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



101.1

L 62

## 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: (a)

(c)

(0)

1. 2.

3.

4.

 $\mathcal{P}$ 

001982

 $(\mathfrak{F}_{\mathfrak{F}})$ 

Derived From Schneider MFR
Declassify August 27, 2022

ALT

(c)

(c)

(c)

(c)
(u) Issues:
(c)
(C)

(c)

(c) Comment [mi]: b5) (c)<sup>\*</sup> Comment (m2): 65 (,) Comment [m3]: 65  $(c)^{\circ}$ 

(c)°

(c)°

(0)

ره).

(c)

(-)

( )

(c)

(c)

The Article 29 Working Party C 65 I word, "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)

( < ) '

(0

(0)

<< )

(c):

. liven 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)

cc: Paul Rosenzweig, Counselor







662 Deleted: May 2, 2007 INFORMATION Stewart Baker Marisa Lino, Senior Advisor, PLCY/OIA Michael Scardaville, Deputy Director for European Affairs Key Issues for the May 3, 2007 PNR VTC Deleted: Deleted: Deleted: Daleted: 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"

(23)

MEMORANDUM FOR:

THROUGH:

FROM:

SUBJECT:

Overview:

1. 2.

4.

(c)

(c)

Derived from Schneider MFR Declassify August 30, 2022 001258

Formatted: Bullets and Numbering

Formattad: Indent: Left: 0.5", Hanging: 0.5", Tabs: 1", List tab + Not at 1.25"

Formatted: No bullets or

Deleted: that

Deleted: 1

numbering

(c)	-	
(c)		Defeted: that
Cali		
		Deleted: ad
X 1		
(c)!	,	Oeleted: that
	/	Celeted: and
		Seleted: of
We will be the second of the s		Onleted: the
		Daleted: s
·		Deleted: a
1		Defeted:
(c)		Formatted: Font: Italic
(u) Issues:		
(c)·.		
(4)		
(c)		
	<b>\</b>	
1	. \	
	$\sim$ 1	
	<b>V</b> (	
<del>{ C }</del>		
(0)		Deleted: those
		Deleted: those Deleted: would

(c)		Deleted: ¶
(c).		Comment (m2 65)
(CC)		Deleted: Since 1  Deleted: us  Deleted: as  Deleted: As mich, i  Deleted: re  Deleted: that  Deleted: are going to be  Deleted: ied
(c)		Deleted: to Deleted: on Formatted: Not Highlight Comment  Deleted: so long as it was Deleted: who have
1 (c ) °	,	Deleted: w Deleted: additional

entaro

(c)°	Deleted: i  Deleted: w  Deleted: cd
(c) · (c)	Deleted: ' Formatted: Underline  Deleted: In addition Formatted: Font: Bold  Deleted: that
(c)	Oqualitati inge
(c)·	Deleted: for Deleted: Deleted: for Deleted: their Deleted: notice Deleted: f

60:271

	÷	Comment (mri5) Opleted:
(5)		Comment [mris 65]
(c) ·		
(c)	6	Deleted: their
		Deleted: ar
(c)		Oalated: to
The state of the s		Deleted: £65 3 Deleted: do  Daleted: has
(c)		Deleted: C 65 3
		Deleted: It  Deleted: C 65 ]  Deleted: on
_		Defeted: 10
should be provided to p  Even if the transfer of	ng Party C S noted, "The Working Party considers assengers no later than the moment when the passenger gives their agreeme PNR data has become in practice a condition to traveling to the US, passen	nt to buy the ticket
of what that means in to	arms of the processing of their personal data if the information is given to the	Defeted: "

.

(c) ·		Doloted: 1
(c)·	bl	Defetad:
		Deleted: of the  Deleted: pressed
(c)		Deletad: • 65 ]
(c)		Deleted: (sec

Deleted C b5 7

cc: Paul Rosenzweig, Counselor

001.274

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



Homeland Security

しんてコ

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

(a) Overview:

(c)

b 1

(c)

001275

 $\left(\mathcal{Y}\right)$ 

Derived from Schneider MFR Neclassify Aug. 27, 2022

(c) (e)

(c)

(c)

(u) <u>Issues:</u> (c) •

(c)

(c)

(c)

--(<u>-</u>c)

(c).

(c)

(c) °

(c) (c)(r)° (c) (c). (c) - 5 65

(C)

(c)

---(c-)-

(5)

(c)

The Article 29 Working Party 65 anoted, 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)

(c)

- (c)

(c)·
(c).

(c)·

 $(\epsilon)$ 

(c)

61

cc: Paul Rosenzweig, Counselor

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



148.1

T62 ]

् Celeted: May 2, 2007

NEORMATION

MEMORANDUM FOR:

Stewart Baker

THROUGH:

Marisa Lino, Senior Advisor, PLCY/OIA

FROM:

Michael Scardaville, Deputy Director for European Affairs

(u) si

SUBJECT:

Key Issues for the May 3, 2007 PNR VTC

- 1

Ň.

Overview:

(c)

(

T....

\ \ \

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

Deleted:

Deleted:

Formatted: Indent: Len: v...
Ine: 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 builets or numbering

Deleted: [ 65

Formatted: Indent: Left: 0.5", Hanging: 0.5", Tabs: 1", List tab

Formatted: Builets and Numbering

Deleted: that

Deleted: the

Deleted: 1

Formatted: No builets or numbering, Tabs: 1.25", List tab

Formatted: Indent: Left: 0.5", Hanging: 0.5", Tabs: 1", List tab

001282

(35)

Derived from Schneider MFK Declassify Aug. 30, 2022

(e)		
		Celetad: that
(c)		Deleted: cd
(6)1	b	
	- (	Defated: that
1		Deleted: and
		Deletad: of
(c) (c) (u) <u>Issues:</u>		Deleted: non- Comment [RR1] C Deleted: thc
		Oeleted:
(c)		Deleted: a
(u \ <u>Issues:</u>		Deleted: ' Formatted: Font: (talic
(c) (c)		Constitution Constitution
l	<u> </u>	
(A)	01	
(0)		Oeleted: those

1	(no	ilated: would
	-	
		eleted: 6 5 1
		eleted:
(C)	Co	imment [mri2]: This doesn't make
	De	leted: o p b5 7
	Oe.	eletad:
	Ja	leted: 1
	Oe	eleted: [ bs ]
	Fo	rmatted: Indent: Left: 0.25", bs: 0.63", List tab + Not at 0.25"
\ \	Fo	rmatted: Bullets and Numbering
	Tal	rmatted: Indent: Left: 0,58", bs: 0.88", List tab + 1.13", Left + t at 0.55"
	De	leted: Z
	Tal	rmatted: Indent: Left: 0.58*, bs: 0.63*, List tab + 0.88*, List o + Not at 0.55*
		rmatted: Indent: Left: 0.25", bs: 0.63", List tab + Not at 0.25"
(c) ·	- Spaint 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	rmatted: Indent: Left: 0.25", ace After: 0 pt, Outline numbered .evet 1 + Numbering Style: 1, 2, + Start at: 1 + Alignment: Left .ligned at: 0" + Tab after: 0.25" .ndent at: 0.25", Tabs: 0.63", List + Not at 0.25"
$(\epsilon)$	Ž	leted 5
- /	may School	Teted: Since t
1	S were	leted: us
	فالإفطالار ا	leted: 45
	, ), <u>, , , , , , , , , , , , , , , , , </u>	leted: As auch, i
		leted: ie
	2450000	leted: that
(c)	pia-sti-et-	leted: are going to be
		leted: icd
	Transition of	letad: would
·	7 me 'n .	leted: to
	,	leted: on
	, % ++ K'	rmatted: Not Psyslight
	1.50	Johnson /7 Market

Deleted: Del	2_	Delated: . /ormatted: dulets and Numbering
Deleted: b  Deleted:  Dele	(6)	and the second s
Deleted: Deleted:  Deleted	9	Deleted: 65
Deleted: ad	(c)	Defeted:
	(c)	
		Deleted: cd
CC) • Deleted: ' (C) • Formatted: Underline	<u>,'</u>	The state of the s
Ocieted L 65 3 Formatted: Fort: Bold	(c)	Deleted L 65 3

001.285

		Caleted: that
Ĺ		
$(\mathcal{E}_{i})$		
#		
·	, )	
. 1		Deleted: for
2	. We in the control of the control o	Oeletedi
<del>)</del>		Deleted: for
		Oeleted: their
		Deleted: notice
		Ocieted:
		Deleter 6
		Comment [mri3]:
	•	
		Deleted: Deleted:
- _ \		
5 )L		Convent (mr14):
i		. 63
1 		Oeleted:
		Deleted: 63
(c)•		
The Article 29 Working Party	noted, "The Working Party considers that information	· Daleted:
should be provided to passengers n  Even if the transfer of PNR data t	to later than the moment when the passenger gives their agreement to buy the ticket	Deleted: r
of what that means in terms of the	processing of their personal data if the information is given to them before they buy	The control of the co
the ticket."	65	Deleted: "
<b>L</b>	<del></del>	

001.286

(C)		Deleted: their
		Deleted: to
(E)	6	Deletad: L 65 D  Deletad: (.  Deletad: 7)
(e)		Deleted: It  Oeleted: C 6 5 1  Oeleted: ua  Deleted: c  Oeleted: c
(c)·		
(°)		Deleted: (
(c)·		Deleted: 65)

		Deleted: of the
1		Defated: pressed
	1 ,	Deleted: 65 3
	61	Deleted: c
?		Deleted: issue
~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~	-	
		Deleted: 5 b5 3
cc: Paul Rosenzweig, Couns	elor	

Page 3: [1] Deleted	michael,scardaville	5/2/2007 4:57:00 PM
<u> </u>	b 5	$\mathcal{L}_{\mathcal{L}}$
Page 3: [2] Deleted	michael.scardaville	5/2/2007 4:58:00 PM
<u></u>	b5 3	



# [62 ]

## 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)

\ \ \

001290

( ) ( )

Derived from Schneider INFR Declassify September 7, 2022 C i (c) (C) (c)



(c)

(c).

Comment [m1' b5 ]

(c) = -

6

(6) 0

Comment (m2):

(c)

Comment (m3) 65 2

(c) ·

001.202



(0)

(C)

The Article 29 Working Party C 55 > 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.



(4)

(c).

(0)

(0)

(c).

. Even if the transfer of PNR data has become in gractice 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.

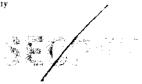
corroai

(e) (c)

(6)

ce: Paul Rosenzweig, Counselor





[ 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 ( )

Overview:

Deleted: Formatte line: 0", Tabs: 0.5", List tab

Deleted: that

Formatted: No builets or

numbering

Formatted: Indent: Left: 0.5", Hanging: 0.5", Tabs: 1", List tab

Formatted: No bullets or

numbering

Deleted: Lb5

Formatted: Indent: Left: 0.5", Hanging: 0.5", Tabs: 1", List tab

Formatted: Bullets and Numbering

Deleted: that

Deleted: the

Deleted: 1

Deleted: 1

Formatted: No bullets or numbering, Tabs: 1.25°, List rab

Formatted: Indent: Left: 0.5", rianging: 0.5", Tabs: 1", List tab

Derived from Schneider MFR Declassify September 7, 2022

e/		7/2	1
	1	/	

(c)		
C-//		Deleted: that
(c)		
- /!		Deleted: ed
(6)		Deleted: that
<b>;</b>	\ \	Deleted: and
ì	\_ \	Deleted: of
	<b>1</b> 0 '	Deleted: the
	The state of the second desirence of the second sec	Defeted: s
i I		Deleted: a
		Deleted:
(c)		Formatted: Font: Italic
*		
(u) issues:		
(c).		
(c)	1 1	
,	$\wp$ $\iota$	
1	•	

L 65

(c)	Deleted; those
	Deleted: would
	Deleted: d
	Comment [mri1]: This doesn't make
	Deleted: -
	Deleted: 65
	Deleted: Y
(c)	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"
(c)	Comment [m2]: 5 ]
	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"
	Deletari.
(c) · (c)	[ P2 ]
(c)	Deleted: Since t
•	Deleted: us
	Deleted: as
	Deleted: As such, i
	Deleted: re
• •	Deleted: that
$(\mathcal{E})$	Deleted: are going to be
	Deleted: icd
	Deleted: would
	Deleted: to
1	Deleted: on
	Formatted: Not Highlight

	Deleted: 65 7
(c) °	Deleted: 65
(c) ·	Deleted: 65 7 Deleted: C 65 7
(c) o	Deleted: \(\frac{1}{2}\) Deleted: \(\cdot\)
(c) (c)	Deleted:
(c)	Formatted: Underline  Deleted: [ 5 2 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5

(G)	•	
, <u> </u>	<b>\</b>	Deleted: for
( C )		Deleted:
		Deleted: for
1. 1. 1. 1.	<i>( )</i> ·	Deleted: their
	•	Deleted: nature
	ஆக் நிரு வருண்ணும் இரு இதன்கள் அன்று நிரு இரு முற்று வரும் முற்றும் முற்றும் இரு இரு இரு இரு இரு இரு இரு இரு இரு	Deleted: , (
ì		Deleted: deployment
(c)		Deleted:  Deleted:  Deleted:  Deleted:  Deleted:
(s)		Comment [mri4]:
(°)	•	Deleted: Deleted:
(c)	· · · · · · · · · · · · · · · · · · ·	
1	The Article 29 Working Party _ 65 3 noted, "The Working Party considers that information	Seleted:
	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 to: traveling to the US, passengers are only aware	Deleted: r
:	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."	Deleted:

(3)

		Deleted: at
[c]		Deleted: LD
		Deleted [ 65 ]
		Deleted: has
(c)	•	Deleted: ( b3 5
,	1	Deletad: ?)
		Deleted: tr
entante saulin man ou des Addresses recognité impresson que es establisse et		Deleted: on
		Deleted: to
c) ·		
<b>9</b>		Deleted: t
: )		Deleted:   55
• )		Delated:

Deleted: pressed

Deletad:

Ь5

Deleted: Issue

Deleted: [ 65 ]

ce: Paul Rosenzweig, Counselor

Background: === 65 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 65 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. )

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

Derred: Schneide MPLaw Enforcement Sensitive

(25)



Man Jan 19

(7)

(C)

(0)

Mrss mil

(c)

(C) \*

<sup>2</sup> EDPS Press Release, May 30, 2006

001370

Law Enforcement Sensitive

6

C/Post

6°

(c) >

f) >

001371

Law Enforcement Sensitive

(b)

(G) \*!

### Options for PNR Negotiations with the El-

7.28 m Background: an informational agreement was struck between DHS and the St. in 2004 got arrong ( 39%) to rese to PNR from the all the agreement was junckly enaderged a court by the bur pear Par fament. On 5:30:05 the European Court of Isable rided that the release appropriately entered into this Spriament. On 3 00 05 the Euch pean south of cause onest matches is appropriate concernment as the grounds that the 1905 Objective and matches 2 Objective is mash. Possiblenes and re-Commission terminated the agreement effective 9.30.06. The Famon Presidency also received a handate from the European Council to negotiate a replacement agreement by 9.30. The Commission are sented the  $\ell$  SG with a people sent text on  $^{\frac{1}{2}}$  . S

Further Parliament Com Motion for a Resolution on the least of Committee autain in the SWAP Contemby the Living terminal content of Swap Contemby

Law Forth Sensitive

Derina Schnedu MAR

112 Harris - 2/2021

(6)

 $C_{i}$ 

i/Poz.

(()

<sup>2</sup> EDPS Press Release, May 30, 2006

Law Enforcement Sensitive

Law Enforcement Sensitive

(C)

(1)

(c) \*

6

CHIZEHIM.

Law Enforcement Sensitive

	Options for PNR Negotiations with the EU	
(0)	Background:   San international agreement was struck between DHS and the Et. in 2004 governing CBP's access to PNR from the Et The agreement was quickly challenged in court by the European Parhament. On 5.30.05 the European Court of Justice ruled that the Et. inappropriately entered into this agreement on the grounds that the 1995 Directive did not apply   On 7.3.06, the Finnish Presidency and the Commission terminated the agreement effective 9.30.06. The Finnish Presidency also received a mandate from the European Council to negotiate a replacement agreement by 9.30. The Commission presented the 1.5G with a proposed text on 7.15.	Deleted b _ ]
(C)		Deleted: C65]
		b l
		Deleted: C 65 3 Deleted: .

Law Enforcement Sensitive

Periodi Schneider MFR Pe duii : 7/dux1

1

001377

Deleted: us

Deleted: 1



<sup>&</sup>lt;sup>1</sup> 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

<b>Options</b>	for	<b>PNR</b>	Negotiations	with	the	EU
-			7/28/06			

CONTINENTAL

1		ie (C. 1717)
a P		
_		
(C)1 1/PGZ		
1/PG7.		we.
· ·		
(C)		0
		. Deleted: M
EDPS Press Release, May 30, 2006	Law Enforcement Sensitive	Deleted: C 5 5

(C)			(6)	Deleted: \
			,	Deleted: 12
			.(0)	Deleted: L 55 5
(()				Deleted: A Deleted: M Deleted: M
				Deleted: W Deleted: S Deleted: P
				Deleted: \\ Deleted: \\ Deleted: \( \)
C/CGF Mal			8	[2]
				Deleted: W
				Deleted: \(\)
C/#			D.	Deleted: S  Deleted: P  Deleted: P  Deleted: Note: The second of the sec
CAROT				Deleted:
(6)	Law Enforcement Sensit	ıve		Deleted: W
	,		/	

Law Enforcement Sensitive

	Deleted: Deleted: Deleted: Deleted: Deleted: Deleted: Deleted:
	Deleted: W Deleted: W

# Options for PNR Negotiations with the EU $^{2.28\,\%}_{0.00}$

	Background: C  Jan international agreemer access to PNR from the EU. The Parliament. On 5.30.05 the European agreement on the grounds that the 199 Commission terminated the agreeme mandate from the European Council is presented the USG with a proposed text.	25 Directive did not apply 2	ne EL inappropriately ente	red into this
CC)	Schnish man san ma	orespect Sensor	· · · · · · · · · · · · · · · · · · ·	1.381

(c)

C/For

(c)

 $\mathcal{P}$ 

(0)

E

(6)

(0)

(X

(0)

(1)

(1)

C/PGF Med

(2)

(O)

C/PGJ-M

CC

(1)

001383

Law Enforcement Sensitive

17/

(1)

arm Kali

001384

Law Enforcement Sensitive

Options for PNR Newsonia

	Background:	
	It international agreement was struck between OHS and the EU in 2004 governing CBP parliament. On 173 IS the European Court of Towards and the EU inappropriately entered into the 2005 Directive did not apply.	in is
	Finnish Presidency also received a mandate from the managed the agreement effective 130.96. The	e t
6		
		ेबांबरबर्त: <sub>उ</sub>
(8		
(A)		
i		S <b>eletod:</b> रिक
(E)		Defeted: few Defeted: decisions Defeted: metaling
-()		
<u> </u>		

Derail Schnolder - FR. Decinal 2/Lax



Options for PNR Segotiations with the Et

Deleted: Defeted: Deleted: at least Deleted: C 65 3 Deletad: Sat any Deleted: .1 Formatted: Fort Sold Formanted: Indent .aft: 0.75" Formatted: 'ont 30st Formatted: (vident | eff | ) 15th Deletod: and a

Formatted: Fort: Bold Formatted: Indent: Left: 0.75\*

Deleted: , each of which is discusse below

Deleted: ing

(0)

b

Delessa.

Law Enforcement Sensitive

FOR OFFICE LUSE ONLY

CONFIDENTIAL

Attachment B

Substantive DHS Comments on NSC Draft Discussion Paper

65

(c)

6

61

FOR OFFICIAL SE ONLY

Period Tohnelle MFR

Pesting 1 1/2022

CONFIDENTIAL

FOR OFFICE LISE ONLY

CONFIDENTIAL

(7)

b

(6)

Paue 4 - L

(v)

b 5

(1)

6

CONFIDENTIAL

FOR OFFICIAL I SE ONLY

CONFIDENTIAL

Historical Background (V)

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 he no ambiguity about the capability to create rights in favour of third parties.

 L 65 3 the Canadian governmen	it incorporated their "Commi	itments", the fa	nctional	
equivalent of CBP's Undertakings, in	to domestic regulations (	65	こ	
L 65	⊃ <u>Sæ</u>	<u>e</u>		. 😺
tip, canadagazette go ca partil 2005	5 2005, 2, 4 html/sor246 e h	tm: and a copy	ot thin	Vq
ommimients contained in Autex A	hereoft		7	Comment L 13   sent light co
r	<b>-</b> ~		1	his this squality, against white
L	62			ordingly,

CONFIDENTIAL

Derived: Schreider MFR Declars: 31 Dec 2021

COMPLEMENTAL

(W) [ 65

legal Impact of Making Undertakings "Binding" (V)

(0)

(C)

331457

TO FULL IN

DEPUTIES MEETING ON PNR

DATE:

Tousday, July 15, 2016

TIME:

and Francisco

LOCATION:

TBD

FROM:

Stawart Baker, Assistant Secretary for Policy

### OBJECTIVES DESIRED OUTCOME OF MEETING:

Establish an interagency negotiating position

65 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.

#### PARTICIPANTS:

Non-DHS

 $\triangle HS$ 

Deputy Secretary Jackson

PRESS PLAN: "Closed"

#### ATTACHMENTS:

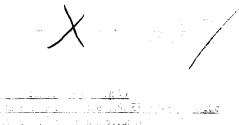
- A. Discussion Document: Analysis of United States Interests in the U.S.-EU PNR dialogue (7,13/96)
- B. Memo: Summary of Potential Changes to the Undertakings (PENDING)
- C. Member State Positions known as of 7/20/06
- D. Background on EU views of consent as a solution
- E. DHS' Response Options to European Court of Justice Decision (February 2005)

Prepared by: Michael Sciedaville, PDEV, L

62 (10~)

601499

FOR OFFICAL USE ONLY



Purpose

To provide you with background information on the Passenger Name Record (PNR) issue and ulated 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', 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 duropean standards, and commercial data transfers to the U.S. have long been restricted by the lack m'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.

BP 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

001875

Derived: Schneider MFLL Subject: Eulphe Declass: 20 July 2031

Biack Formsthaa: Centered, Indent: Left:

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

Fernantical Font: 12 pt. Fant color:

Dalated: U.S. Orpanissis is Washington, DC 205285

<sp> Formatted: Top: 1", Bottom: 1" Deleted: 4

Formatted: Centered Formatted: Font: Not Italic Deleted: 1



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.

(W)

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. <u>The USO received a proposed replacement text from the Family Prestage Commission of Commission of Commission of Commission of Commission of Commission of Commission as a technical change that would put the same agreement back in place, albeit under a different legal authority.</u>









(n)

<sup>2</sup> CBP can share PNR data with other law enforcement agencies, but only on a case-by-ease basis and only for the purpose of combating terrorism and serious transmational 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.

(n)

et in de Negari nome of Nuly induscriolland oes 1936, has e Amarinet in pressions degations die dead copacit d Post in the 19 of 1995 in 12 degree by the least lead. Confessionalistic contra Rights in additional of the co Large of the signal and self for Long tropen by the Least sector folic (Rendes



\ \ \

### Background

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

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

bl

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

(c)

(0)

(0)

r\_\_\_\_.

(0)

4

SE





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."

<sup>a</sup> 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."

61

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.

b

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

60 z

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.

<sup>1</sup> 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.



المؤذ

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

† "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

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.

7



## Analysis & Recommendation

(2)



<sup>13</sup> 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.

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.

X

Formatted: Font: Bold, Underline

1 ' memsion

\

b

Deleted: C 65 T

## Conclusion

(10)

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.



b

9

For Office Vess Only

ನೆಂದಾರುವುದು Centered

6

10



The second secon

<u>, Table Table of Belle de Ballet bellebourbary (AMENT ASSOCRABER OF SCH</u>urch). Table 185

65. 56.

#### 22.24.8

1. This Back of a smile of the conferences as at contoured data which or purply by any many many many of the contour of the

and the state of t

The second of modes in this tentils to be despited at Community for some since the first to fitted A and Ad an ine frequent European Union and at any case in processing a succession of control of the Assault of the fitted and the second of the second of the second of the fitted and the fitted of the fitted and the fitted of the fitted o

भारतराह उठ

#### Unformations

As Any of derogation if the Article 15 and sails offices otherwise provided by demestic low easy entirely particular cases. Member States of all to uside that a transfer or a set of transfers of carbonal data to a third or other a finish loss that ensure an adequate level of projection of thin the treatened of these 25 can got take place a castrodic or had

is the face at just thus are one as exposent they followed by the produced transfer, in

Late maps on is independent for the performance of a commact between the data subject, and the complete in the supplier command in a commandate the acceptance taken in respected to the state constate the state of the state constate of the state of the

The admention's necessary for the expression of a continuous of a contract concluded in the
construct be large adjusted to see continuous and a four party; or

och men yr Abrae a<u>tt Remain ochbug hasnog</u>ian av Esingeen olluget och die einsteben 3. miljohen och der den dater

the last training the property and the contract of the last of the last princety of

Traffe trade to a traffe traverse repaire to the first of the secretary of the problem to a traffer to the secretary of the se

A. Figial Englished to Josephank II. a. Let 1001 black may be the read a manager of a set of
abeliant of personal deep to a long Judent long of deep repeats an adequate (excel) of
tection of the major of the North and tection of the amount additional and repeats against a sequence.

Prophysical Centered

Firm stedt Font: Bold

Formatted: Font: (Default) Times New Roman, 12 pt Formatted: Indent: Left: 0"

i I



on a <u>describenta da severa da la capación de la capación de ser el ser el ser el transportante de la capación</u> de La capación de la cap

Let Medices Same on the Castimism of the later as a surfied greatures (2.1.1.2.2.10) indirection, if the province and fundamental rights and freedoms of individuals, the Commission shall take analysis reasons in accommission while an arrivation land down in Article 31 (2).

The mean States shall take the necessary measures to comply with the Compression's accretion

A best the community of the design accordance with the procedure referred to an Article of the following transferred standard in a calculated transfer to surficient safegues as a required by paragraph a standard standard has been accessed on the sample of the following standards of the community of the sample of the following standards.

CHAPTER OF BANSET COMMERCACIALA LA CULTURA DE COLO RIEN

di Danisia

If the Interment States are all a scale are the measure of a direct enemies of personal data which are a defection as more series of the measure of the meas

Like adjection. The control of protestion attended to a third country that the assessed in the attended on the first and the control of the data that the property of the data the perpension of the data the perpensional and the property of the third country to measure and the protessional also and results measures which are excepted with in that country.

The Memory states and a projumnostion snarrational each other of cases where they consider that ordinary does not assure an adequate sevel of protection or thin the meaning of a factorian 2.

4. Species of Computation and Associated the presenting Conversed Computations of a 20, and a physical Conversed Computation of the Conversed C

5. \* The size, while the confidential expension of a large size of the size of the confidence of the confidence of the size of the size

t. The Commission may limit in accordance with the procedure referred as in Ambre 2012. This along security shorts we adequate level of materials within the obtaining of paragraph 2 of The Amicle, in reason, it is domestic that in or the international commitments in has entered.

and a second of the second of

- 1.1. Section of the Property of police and Protected respective to personal Later to revert in the framework of police and Protected respectition to criminal matters

1. Oak 1

Land of the second of the But the But the But the second of the But the But the But the Second of the But the

25. The makes fixed a 24 de mai densina. This technical friance bette at a fame of the more and authority of more employees. State and the first and manifered in comprehen a according to the fixed scanners of the intermational bodies except it such transfer is in compliance with this transfer of the Decision and, an particular, all the fellowing requirements are met.

4. The plantier is provided for by law tlearn with give or authorising it.

The transfer is necessary for the purpose the data concerned were transitived or made evaluable for or for the purpose of the prevention, intestigation, detection or prosecution of extramal frences of for the purpose of the prevention of threms to public security or to a person, except there such considerations are occurrided by the need in protocit the interess or fundamental mants the data of great

(c) The competent concerns of another Member State that has nonsmitted or made a concern the land converned to the competent surhorits that extend to during the them has given its prior a page to concern for the prior of page to contain a page.

(a) A physical exist of gate proposition as each to the first of Decimal to the Parish of Containing to Today to the first large reach mediance, for standing of

- An An Antage of the Antage o

The Montest places and the Commission of the ELIGIBLE And Internal Sizes in the City and the Commission of Commission of the Commission of Commissio

3 a type, an set the procedure provided for an active 15. It is established that a third coupling or the manufact for an adequation of paragraph. Member States shall take the measures makes are to proport any transfer of paragraph.

Formatted: Indent: Left: 0"

Formacted: Font: (Default) Times New Roman

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

Formatted: Font: (Default) Times hew 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

Formattad: Font: (Default) Times New Roman

13

001593

UNCLASS



• Louis College of the second control of the second college of the second second second of the college of the second of the second college of the secon

The reference of the sound of a received of the fire connectent anthorne, of another the reference of the description of the description of the sound of the soun

Tormained: Centered

Romatted: Font: (Default) Times New Roman

Formatted: Font: (Default) Times New Roman

14

001639

UNCLASS

Moshington, DC 20528





b5

# <u>DISCUSSION DOCUMENT</u> <u>Analysis of United States Interests in the U.S.-EU PNR dialogue</u> Department of Homeland Security

ruly 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<sup>4</sup>, 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

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 planted in advance with local authorities. Analysis continues up to arrival and is further supported by the collection of manifest information.

302.

Denved: Schneider MFR Subject: Eul PAR 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.

65

Chair

b 1

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

ECBP 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. 

USG received a proposed replacement text from U by the Finnish Presidency on July 19th, although Commission officials have indicated that this draft may not be 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.

(S)

b

## Background

- Two converging events in Europe the recent European Court of Justice decision on the legality of the EU-US PNR Agreement and a draft EU Framework Decision on Exchange of Criminal Data -- have major implications for US law enforcement and security.
- 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
- Both the Departments of State and Hospeland Security have a number of questions regarding the legal impact of a variety of wording chances, including references to the European Convention on Parties Rights. Additional policy coallysts is underway and will be further power by the decisions of the Deputies.

## For Official See C niv

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

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



w !

<sup>6</sup> 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."

0

## For Official Use Cally

The ECLENR 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 ECI 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 ECI held (as the US had argued earlier) that the requirement that PNR data be sent to the US was a law enforcement and national security matter. Such transfers, the court held, were excluded from the data protection directive governing commercial data exports. If they are to be regulated, the court implied, it would have to be done under the "Third Pillar."

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

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.

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.

.001695

Re Official Use Caly

alfrice)

<sup>3</sup> 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.

drig)

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 30<sup>th</sup> 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



<sup>12</sup> 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.

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-IIHS MOU.

<sup>&</sup>lt;sup>14</sup> 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.

Per Official Use Only

(5)

Conclusion

<

6

Conclusion

001693

# For Official Vet Caly

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.



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.



- 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**

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

(Clair) 1

61

001704

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.

(2)

FOR OFFICIAL USE ONLY

Derived: Schneider MFe Subject: EV (PNR) Declass: 13 July 2031 266.

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 (ECI) 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. 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

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 mustration over losing access to this information:

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.

(5)

(5)

## Background

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

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. Several of the limitations in those Undertakings

(c)

b



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

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

1.

------

7

bl

FOR OPEICIAL USE ONLY

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) tiled two suits in the European Court of Justice (ECJ) challenging the information sharing arrangement.

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."

( hos

FOR OF CLAL USE ONLY

- On May 30, 2006, the ECJ issued its opinion in the lawsuits. The opinion did not address the merits of the EU-US PNR Agreement or the role of the Parliament. Rather, the decision turned on the lack of competence of the Commission and Council to enter into the Agreement in the first instance. The EU had based its authority on the so-called "First Pillar," which allows the EU to regulate trade and commercial matters. The ECJ held (as the US had argued earlier) that the requirement that PNR data be sent to the US was a law enforcement and national security matter. Such transfers, the court held, were excluded from the data protection directive governing commercial data exports. If they are to be regulated, the court implied, it would have to be done under the "Third Pillar."
- That is what the EU proposes to do. It has obtained authority from its Member States to creek 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.
  - b
- EU Proposals on Sharing Law Enforcement Information. If that were all that is at stake, this would be an interesting diplomatic and legal problem for DHS. But it is not. The PNR negotiations will be closely intertwined with a broader effort 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.

P1

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 tlights.

FOR OFFICIAL USE ONLY



 $(5)^{\mathsf{T}}$ 

Chair

6

(clay)

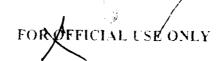
For example, the Draft Decision contains provisions on time limits for retention of shared data, ensuring the accuracy of shared data, logging and audit trails, as well as restrictions limiting further use of the data to the original purpose for which it was first transmitted. In effect, it borrows heavily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

(0/23/2)

bl

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 30<sup>th</sup> 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.

## Analysis & Recommendation

(C)

FOR OXFICIAL USE ONLY

<sup>&</sup>lt;sup>2</sup> 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.

<sup>(</sup>a) 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.

<sup>\*</sup>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.

-(5)

b

## Conclusion

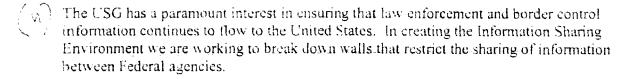
(0)

(5)

6 l

<sup>15</sup> 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 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)

6

## (c)

## 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)

001713

FOR OFFICAL USE ONLY

## Attachments:

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

			-
A 1	rtic	· I A	- 4
. "			

Scope	
-------	--

- 1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.
- 2. This Directive shall not apply to the processing of personal data:
- in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,

#### Article 26

## **Derogations**

- 1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:
- (a) the data subject has given his consent unambiguously to the proposed transfer; or
- (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or
- (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or
- (d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or
- (e) the transfer is necessary in order to protect the vital interests of the data subject; or
- (f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.
- 2. Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.
- 3. The Member State shall inform the Commission and the other Member States of the authorizations it grants pursuant to paragraph 2.

FOR OFFICIAL USE ONLY

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

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

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

## CHAPTER IV TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES -

Article 25

### Principles

- 1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.
- 2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.
- 3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.
- 4. Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.
- 5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.
- 6. The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.

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

FOR OFFICIAL USE ONLY
UNCLASS

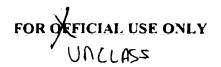


B. Proposal for a COUNCIL FRAMEWORK DECISION on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters

Article 15

Transfer to competent authorities in third countries or to international bodies

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

FOR OFFICIAL USE ONLY



#### Attachment C

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

July 13, 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<sup>1</sup>, protecting against mid-flight hijackings and bombings.

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

(1/6)

6

001713

CBP may automatically access PNR data from European earriers 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. 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

FOR OFFICIAL USE ONLY

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.

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 malysis is underway and our response will be driven by the decisions of the Deputies.



(5)

b

7;

٤

#### Background

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

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. Several of the limitations in those Undertakings

P.

001720

FOR OFFICIAL USE ONLY

SECRE

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

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

1.

4

61

FOR OFFICIAL USE ONLY



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.

"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."

(

FOR OFFICAL USE ONLY

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

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

6

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.

61

001.723

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 ECI 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.

6

(/m)

<sup>9</sup> 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.

bl

001734

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 30<sup>th</sup> 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. <sup>13</sup>

#### Analysis & Recommendation



FOR OFFICIAL USE ONLY

<sup>12</sup> 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.

<sup>&</sup>lt;sup>13</sup> 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.

<sup>&</sup>lt;sup>14</sup> 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.

#### Conclusion

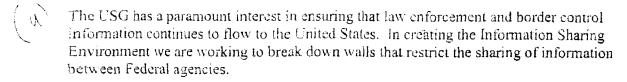


001726



<sup>15</sup> 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 6<sup>th</sup>; France 9<sup>th</sup>; the Netherlands 10<sup>th</sup>; and Italy 17th.





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.



#### Attachments

- A. Excerpt from EU Data Protection Directive 95/46/EC (24 October 1995) (u)
- B. Excerpt from Draft Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matter (October 2005)

001.727



#### Attachments:

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

Article 3

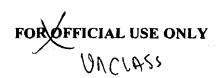
Scope

- 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.



001728

-



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.

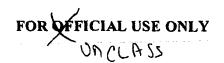
#### CHAPTER IV TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

#### 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.



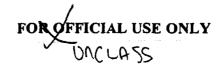


B. Proposal for a COUNCIL FRAMEWORK DECISION on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters

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.



06L730



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

FOR OFFICIAL USE ONLY
UN CLASS