

Deleted [b5]

Formatted: Font: Bold

(c)

(c)

(c)

(c)

(c)

(c)

(c)

b1

b5

Deleted: that

(c)

(c)

b1

(c)

Deleted: for

Deleted:

Deleted: for

Deleted: their

Deleted: notice

Deleted: , f

Deleted:

Deleted: [b5]

Comment [mri3]:

Deleted:

Deleted: [b5

(5)

Comment [mri4]:

b5

Deleted:

Deleted: b5]

(c)

[2] The Article 29 Working Party [b5] noted, "[The Working Party considers that information should be provided to passengers no later than the moment when the passenger gives their agreement to buy the ticket. . . . Even if the transfer of PNR data has become in practice a condition for traveling to the US, passengers are only aware of what that means in terms of the processing of their personal data if the information is given to them before they buy the ticket."

[b5]

Deleted:

Deleted: r

Deleted: "

(c)

Deleted: their

Deleted: at

Deleted: to

(c)

Deleted: [b5]

Deleted: do

Deleted: has

b1

Deleted: [b5]

(c)

Deleted: (.

Deleted: ?)

Deleted: It

Deleted: [b5]

Deleted: on

Deleted: to

Deleted: e

(c)

(c)

Deleted: t

(c)

(c)

Deleted:

Deleted:

leted:

[b5]

Deleted: of the

Deleted: pressed

(c) b1

Deleted: b5 J

Deleted: c

Deleted: issue

(c)

Deleted: c b5 J

cc: Paul Rosenzweig, Counselor

Page 3: [1] Deleted	michael.scardaville	5/2/2007 4:57:00 PM

[b5]

Page 3: [2] Deleted	michael.scardaville	5/2/2007 4:58:00 PM

[b5]

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

Homeland Security

[b2]

INFORMATION

MEMORANDUM FOR: Stewart Baker

THROUGH: Marisa Lino, Senior Advisor, PLCY/OIA

FROM: Michael Scardaville, Deputy Director for European Affairs

SUBJECT: Key Issues for the May 3, 2007 PNR VTC

Overview:

(c)

b1

(c)

001299

(26)

Derived from Schneider MFR
Declassify September 7, 2022

(c)

(c)

(c)

b1

(c)

(c)

(c)

b1

(c)

(c)

(c).

(c)

(c) b1

(c).

(c).

(c).

Comment [m1]: [b5]

Comment [m2]: [b5]

Comment [m3]: [b5]

(c) .

(c)

(c) .

(c)

(c)

b1

(c)

(c) .

(c)

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

(c)

(c).

(c)

(c)

61

(c)

(c).

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

65

(c)

(c)

(c)

(c)

b1

(c)

(c)

cc: Paul Rosenzweig, Counselor

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

Homeland Security

[b2]

Deleted: May 2, 2007

INFORMATION

MEMORANDUM FOR: Stewart Baker

THROUGH: Marisa Lino, Senior Advisor, PLCY/OIA

FROM: Michael Scardaville, Deputy Director for European Affairs

SUBJECT: Key Issues for the May 3, 2007 PNR VTC (u)

(u) Overview:

(c)

(c)

b1

b5

Deleted:
Deleted:
Deleted:
Deleted:
Deleted:
Deleted:
Deleted:
Deleted:
Deleted:
Deleted:
Deleted:
Formatte
line: 0", Tabs: 0.5", List tab
Deleted: that
Formatted: No bullets or numbering
Formatted: Indent: Left: 0.5", Hanging: 0.5", Tabs: 1", List tab
Formatted: No bullets or numbering
Deleted: [b5]
Formatted: Indent: Left: 0.5", Hanging: 0.5", Tabs: 1", List tab
Formatted: Bullets and Numbering
Deleted: that
Deleted: the
Deleted: ¶
Deleted: ¶
Formatted: No bullets or numbering, Tabs: 1.25", List tab
Formatted: Indent: Left: 0.5", Hanging: 0.5", Tabs: 1", List tab

001397

Derived from Schneider MFR
Declassify September 7, 2022

27

(c)

(c)

(c)

(c)

b1

(c)

(u) [illegible]

(c)

(c)

b1

Deleted: that

Deleted: ed

Deleted: that

Deleted: and

Deleted: of

Deleted: the

Deleted: s

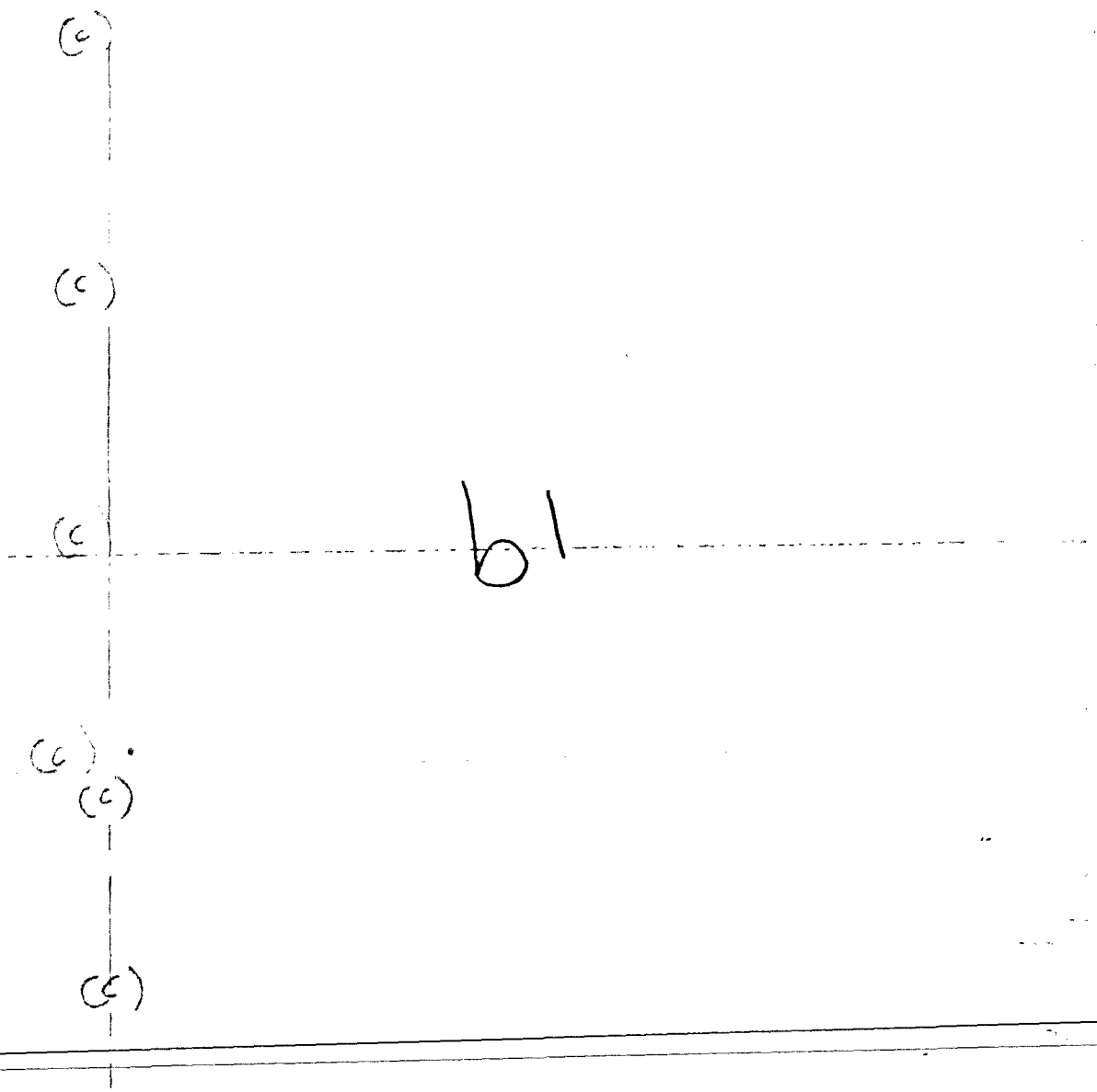
Deleted: a

Deleted:

Formatted: Font: Italic

E b5]

001383



Deleted: those

Deleted: would

Deleted: d

Comment [mrl1]: This doesn't make sense.

Deleted: [bs]

Deleted:

Deleted:

Deleted: ¶

Formatted: Indent: Left: 0.25", Tabs: 0.63", List tab + Not at 0.25"

Formatted: Bullets and Numbering

Formatted: Indent: Left: 0.58", Tabs: 0.88", List tab + 1.13", Left + Not at 0.55"

Formatted: Indent: Left: 0.58", Tabs: 0.63", List tab + 0.88", List tab + Not at 0.55"

Formatted: Indent: Left: 0.25", Tabs: 0.63", List tab + Not at 0.25"

Comment [m2]: [bs]

Formatted: Indent: Left: 0.25", Space After: 0 pt, Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0" + Tab after: 0.25" + Indent at: 0.25", Tabs: 0.63", List tab + Not at 0.25"

Deleted: [bs]

Deleted: Since t

Deleted: us

Deleted: as

Deleted: As such, i

Deleted: re

Deleted: that

Deleted: are going to be

Deleted: ied

Deleted: would

Deleted: to

Deleted: on

Formatted: Not Highlight

(c)

(c)

(c)

(c)

(c)

(c)

(c)

(c)

61

Deleted: [65]

Deleted:

Formatted: Bullets and Numbering

Deleted: [65]

Deleted:

Deleted: [65]

Deleted:

Deleted: [65]

Deleted:

Deleted:

Deleted:

Deleted:

Formatted: Underline

Deleted: [65]

Formatted: Font: Bold

Deleted:

(5)

(c)

(c)

b1

(5)

(c)

(c)

Deleted: for

Deleted:

Deleted: for

Deleted: their

Deleted: notice

Deleted: ,f

Deleted: deployment

Deleted:

Commer [b5]

Deleted:

Deleted: [b5]

Comment [mri4]:

[b5]

Deleted:

Deleted:

[The Article 29 Working Party [b5] noted, "The Working Party considers that information should be provided to passengers no later than the moment when the passenger gives their agreement to buy the ticket. Even if the transfer of PNR data has become in practice a condition for traveling to the US, passengers are only aware of what that means in terms of the processing of their personal data if the information is given to them before they buy the ticket."

b5]

Deleted:

Deleted: s

Deleted:

(c)

(c)

(c)

b1

(c)

(c)

(c)

(c)

Deleted: their

Deleted: at

Deleted: to

Deleted [b5]

Deleted: do

Deleted: has

Deleted [b5]

Deleted: (

Deleted: ?)

Deleted: It

Deleted: [b5]

Deleted: on

Deleted: to

Deleted: e

Deleted: t

Deleted:

Deleted:

Deleted: [b5]

Deleted: of the

Deleted: pressed

Deleted: b5

Deleted:

b1

Deleted: issue

Deleted: b5

cc: Paul Rosenzweig, Counselor

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

Background:

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

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

(C)

(C)

(C)

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

Derived: Schneider MPR
Reason: 7/2021

Law Enforcement Sensitive

(c)

(c)

(c)

b1

7/28
mrd

(c)

(c)

(c)

(c)

[2] EDPS Press Release, May 30, 2006

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

(c)

(c)

(c)

(c)

(c)

b1

(c)

C/FOI
MCA

(c)

(c)

(c)

C/FOI
MCA

(f)

001371

(c)

(c)

(c)

(c)

b1

(c)

Options for PNR Negotiations with the EU
[illegible]

Background: (U)

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

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

(C)

(C)

b1

(C)

European Parliament [illegible] Motion for a Resolution [illegible] transfer data [illegible] SWIFT system by the US secret services [illegible] 2006

001373

(c)

(c)

(c)

b1

(c)

(c)

(c)

(c)

(c)

b1

[1] EDPS Press Release, May 30, 2006

Formatted: Font color: Auto

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

(c)

(c)

(c)

(c)

(c)

(c)

(c)

(c)

(c)

(c)

(c)

(c)

(c)

(c)

b1

(c) b1

Formatted: Font color: Auto

Law Enforcement Sensitive

001375

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

(C)

(C)

(C)

b1

(C)

(C)

Law Enforcement Sensitive

Options for PNR Negotiations with the EU

7 28 06

Background: [b5] an international agreement was struck between DHS and the EU in 2004 governing CBP's access to PNR from the EU. The agreement was quickly challenged in court by the European Parliament. On 5.30.05 the European Court of Justice ruled that the EU inappropriately entered into this agreement on the grounds that the 1995 Directive did not apply [b5] On 7 3 06, the Finnish Presidency and the Commission terminated the agreement effective 9.30.06. The Finnish Presidency also received a mandate from the European Council to negotiate a replacement agreement by 9/30. The Commission presented the US G with a proposed text on 7 16

Deleted: [b5]
Deleted:

Deleted: [b5]
Deleted:

(U)

(C)

b1

(C)

b1

Deleted:
Deleted: [b5]
Deleted:

(C)

Deleted [b5]

Deleted: us

Deleted:

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

Law Enforcement Sensitive

Derived: Schneider MFR
Declass: 7/2031

001377

23

30

CONFIDENTIAL

Deleted: M

Deleted:

[2] EDPS Press Release, May 30, 2006

001378

Options for PNR Negotiations with the EU

7 28 06

(C) b1

Deleted:

Deleted:

Deleted:

(C) b1

Deleted:

Deleted:

Deleted:

Deleted:

Deleted:

Deleted:

Deleted:

Deleted:

Deleted:

Deleted:

Deleted:

Deleted:

(C) b1

Deleted:

Deleted:

b1

Deleted:

Deleted:

Deleted:

Deleted:

(C) b1

Deleted:

Deleted:

Deleted:

Law Enforcement Sensitive

001379

Options for PNR Negotiations with the EU

7 28 06

Deleted:

(c)

Deleted:

Deleted:

Deleted: (b5)

Deleted:

Deleted:

Deleted:

(c)

(c)

Deleted: W

Deleted: W

(c)

b1

Law Enforcement Sensitive

001380

Options for PNR Negotiations with the EU

7/28/06

Background:

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

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

•

•

001381

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

(C)

C/POS
mod

(C)

b1

(C)

€

(C)

(C

(C

(c)

(c)

(c)

b1

c/pgt
mod

(c)

(c)

c

c/pgt - no

(c)

(c)

(c)

(c)

(c)

b1

001384

Options for PNR Negotiations with the EU
28 06

Background:

An international agreement was struck between DHS and the EU in 2004 governing CBP's access to PNR in the EU. The agreement was quickly challenged in court by the European Parliament. On 5/30/06 the European Court of Justice ruled that the EU inappropriately entered into this agreement on the grounds that the 1995 Directive did not apply.

On 7/3/06, the Finnish Presidency and the Commission terminated the agreement effective 7/30/06. The Finnish Presidency also received a mandate from the European Council to negotiate a replacement

Deleted: s

Deleted: for

Deleted: new

Deleted: decisions

Deleted: including

(C)

(C)

/Post Mtg

(C)

(C)

(C)

(C)

(C)

b1

Deleted:

Deleted:

Deleted:

Deleted:

Deleted: at least

Deleted: (b5)

Deleted: that any

Deleted: is

Formatted: Font: Bold

Formatted: Indent: Left: 0.75"

Formatted: Font: Bold

Formatted: Indent: Left: 0.75"

Deleted: and a

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

(C)

(C)

(C)

(C)

(C)

(C)

(C)

(C)

(C)

(C)

(C)

(C)

b1

Formatted: Font: Bold

Formatted: Indent: Left: 0.75"

Deleted: , each of which is discussed below

Deleted: ing

001387

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

(c)
(c)

b1

Deleted: . h

Law Enforcement Sensitive

CONFIDENTIAL

Attachment B

Substantive DHS Comments on NSC Draft Discussion Paper

Page 2 [redacted]

(b)(5)

(c)

(c)

b1

(c)

(c)

(c)

(c)

b1

FOR OFFICIAL USE ONLY

Received: Schmidt MFR

Declassified 12/2022

CONFIDENTIAL

(c)

b1

(c)

Page 4 - 2

(v) [

b5

]

(c)

b1

CONFIDENTIAL

Historical Background (U)

(C-PGI/mod)

b1

The Working Party underlines the necessity to have commitments from the US side that are officially published at least at the level of the Federal Register and fully binding on the US side. *In particular, there should be no ambiguity about the capability to create rights in favour of third parties.* [b5]

(U)

(C-PGI/mod)

b1

(U) [b5] the Canadian government incorporated their "Commitments", the functional equivalent of CBP's Undertakings, into domestic regulations [b5] [b5] See ttp://canadagazette.gc.ca/partII/2005/2005/...4.html/sor346-e.html and a copy of the Commitments contained in Annex A hereof.[b5]

Comment: [b6] I sent you copies of [illegible] accordingly.

001456

CONFIDENTIAL

Derived: Schneider MFC
Declass: 31 Dec 2021

(W) [65]

Legal Impact of Making Undertakings "Binding" (c)

(c)

(c)

FOR OFFICIAL USE ONLY

DEPUTIES MEETING ON PNR

DATE: Tuesday, July 25, 2006
TIME: 2:30 – 3:30
LOCATION: TBD
FROM: Stewart Baker, Assistant Secretary for Policy

OBJECTIVES DESIRED OUTCOME OF MEETING:

- Establish an interagency negotiating position

[b5 b2(H) b7E]

BACKGROUND:

- On May 30, 2006 the European Court of Justice (ECJ) ruled that the legal instrument the European Union utilized as a basis for entering into a 2004 agreement with DHS on CBP's access to PNR was inapplicable and required the EU to terminate the agreement by September 30, 2006. The EU has since provided notice that it is terminating the agreement effective that date.
- [

b1

PARTICIPANTS:
Non-DHS

DHS
Deputy Secretary Jackson

PRESS PLAN: "Closed"

ATTACHMENTS:

A. Discussion Document: Analysis of United States Interests in the U.S.-EU PNR dialogue (7/13/06)
B. Memo: Summary of Potential Changes to the Undertakings (*PENDING*)
C. Member State Positions known as of 7/20/06
D. Background on EU views of consent as a solution
E. DHS' Response Options to European Court of Justice Decision (February 2006)

Prepared by: Michael Scardaville, PDEV, E b2(low) J

001489

FOR OFFICIAL USE ONLY

(34)

30

Formatted: Font: 12 pt, Font color: Black

Formatted: Centered, Indent: Left: 0"

Formatted: Font: 12 pt, Not Italic, Font color: Black

Deleted: U.S. Department of Homeland Security ¶
Washington, DC 20528¶
<sp>

Formatted: Top: 1", Bottom: 1"

Deleted: ¶

(U) [b5]

Formatted: Centered

Formatted: Font: Not Italic

Deleted: ¶

Purpose

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

Summary

(U) Before September 11, the government knew very little about the people getting on planes bound for the United States. After the attacks, airlines were required to provide information about their U.S.-bound passengers. Some of this information – name, contact information, and the like – was drawn from information supplied to the airline as part of the reservation process. DHS uses the information to screen for no-fly violators and terrorist suspects prior to arrival, and even before the plane takes 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 by the lack of a broad adequacy finding. While the EU lacks similar requirements for the transfer of law enforcement information between the EU and third parties, a Framework Decision is currently being considered that would mirror the requirements applied in the commercial realm.

b5

b1

(U) [1] 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.

Formatted: Centered

Derived: Schneider MFR
Subject: EU PNR
Declass: 20 July 2031

Formatted: Centered

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

Because the agreement was entered under the wrong authority, the Court ruled it invalid but delayed the effective date of its decision until September 30 in the hope that the jurisdictional problem could be quickly solved. To cure the problem, the EU has obtained authority from the Member States to renegotiate the PNR Agreement under the Third Pillar. As required by the Agreement, the EU also notified the United States that it will terminate the current Agreement on September 30, 2006 and has set a goal of establishing a new agreement by this date. [illegible] proposed replacement text from [illegible], although Commission officials have [illegible] final. Commission representatives have portrayed their proposal as a technical change that would put the same agreement back in place, albeit under a different legal authority.

[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.

[illegible]

001677

Formatted: Centered

(S)

b1

(S)

Background

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

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

(C)

b1

Formatted: Centered

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

(c)

(c)

(c)

b1

(c)

(c)

Formatted: Centered

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.

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

[8] 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."

[9] 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

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 to establish restrictive, EU-wide rules for information sharing in the area of law enforcement. Last October the EU put forward two draft documents that concern data sharing and protection in the law enforcement context. They consist of a draft Framework Directive of the European Parliament and Council on the retention of data and a proposed Council decision on the protection of personal data in criminal matters.

b5

b1

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.

b1

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.

Formatted: Centered

b1

b1

Communicable Diseases. One indicator of the extent to which EU data protection authorities prioritize the expansion of such roles over public safety concerns can be found in the European reaction to another US initiative relating to avian flu. If air passengers are exposed to a pandemic strain of avian flu, the government will need to locate all of the passengers and crew, quickly. So the

b1

[3] 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

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

Analysis & Recommendation

(C)

(S)

b1

(C)

(S)

[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.

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

Formatted: Centered

Formatted: Font: Bold, Underline

(C)

(S)

b1

Deleted: (b5 1

Deleted: ure

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.

(S)

b1

Formatted: Centered

61

DIRECTIVE [illegible] OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of [illegible]

[illegible]

Scope

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

[illegible] This Directive shall not apply to the processing of personal data:

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

Article 26

Derogations

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

(a) the data subject has given his consent [illegible] to the proposed transfer; or

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

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

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

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

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

2. Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of [illegible]

Formatted: Centered

Formatted: Font: Bold

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Indent: Left: 0"

[illegible]

[illegible]

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

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

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

CHAPTER [illegible] TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

Article 25

[illegible]

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

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

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

4. Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of [illegible]

[illegible]

[illegible] the Commission shall enter into negotiations [illegible]

[illegible]

[illegible] The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered

001637

UNCLASS

X

Formatted: Centered

Formatted: Indent: Left: 0"

COUNCIL FRAMEWORK DECISION on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters

Formatted: Font: (Default) Times New Roman

Formatted: Indent: Left: 0", Right: 0", Space Before: 0 pt, After: 0 pt, Hyphenate, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Font: (Default) Times New Roman, 12 pt, English (U.S.)

Formatted: Font: (Default) Times New Roman

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Indent: Left: 0.13"

Formatted: Font: (Default) Times New Roman

Formatted: Font: (Default) Times New Roman

891693

UNCLASS

Formatted: Centered

Formatted: Font: (Default) Times New Roman

Formatted: Font: (Default) Times New Roman

3. Personal data processed by the competent authority of another Member State may be further transferred to competent authorities of third countries or international bodies in order to safeguard the essential interests of a Member State or for the prevention of imminent serious danger threatening public security or a specific person or persons.

Washington, DC 20528

Homeland Security

b5

DISCUSSION DOCUMENT

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

Department of Homeland Security

July 20, 2006

Purpose

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

Summary

Before September 11, the government knew very little about the people getting on planes bound for the United States. After the attacks, airlines were required to provide information about their U.S.-bound passengers. Some of this information – name, contact information, and the like -- was drawn from information supplied to the airline as part of the reservation process. DHS uses the information to screen for no-fly violators and terrorist suspects prior to arrival, and even before the plane takes off[1], 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

[1] 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.

Derived: Schneider MFR
Subject: EU/PNR
Declass: 20 July 2021

European standards, and commercial data transfers to the U.S. have long been restricted by the lack of a broad adequacy finding. While the EU lacks similar requirements for the transfer of law enforcement information between the EU and third parties, a Framework Decision is currently being considered that would mirror the requirements applied in the commercial realm.

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

Because the agreement was entered under the wrong authority, the Court ruled it invalid but delayed the effective date of its decision until September 30 in the hope that the jurisdictional problem could be quickly solved. To cure the problem, the EU has obtained authority from the Member States to renegotiate the PNR Agreement under the Third Pillar. As required by the Agreement, the EU also notified the United States that it will terminate the current Agreement on September 30, 2006 and

[7] 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.

has set a goal of establishing a new agreement by this date. [b5] The USG received a proposed replacement text from [b5] the Finnish Presidency on July 19th, although Commission officials have indicated that this draft may not be final.[3] Commission representatives have portrayed their proposal as a technical change that would put the same agreement back in place, albeit under a different legal authority.

(C)

(5)

b1

(5)

Background

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

(U) **The EU-US PNR Agreement.** As noted, in May 2004, after substantial negotiations, the Department of Homeland Security entered into an agreement relating to the sharing of PNR information collected by air carriers flying to the United States from Europe. The Agreement was

(U) [3] Both the Departments of State and Homeland Security have a number of questions regarding the legal impact of a variety of wording choices, including references to the European Convention on Human Rights. Additional policy analysis is underway and will be further driven by the decisions of the Ministries.

001282

intended to resolve a perceived conflict between EU law (which limits the sharing of personal information collected by commercial entities with governmental entities) and US law (which required the collection and dissemination of PNR data). Central to the Agreement was a set of Undertakings made by Customs and Border Protection (CBP) regarding how it would treat the PNR data transmitted to it.[4] Several of the limitations in those Undertakings significantly restrict US opportunities to use information for investigative and law enforcement purposes.

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

(b)

(b)

(b)

(b)

(b)

(b)

(c)

(c)

b1

(s)

(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."

(c)(4)-Not

b1

001894

(3) **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.

(3) On May 30, 2006, the ECJ issued its opinion in the lawsuits. The opinion did not address the merits of the EU-US PNR Agreement or the role of the Parliament. Rather, the decision turned on the lack of competence of the Commission and Council to enter into the Agreement in the first instance. The EU had based its authority on the so-called "First Pillar," which allows the EU to regulate trade and commercial matters. The ECJ held (as the US had argued earlier) that the requirement that PNR data be sent to the US was a law enforcement and national security matter. Such transfers, the court held, were excluded from the data protection directive governing commercial data exports. If they are to be regulated, the court implied, it would have to be done under the "Third Pillar."[3]

(4) 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.

(5)

b1

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

55

(4) [3] Acting under the First Pillar, the EU has also entered into a PNR sharing agreement with Canada. In light of the EU's determination that the US Undertakings provided "adequate" privacy protections, the EU-Canada agreement authorizes Canada to share PNR data received from the EU with the US. Even though the ECJ has struck down the EU-US agreement, the EU contends that its similar agreement with Canada remains in effect. Some Canadian government sources are concerned, however, that the absence of an "adequacy" finding (which is a First Pillar concept) may now have the effect of *prohibiting* US-Canada information sharing derived from EU-originated flights.

b1

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

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

Communicable Diseases. One indicator of the extent to which EU data protection authorities prioritize the expansion of such roles over public safety concerns can be found in the European reaction to another US initiative relating to avian flu. If air passengers are exposed to a pandemic strain of avian flu, the government will need to locate all of the passengers and crew, quickly. So the Centers for Disease Control has proposed a rule requiring airlines to retain PNR for up to 60 days for that purpose. The top data protection authorities of Europe, known as the "Article 29 Working Party," have now decided that this sort of data retention violates EU privacy directives. If given effect, the Working Party's opinion would place air carriers legal jeopardy because of inconsistent legal régimes. It reflects a widespread EU view that privacy trumps even the critical public health interests of the United States. [13]

Analysis & Recommendation

b1

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

[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.

(C)

(S)

b1

Conclusion

(C)

(S)

b1

Conclusion

(4) 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.

(5) 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.

(5)

b1

(C)

1693

Attachment: Excerpts from the EU data protection Directive and proposed Framework Decision.

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

Article 3

Scope

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

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

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

Article 26

Derogations

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

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

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

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

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

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

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

2. Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of

individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.

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

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

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

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

CHAPTER IV TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

Article 25

Principles

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

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

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

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

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

6. The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered

into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.

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

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

Article 15

Transfer to competent authorities in third countries or to international bodies

1. Member States shall provide that personal data received from or made available by the competent authority of another Member State are not further transferred to competent authorities of third countries or to international bodies except if such transfer is in compliance with this Framework Decision and, in particular, all the following requirements are met.
(a) The transfer is provided for by law clearly obliging or authorising it.
(b) The transfer is necessary for the purpose the data concerned were transmitted or made available for or for the purpose of the prevention, investigation, detection or prosecution of criminal offences or for the purpose of the prevention of threats to public security or to a person, except where such considerations are overridden by the need to protect the interests or fundamental rights of the data subject.
(c) The competent authority of another Member State that has transmitted or made available the data concerned to the competent authority that intends to further transfer them has given its prior consent to their further transfer.
(d) An adequate level of data protection is ensured in the third country or by the international body to which the data concerned shall be transferred.

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

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

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

001702

UNCLASS

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

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

Attachment B

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

July 13, 2006

Purpose

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

Summary

(U) Before September 11, the government knew very little about the people getting on planes bound for the United States. After the attacks, airlines were required to provide information about their U.S.-bound passengers. Some of this information – name, contact information, and the like – was drawn from information supplied to the airline as part of the reservation process. DHS uses the information to screen for no-fly violators and terrorist suspects prior to arrival, and even before the plane takes 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 by the lack of a broad adequacy finding. While the EU lacks similar requirements for the transfer of law enforcement information between the EU and third parties, a Framework Decision is currently being considered that would mirror the requirements applied in the commercial realm.

b5

(C/FGI-MOD) b1

001704

(U) [1] CBP may automatically access PNR data from European carriers up to 72 hours in advance of a flight. During this pre-departure period, information is screened against CBP automated systems and risk scores begin to be generated. In some cases, particularly airports where CBP maintains a presence through the Immigration Advisory Program, coordinated law enforcement action is also planned in advance with local authorities. Analysis continues up to arrival and is further supported by the collection of manifest information.

Derived: Schneider Mfe
Subject: EU/PNR 266.2
Declass: 13 July 2031

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

Because the agreement was entered under the wrong authority, the Court ruled it invalid but delayed the effective date of its decision until September 30 in the hope that the jurisdictional problem could be quickly solved. To cure the problem, the EU has obtained authority from the Member States to renegotiate the PNR Agreement under the Third Pillar. As required by the Agreement, the EU also notified the United States that it will terminate the current Agreement on September 30, 2006 and has set a goal of establishing a new agreement by this date. The USG received a proposed replacement text from the Finnish Presidency on July 19th, although Commission officials have indicated that this draft may not be final.[3] Commission representatives have portrayed their proposal as a technical change that would put the same agreement back in place, albeit under a different legal authority.

61

[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.

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

(S) b1

(S)

Background

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

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

(C) b1

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

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

1.

(c)

b1

(c)

(c)

(c)

b1

(C)

b1

(C)

(S)

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

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

(U//FOUO)

b1

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

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 to establish restrictive, EU-wide rules for information sharing in the area of law enforcement. Last October the EU put forward two draft documents that concern data sharing and protection in the law enforcement context. They consist of a draft Framework Directive of the European Parliament and Council on the retention of data and a proposed Council decision on the protection of personal data in criminal matters.

b5

b1

[8] Acting under the First Pillar, the EU has also entered into a PNR sharing agreement with Canada. In light of the EU's determination that the US Undertakings provided "adequate" privacy protections, the EU-Canada agreement authorizes Canada to share PNR data received from the EU with the 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.

(5)

b1

c/fgi-mod

c/fgi-mod

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

c/fgi-mod

b1

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

(4) **Communicable Diseases.** One indicator of the extent to which EU data protection authorities prioritize the expansion of such roles over public safety concerns can be found in the European reaction to another US initiative relating to avian flu. If air passengers are exposed to a pandemic strain of avian flu, the government will need to locate all of the passengers and crew, quickly. So the Centers for Disease Control has proposed a rule requiring airlines to retain PNR for up to 60 days for that purpose. The top data protection authorities of Europe, known as the "Article 29 Working Party," have now decided that this sort of data retention violates EU privacy directives. If given effect, the Working Party's opinion would place air carriers legal jeopardy because of inconsistent legal régimes. It reflects a widespread EU view that privacy trumps even the critical public health interests of the United States. [13]

Analysis & Recommendation

(C)

(5) b1

(C)

(4) [2] If adopted without the offered exemptions, the Draft Decision could conflict with a number of binding and non-binding information sharing arrangements that the United States has signed. For example, we have signed a 2003 Mutual Legal Assistance Agreement (MLAT) with the European Union and a 2001 information sharing agreement with Europol (the EU-level police agency); with respect to member states, we signed a 2003 MLAT with Germany, which builds on numerous other MLATs already in force with other EU member states. The United States also has many executive agreements and memoranda of understanding with member states under which critical information is currently being shared. Under EU law, directives supersede bilateral treaties and agreements and member states must conform their existing agreements to the directive.

(4) [3] Conversely, Paragraph 34 of the Undertakings allows for the exchange of PNR for public health purposes and neither the Commission nor the Article 29 Committee have challenged the DHS-HHS MOU.

(4) [4] Unlike in 2003, this risk is present now because the Court has conclusively ruled that the transfer of PNR data is a law enforcement matter. While European integration has been the greatest in areas associated with the Common Market, law enforcement and public security is a relatively new area of activity at the community level and many responsibilities still fall to the EU Member States. The ECJ firmly placed PNR in the area of law enforcement and public security, and as result, any actions taken in this area are likely to set precedents for further community involvement in other law enforcement matters.

(S) b1

Conclusion

(C)

(S) b1

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

(3) 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.

(4) 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.

(5)

b1

(C)

Attachments

A. Excerpt from EU Data Protection Directive 95/46/EC (24 October 1995) (٩)

B. Excerpt from Draft Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matter (October 2005) (٤)

001743

Attachments:

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

Article 3

Scope

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

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

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

Article 26

Derogations

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

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

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

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

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

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

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

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

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

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

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

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

CHAPTER IV TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

Article 25

Principles

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

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

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

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

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

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

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

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

Article 15

Transfer to competent authorities in third countries or to international bodies

1. Member States shall provide that personal data received from or made available by the competent authority of another Member State are not further transferred to competent authorities of third countries or to international bodies except if such transfer is in compliance with this Framework Decision and, in particular, all the following requirements are met:
(a) The transfer is provided for by law clearly obliging or authorising it.
(b) The transfer is necessary for the purpose the data concerned were transmitted or made available for or for the purpose of the prevention, investigation, detection or prosecution of criminal offences or for the purpose of the prevention of threats to public security or to a person, except where such considerations are overridden by the need to protect the interests or fundamental rights of the data subject.
(c) The competent authority of another Member State that has transmitted or made available the data concerned to the competent authority that intends to further transfer them has given its prior consent to their further transfer.
(d) An adequate level of data protection is ensured in the third country or by the international body to which the data concerned shall be transferred.

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

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

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

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

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

Attachment C

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

July 13, 2006

Purpose

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

Summary

(U) Before September 11, the government knew very little about the people getting on planes bound for the United States. After the attacks, airlines were required to provide information about their U.S.-bound passengers. Some of this information – name, contact information, and the like – was drawn from information supplied to the airline as part of the reservation process. DHS uses the information to screen for no-fly violators and terrorist suspects prior to arrival, and even before the plane takes 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 by the lack of a broad adequacy finding. While the EU lacks similar requirements for the transfer of law enforcement information between the EU and third parties, a Framework Decision is currently being considered that would mirror the requirements applied in the commercial realm.

b1

[1] (U) CBP may automatically access PNR data from European carriers up to 72 hours in advance of a flight. During this pre-departure period, information is screened against CBP automated systems and risk scores begin to be generated. In some cases, particularly airports where CBP maintains a presence through the Immigration Advisory Program, coordinated law enforcement action is also planned in advance with local authorities. Analysis continues up to arrival and is further supported by the collection of manifest information.

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

Because the agreement was entered under the wrong authority, the Court ruled it invalid but delayed the effective date of its decision until September 30 in the hope that the jurisdictional problem could be quickly solved. To cure the problem, the EU has obtained authority from the Member States to renegotiate the PNR Agreement under the Third Pillar. As required by the Agreement, the EU also notified the United States that it will terminate the current Agreement on September 30, 2006 and has set a goal of establishing a new agreement by this date. The USG received a proposed replacement text from the Finnish Presidency on July 19th, although Commission officials have indicated that this draft may not be final.[3] Commission representatives have portrayed their proposal as a technical change that would put the same agreement back in place, albeit under a different legal authority.

61

[3] CBP can share PNR data with other law enforcement agencies, but only on a case-by-case basis and only for the purpose of combating terrorism and serious transnational crimes. This restriction prevents PNR information from being shared in bulk with the intelligence and law enforcement community, and it denies those agencies direct access to the records. Broader access would allow other agencies to look for patterns in the travel of individuals not deemed to be high risk and to assess connections between passengers. ICE, for example, has expressed its frustration over losing access to this information.

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

(S)

b1

(S)

S

Background

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

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

(C) [4] b1

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

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

1.

(C)

(C)

b1

(C)

(C)

b1

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.

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

b1

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

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 to establish restrictive, EU-wide rules for information sharing in the area of law enforcement. Last October the EU put forward two draft documents that concern data sharing and protection in the law enforcement context. They consist of a draft Framework Directive of the European Parliament and Council on the retention of data and a proposed Council decision on the protection of personal data in criminal matters. C. b5

b1

001723

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

(S)

b1

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

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. One indicator of the extent to which EU data protection authorities prioritize the expansion of such roles over public safety concerns can be found in the European reaction to another US initiative relating to avian flu. If air passengers are exposed to a pandemic strain of avian flu, the government will need to locate all of the passengers and crew, quickly. So the Centers for Disease Control has proposed a rule requiring airlines to retain PNR for up to 60 days for that purpose. The top data protection authorities of Europe, known as the "Article 29 Working Party," have now decided that this sort of data retention violates EU privacy directives. If given effect, the Working Party's opinion would place air carriers legal jeopardy because of inconsistent legal régimes. It reflects a widespread EU view that privacy trumps even the critical public health interests of the United States. [13]

Analysis & Recommendation

b1

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

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

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

(S) b1

Conclusion

(C)

b1

(S)

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

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

Attachments

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

B. Excerpt from Draft Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matter (October 2005)

Attachments:

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

Article 3

Scope

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

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

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

Article 26

Derogations

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

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

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

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

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

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

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

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

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

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

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

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

CHAPTER IV TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

Article 25

Principles

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

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

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

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

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

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

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

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

Article 15

Transfer to competent authorities in third countries or to international bodies

1. Member States shall provide that personal data received from or made available by the competent authority of another Member State are not further transferred to competent authorities of third countries or to international bodies except if such transfer is in compliance with this Framework Decision and, in particular, all the following requirements are met.
(a) The transfer is provided for by law clearly obliging or authorising it.
(b) The transfer is necessary for the purpose the data concerned were transmitted or made available for or for the purpose of the prevention, investigation, detection or prosecution of criminal offences or for the purpose of the prevention of threats to public security or to a person, except where such considerations are overridden by the need to protect the interests or fundamental rights of the data subject.
(c) The competent authority of another Member State that has transmitted or made available the data concerned to the competent authority that intends to further transfer them has given its prior consent to their further transfer.
(d) An adequate level of data protection is ensured in the third country or by the international body to which the data concerned shall be transferred.

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

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

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

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

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