William_K._Kelley@who.eop.gov

From:	William_K._Kelley@who.eop.gov
Sent:	Thursday, December 22, 2005 5:49 PM
To:	Bradbury, Steve; Brett_M._Kavanaugh@who.eop.gov
Attachments:	tmp.htm; NSA (b) (5) .final.doc

Attached is the final of the (b) (5) talker for DOJ to finalize and distribute. Steve, can you send back a pdf? Thanks.

duplicate

Bradbury, Steve

From: Bradbury, Steve
Sent: Thursday, December 22, 2005 6:41 PM
To: 'William_K._Kelley@who.eop.gov'
Cc: 'Brett_M._Kavanaugh@who.eop.gov'
Subject: PDF of (b) (5) talkers
Attachments: NSA (b) (5) final.pdf

Bill: As you requested, PDF of the final (b) (5) talkers. Steve

Harriet_Miers@who.eop.gov

From: Harriet_Miers@who.eop.gov
Sent: Saturday, December 24, 2005 9:15 AM
To: Bradbury, Steve; Brett_M._Kavanaugh@who.eop.gov; William_K._Kelley@who.eop.gov
Subject: Re: New article

Have seen it.

-----Original Message-----
From: Steve.Bradbury@usdoj.gov <Steve.Bradbury@usdoj.gov>
To: Miers, Harriet <Harriet_Miers@who.eop.gov>; Kavanaugh, Brett M. <Brett_M._Kavanaugh@who.eop.gov>; Kelley, William K. <William_K._Kelley@who.eop.gov>
Sent: Sat Dec 24 08:33:42 2005
Subject: New article

There's a new article by Risen and Lichtblau in today's NYT.

William_K._Kelley@who.eop.gov

From: William_K._Kelley@who.eop.gov
Sent: Friday, January 06, 2006 6:15 PM
To: Bradbury, Steve; Elwood, John; Harriet_Miers@who.eop.gov; David_S._Addington@ovp.eop.gov; Brett_M._Kavanaugh@who.eop.gov
Subject: RE: (b) (5) Talkers.doc

I agree with Harriet that (b) (5) . In addition:

Paragraph 1: (b) (5) ."

Paragraph 6: (b) (5) . Finally, the last sentence is a run-on, which should be separated into two sentences.

-----Original Message-----
From: Miers, Harriet
Sent: Friday, January 06, 2006 5:48 PM
To: 'Steve.Bradbury@usdoj.gov'; Kelley, William K.; Addington, David S.; Kavanaugh, Brett M.
Subject: RE: (b) (5) Talkers.doc

Should there be (b) (5) ?

-----Original Message-----
From: Steve.Bradbury@usdoj.gov [mailto:Steve.Bradbury@usdoj.gov]
Sent: Friday, January 06, 2006 5:18 PM
To: Kelley, William K.; Addington, David S.; Kavanaugh, Brett M.; Kyle.Sampson@usdoj.gov; Courtney.Elwood@usdoj.gov; Mitnick, John M.; Miers, Harriet
Cc: John.Elwood@usdoj.gov; William.Moschella@usdoj.gov; Brian.Roehrkasse@usdoj.gov
Subject: (b) (5) Talkers.doc

As promised, here are some talkers responding to (b) (5) . I am also copying DOJ's Offices of Leg Affairs and Public Affairs. They will coordinate with you and WH Communications before sharing outside. I'm running now to a meeting at the Sit Room. Thx.

Bradbury, Steve

From: Bradbury, Steve
Sent: Saturday, January 07, 2006 8:45 AM
To: 'Harriet_Miers@who.eop.gov'; 'Katie_Levinson@who.eop.gov'; 'Dana_M._Perino@who.eop.gov'; 'Brett_M._Kavanaugh@who.eop.gov'; 'John_M._Mitnick@who.eop.gov'
Subject: Re: (b) (5) Talkers.doc

Pls note that (b) (5) .

-----Original Message-----
From: Bradbury, Steve <Steve.Bradbury@SMOJMD.USDOJ.gov>
To: 'Harriet_Miers@who.eop.gov' <Harriet_Miers@who.eop.gov>; 'Katie_Levinson@who.eop.gov' <Katie_Levinson@who.eop.gov>; 'Dana_M._Perino@who.eop.gov' <Dana_M._Perino@who.eop.gov>; 'Brett_M._Kavanaugh@who.eop.gov' <Brett_M._Kavanaugh@who.eop.gov>; 'John_M._Mitnick@who.eop.gov' <John_M._Mitnick@who.eop.gov>
Sent: Sat Jan 07 08:38:30 2006
Subject: Re: (b) (5) Talkers.doc

(b) (5) .

-----Original Message-----
From: Harriet_Miers@who.eop.gov <Harriet_Miers@who.eop.gov>
To: Bradbury, Steve <Steve.Bradbury@SMOJMD.USDOJ.gov>; Katie_Levinson@who.eop.gov <Katie_Levinson@who.eop.gov>; Dana_M._Perino@who.eop.gov <Dana_M._Perino@who.eop.gov>; Brett_M._Kavanaugh@who.eop.gov <Brett_M._Kavanaugh@who.eop.gov>; John_M._Mitnick@who.eop.gov <John_M._Mitnick@who.eop.gov>
Sent: Sat Jan 07 08:34:13 2006
Subject: RE: (b) (5) Talkers.doc

(b) (5) .

-----Original Message-----
From: Levinson, Katie
Sent: Saturday, January 07, 2006 8:29 AM
To: Perino, Dana M.; Miers, Harriet; Kavanaugh, Brett M.; 'Steve.Bradbury@usdoj.gov'; Mitnick, John M.
Subject: Re: (b) (5) Talkers.doc

(b) (5)

-----Original Message-----
From: Perino, Dana M. <Dana_M._Perino@who.eop.gov>
To: Miers, Harriet <Harriet_Miers@who.eop.gov>; Kavanaugh, Brett M. <Brett_M._Kavanaugh@who.eop.gov>; 'Steve.Bradbury@usdoj.gov' <Steve.Bradbury@usdoj.gov>; Mitnick, John M. <John_M._Mitnick@who.eop.gov>
CC: Levinson, Katie <Katie_Levinson@who.eop.gov>
Sent: Sat Jan 07 07:53:42 2006
Subject: Re: (b) (5) Talkers.doc

(b) (5)

-----Original Message-----
From: Miers, Harriet <Harriet_Miers@who.eop.gov>
To: Kavanaugh, Brett M. <Brett_M._Kavanaugh@who.eop.gov>; 'Steve.Bradbury@usdoj.gov' <Steve.Bradbury@usdoj.gov>; Mitnick, John M. <John_M._Mitnick@who.eop.gov>
CC: Perino, Dana M. <Dana_M._Perino@who.eop.gov>
Sent: Sat Jan 07 07:47:11 2006
Subject: RE: (b) (5) Talkers.doc

That was my understanding. (b) (5) .

-----Original Message-----
From: Kavanaugh, Brett M.
Sent: Saturday, January 07, 2006 7:40 AM
To: 'Steve.Bradbury@usdoj.gov'; Mitnick, John M.; Miers, Harriet
Subject: RE: (b) (5) Talkers.doc

Am I right in assuming (b) (5) ?

-----Original Message-----
From: Steve.Bradbury@usdoj.gov [mailto:Steve.Bradbury@usdoj.gov]
Sent: Friday, January 06, 2006 8:44 PM
To: Mitnick, John M.; Miers, Harriet; Kavanaugh, Brett M.
Subject: (b) (5) Talkers.doc

Attached are revised talkers that incorporate WHC comments. John Elwood earlier sent a copy of these revised talkers to Bill Kelley. Thx.

<<(b) (5) Talking Points.doc>>

Bradbury, Steve

From:	Bradbury, Steve
Sent:	Saturday, January 07, 2006 9:13 AM
To:	'Katie_Levinson@who.eop.gov'; 'Dana_M._Perino@who.eop.gov'; 'Harriet_Miers @who.eop.gov'; 'Brett_M._Kavanaugh@who.eop.gov'; 'John_M._Mitnick@who.eo p.gov'
Cc:	'Debbie_S._Fiddelke@who.eop.gov'; Moschella, William; Scolinos, Tasia; Roehrkasse, Brian
Subject:	Re: (b) (5) Talkers.doc

Copying Will Moschella, Tasia Scolinos, and Tasia's Deputy Brian Roehrkasse on this message for contact purposes. They can also be reached at any time through the Justice Command Center at 514-5000. Thx

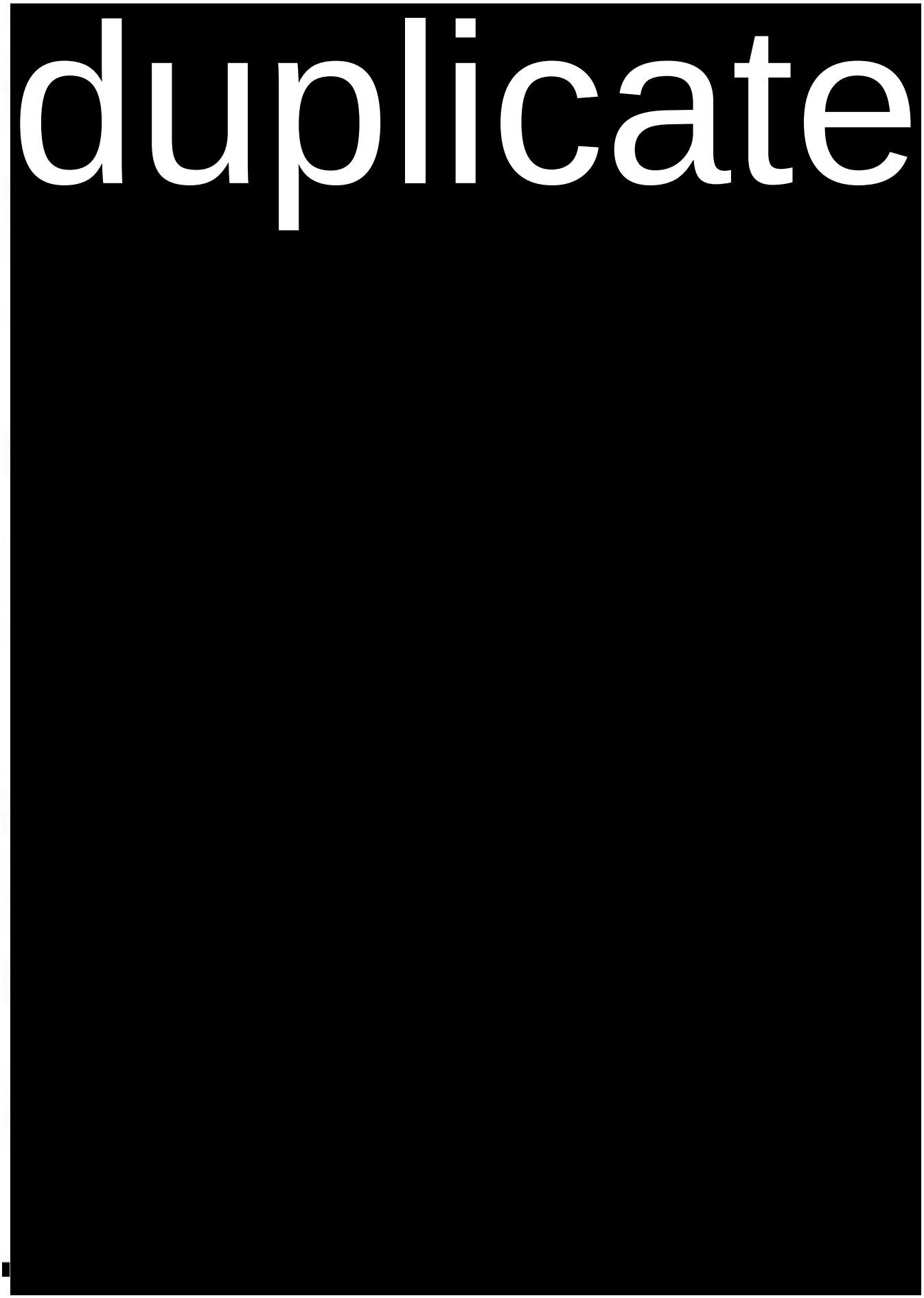
-----Original Message-----
From: Katie_Levinson@who.eop.gov <Katie_Levinson@who.eop.gov>
To: Bradbury, Steve <Steve.Bradbury@SMOJMD.USDOJ.gov>; Dana_M._Perino@who.eop.gov <Dana_M._Perino@who.eop.gov>; Harriet_Miers@who.eop.gov <Harriet_Miers@who.eop.gov>; Brett_M._Kavanaugh@who.eop.gov <Brett_M._Kavanaugh@who.eop.gov>; John_M._Mitnick@who.eop.gov <John_M._Mitnick@who.eop.gov>
CC: Debbie_S._Fiddelke@who.eop.gov <Debbie_S._Fiddelke@who.eop.gov>
Sent: Sat Jan 07 09:01:19 2006
Subject: Re: (b) (5) Talkers.doc

Deb - can your shop handle? I only have member cell phones with me on bberry (b) (5) .

-----Original Message-----
From: Perino, Dana M. <Dana_M._Perino@who.eop.gov>
To: Miers, Harriet <Harriet_Miers@who.eop.gov>; Levinson, Katie <Katie_Levinson@who.eop.gov>; Kavanaugh, Brett M. <Brett_M._Kavanaugh@who.eop.gov>; 'Steve.Bradbury@usdoj.gov' <Steve.Bradbury@usdoj.gov>; Mitnick, John M. <John_M._Mitnick@who.eop.gov>
Sent: Sat Jan 07 08:59:14 2006
Subject: Re: (b) (5) Talkers.doc

I can help coordinate with doj - katie, do you hapen to have contact info for their staff?

-----Original Message-----
From: Miers, Harriet <Harriet_Miers@who.eop.gov>
To: Levinson, Katie <Katie_Levinson@who.eop.gov>; Perino, Dana M. <Dana_M._Perino@who.eop.gov>; Kavanaugh, Brett M. <Brett_M._Kavanaugh@who.eop.gov>; 'Steve.Bradbury@usdoj.gov' <Steve.Bradbury@usdoj.gov>; Mitnick, John M. <John_M._Mitnick@who.eop.gov>
Sent: Sat Jan 07 08:34:13 2006



duplicate

Katie_Levinson@who.eop.gov

From:	Katie_Levinson@who.eop.gov
Sent:	Saturday, January 07, 2006 10:38 AM
To:	Bradbury, Steve; Debbie_S._Fiddelke@who.eop.gov; John_M._Mitnick@who.eop.gov; Brett_M._Kavanaugh@who.eop.gov; Harriet_Miers@who.eop.gov; Dana_M._Perino@who.eop.gov
Cc:	Moschella, William; Scolinos, Tasia; Roehrkasse, Brian; Jamie_E._Brown@who.eop.gov
Subject:	Re: (b) (5) Talkers.doc

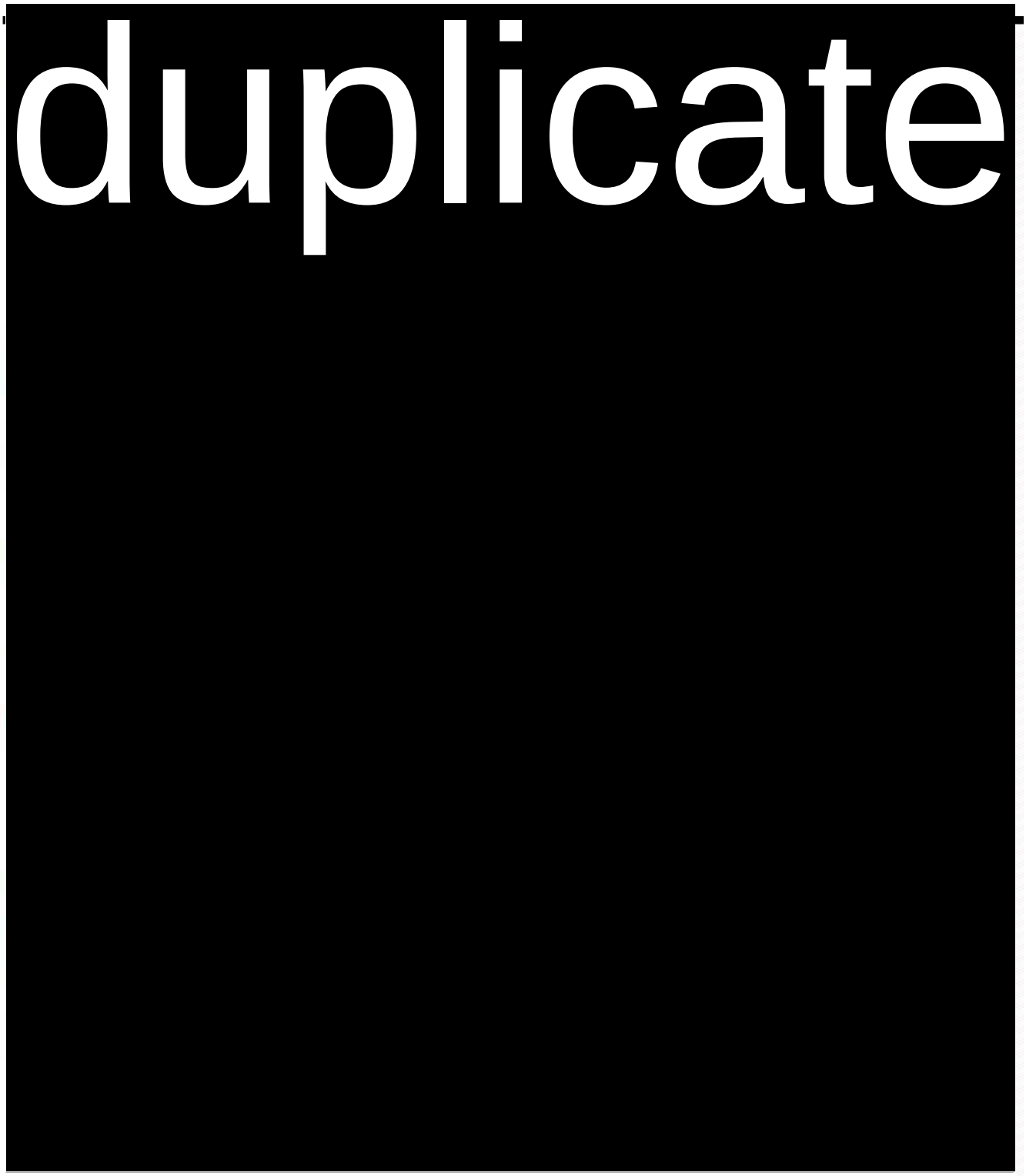
Can you call me? 494-4745

-----Original Message-----
From: Fiddelke, Debbie S. <Debbie_S._Fiddelke@who.eop.gov>
To: 'Steve.Bradbury@usdoj.gov' <Steve.Bradbury@usdoj.gov>; Mitnick, John M. <John_M._Mitnick@who.eop.gov>; Kavanaugh, Brett M. <Brett_M._Kavanaugh@who.eop.gov>; Miers, Harriet <Harriet_Miers@who.eop.gov>; Perino, Dana M. <Dana_M._Perino@who.eop.gov>; Levinson, Katie <Katie_Levinson@who.eop.gov>
CC: 'William.Moschella@usdoj.gov' <William.Moschella@usdoj.gov>; 'Tasia.Scolinos@usdoj.gov' <Tasia.Scolinos@usdoj.gov>; 'Brian.Roehrkasse@usdoj.gov' <Brian.Roehrkasse@usdoj.gov>; Brown, Jamie E. <Jamie_E._Brown@who.eop.gov>
Sent: Sat Jan 07 10:36:54 2006
Subject: Re: (b) (5) Talkers.doc

(b) (5)
.

-----Original Message-----
From: Steve.Bradbury@usdoj.gov <Steve.Bradbury@usdoj.gov>
To: Mitnick, John M. <John_M._Mitnick@who.eop.gov>; Kavanaugh, Brett M. <Brett_M._Kavanaugh@who.eop.gov>; Miers, Harriet <Harriet_Miers@who.eop.gov>; Perino, Dana M. <Dana_M._Perino@who.eop.gov>; Levinson, Katie <Katie_Levinson@who.eop.gov>
CC: William.Moschella@usdoj.gov <William.Moschella@usdoj.gov>; Tasia.Scolinos@usdoj.gov <Tasia.Scolinos@usdoj.gov>; Brian.Roehrkasse@usdoj.gov <Brian.Roehrkasse@usdoj.gov>; Fiddelke, Debbie S. <Debbie_S._Fiddelke@who.eop.gov>
Sent: Sat Jan 07 09:12:17 2006

duplicate



Bradbury, Steve

From:	Bradbury, Steve
Sent:	Saturday, January 07, 2006 10:38 AM
To:	'Harriet_Miers@who.eop.gov'; 'Brett_M._Kavanaugh@who.eop.gov'; 'John_M._Mitnick@who.eop.gov'; Elwood, John; Moschella, William; Scolinos, Tasia; Roehrkasse, Brian
Cc:	'Katie_Levinson@who.eop.gov'; 'Dana_M._Perino@who.eop.gov'; 'Debbie_S._Fiddelke@who.eop.gov'; Eisenberg, John
Subject:	Fw: (b) (5) talkers
Attachments:	tmp.htm; (b) (5) Talking Points.doc

Here are the same talkers with two typos corrected.

-----Original Message-----
From: (b)(6) Steve Bradbury (personal) <(b)(6) Steve Bradbury (personal)>
To: Bradbury, Steve <Steve.Bradbury@SMOJMD.USDOJ.gov>
Sent: Sat Jan 07 10:25:13 2006
Subject: (b) (5) talkers

Debbie_S._Fiddelke@who.eop.gov

From: Debbie_S._Fiddelke@who.eop.gov
Sent: Saturday, January 07, 2006 10:41 AM
To: Bradbury, Steve; Katie_Levinson@who.eop.gov; Harriet_Miers@who.eop.gov; Dana_M._Perino@who.eop.gov; Brett_M._Kavanaugh@who.eop.gov; John_M._Mitnick@who.eop.gov
Cc: Michael_Allen@nsc.eop.gov
Subject: Re: (b) (5) Talkers.doc

Yes, sorry thought this was Alito related. Michael and I will handle.

-----Original Message-----
From: Levinson, Katie <Katie_Levinson@who.eop.gov>
To: Miers, Harriet <Harriet_Miers@who.eop.gov>; Perino, Dana M. <Dana_M._Perino@who.eop.gov>; Kavanaugh, Brett M. <Brett_M._Kavanaugh@who.eop.gov>; 'Steve.Bradbury@usdoj.gov' <Steve.Bradbury@usdoj.gov>; Mitnick, John M. <John_M._Mitnick@who.eop.gov>
CC: Allen, Michael <Michael_Allen@nsc.eop.gov>; Fiddelke, Debbie S. <Debbie_S._Fiddelke@who.eop.gov>
Sent: Sat Jan 07 10:36:15 2006
Subject: Re: (b) (5) Talkers.doc

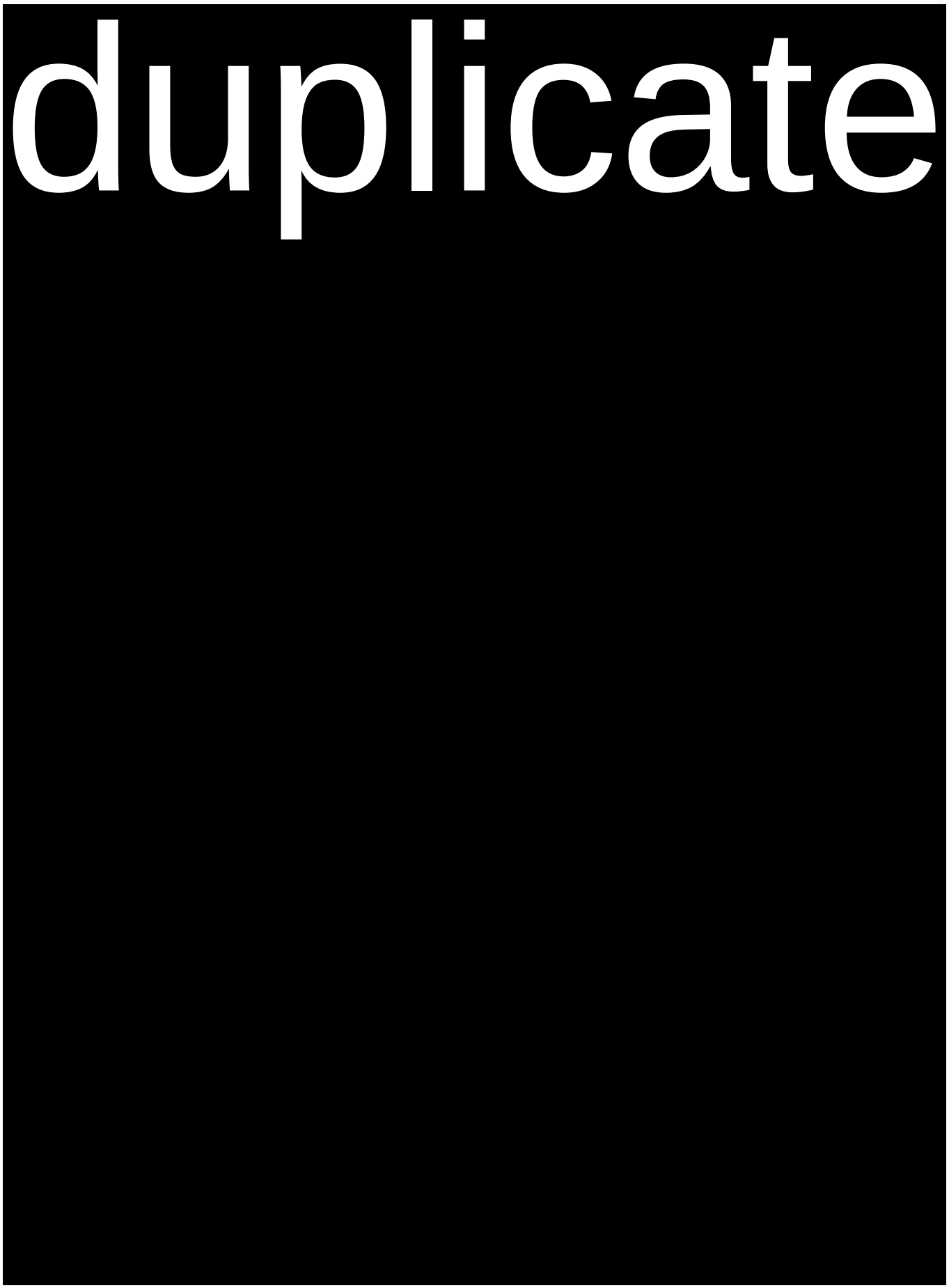
Was just on another email chain with Dan. Can WH leg affairs take lead in getting talkers to staff? Copying Michael Allen and Deb.

-----Original Message-----
From: Miers, Harriet <Harriet_Miers@who.eop.gov>
To: Perino, Dana M. <Dana_M._Perino@who.eop.gov>; Levinson, Katie <Katie_Levinson@who.eop.gov>; Kavanaugh, Brett M. <Brett_M._Kavanaugh@who.eop.gov>; 'Steve.Bradbury@usdoj.gov' <Steve.Bradbury@usdoj.gov>; Mitnick, John M. <John_M._Mitnick@who.eop.gov>
Sent: Sat Jan 07 09:22:22 2006
Subject: RE: (b) (5) Talkers.doc

Dan was thinking (b) (5).

-----Original Message-----
From: Perino, Dana M.
Sent: Saturday, January 07, 2006 8:59 AM

duplicate



Harriet_Miers@who.eop.gov

From:	Harriet_Miers@who.eop.gov
Sent:	Saturday, January 07, 2006 12:40 PM
To:	Bradbury, Steve; Katie_Levinson@who.eop.gov; Michael_Allen@nsc.eop.gov; Dana_M._Perino@who.eop.gov; Brett_M._Kavanaugh@who.eop.gov; John_M._Mitnick@who.eop.gov
Cc:	Debbie_S._Fiddelke@who.eop.gov; Matthew_Kirk@who.eop.gov
Subject:	RE: (b) (5) Talkers.doc

Yes, I am in favor (b) (5) .

-----Original Message-----
From: Levinson, Katie
Sent: Saturday, January 07, 2006 12:39 PM
To: Allen, Michael; Miers, Harriet; Perino, Dana M.; Kavanaugh, Brett M.; 'Steve.Bradbury@usdoj.gov'; Mitnick, John M.
Cc: Fiddelke, Debbie S.; Kirk, Matthew
Subject: Re: (b) (5) Talkers.doc

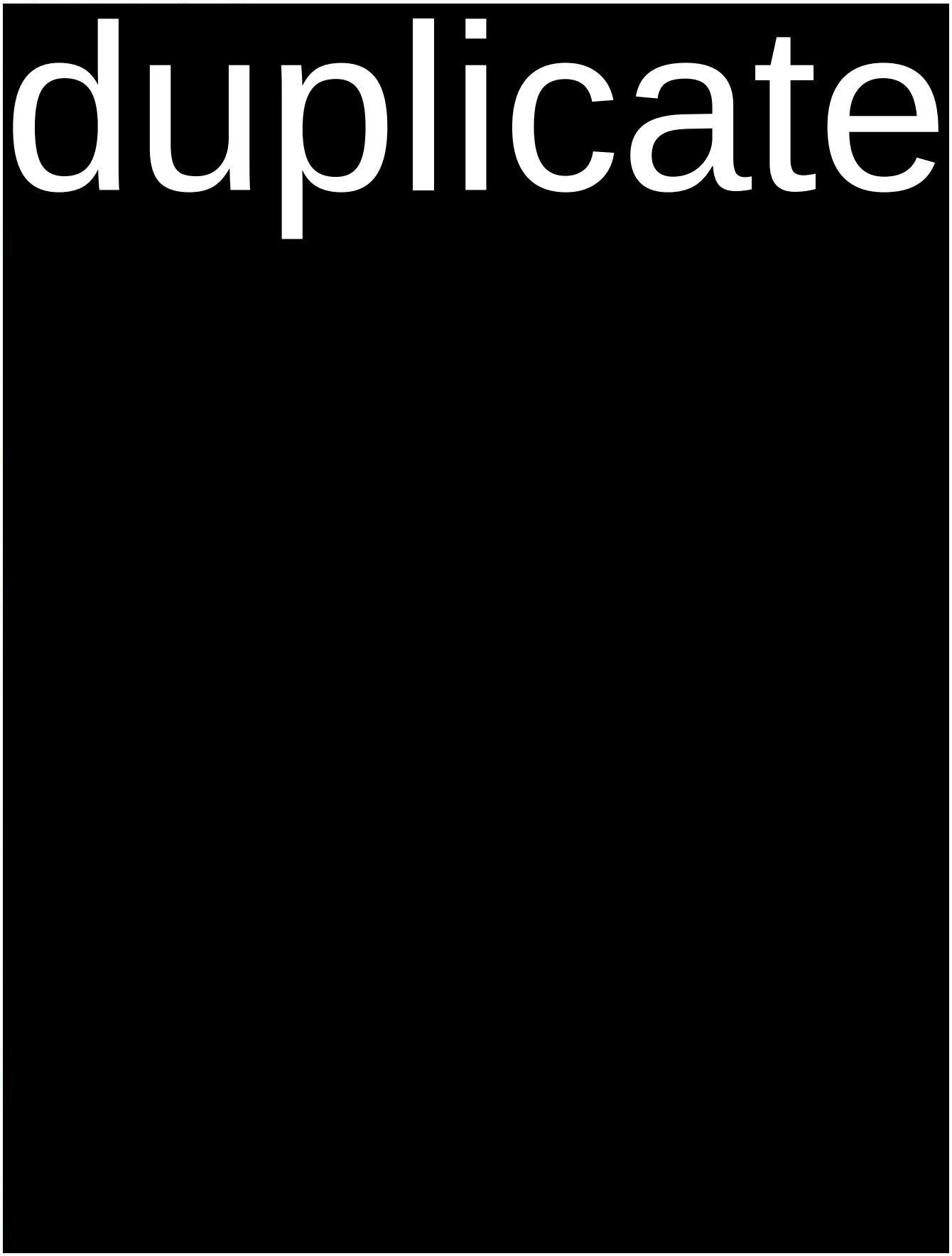
Dan's rec is yes, but he defers to Harriet.

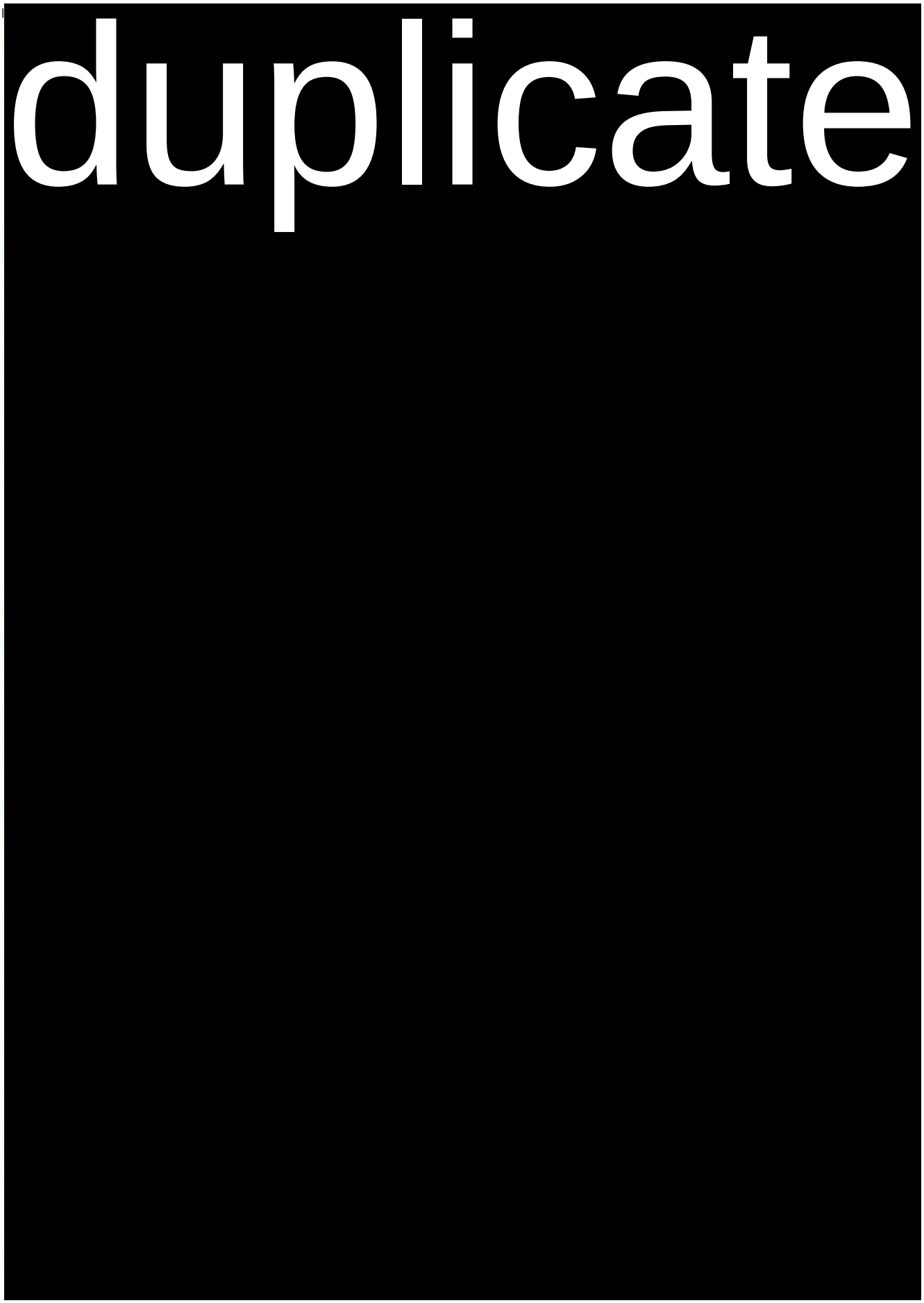
-----Original Message-----
From: Allen, Michael <Michael_Allen@nsc.eop.gov>
To: Levinson, Katie <Katie_Levinson@who.eop.gov>; Miers, Harriet <Harriet_Miers@who.eop.gov>; Perino, Dana M. <Dana_M._Perino@who.eop.gov>; Kavanaugh, Brett M. <Brett_M._Kavanaugh@who.eop.gov>; 'Steve.Bradbury@usdoj.gov' <Steve.Bradbury@usdoj.gov>; Mitnick, John M. <John_M._Mitnick@who.eop.gov>
CC: Fiddelke, Debbie S. <Debbie_S._Fiddelke@who.eop.gov>; Kirk, Matthew <Matthew_Kirk@who.eop.gov>
Sent: Sat Jan 07 12:27:04 2006
Subject: Re: (b) (5) Talkers.doc

(b) (5)
?

-----Original Message-----
From: Levinson, Katie <Katie_Levinson@who.eop.gov>
To: Miers, Harriet <Harriet_Miers@who.eop.gov>; Perino, Dana M. <Dana_M._Perino@who.eop.gov>; Kavanaugh, Brett M. <Brett_M._Kavanaugh@who.eop.gov>; 'Steve.Bradbury@usdoj.gov' <Steve.Bradbury@usdoj.gov>; Mitnick, John M. <John_M._Mitnick@who.eop.gov>

CC: Allen, Michael <Michael_Allen@nsc.eop.gov>; Fiddelke, Debbie S. <Debbie_S._Fiddelke@who.eop.gov>
Sent: Sat Jan 07 10:36:15 2006





duplicate

Harriet_Miers@who.eop.gov

From: Harriet_Miers@who.eop.gov
Sent: Saturday, January 07, 2006 12:41 PM
To: Bradbury, Steve; Matthew_Kirk@who.eop.gov; Katie_Levinson@who.eop.gov; Michael_Allen@nsc.eop.gov; Dana_M._Perino@who.eop.gov; Brett_M._Kavanaugh@who.eop.gov; John_M._Mitnick@who.eop.gov
Cc: Debbie_S._Fiddelke@who.eop.gov
Subject: RE: (b) (5) Talkers.doc

And I defer to others as to the best way but I would make sure the info gets to him.

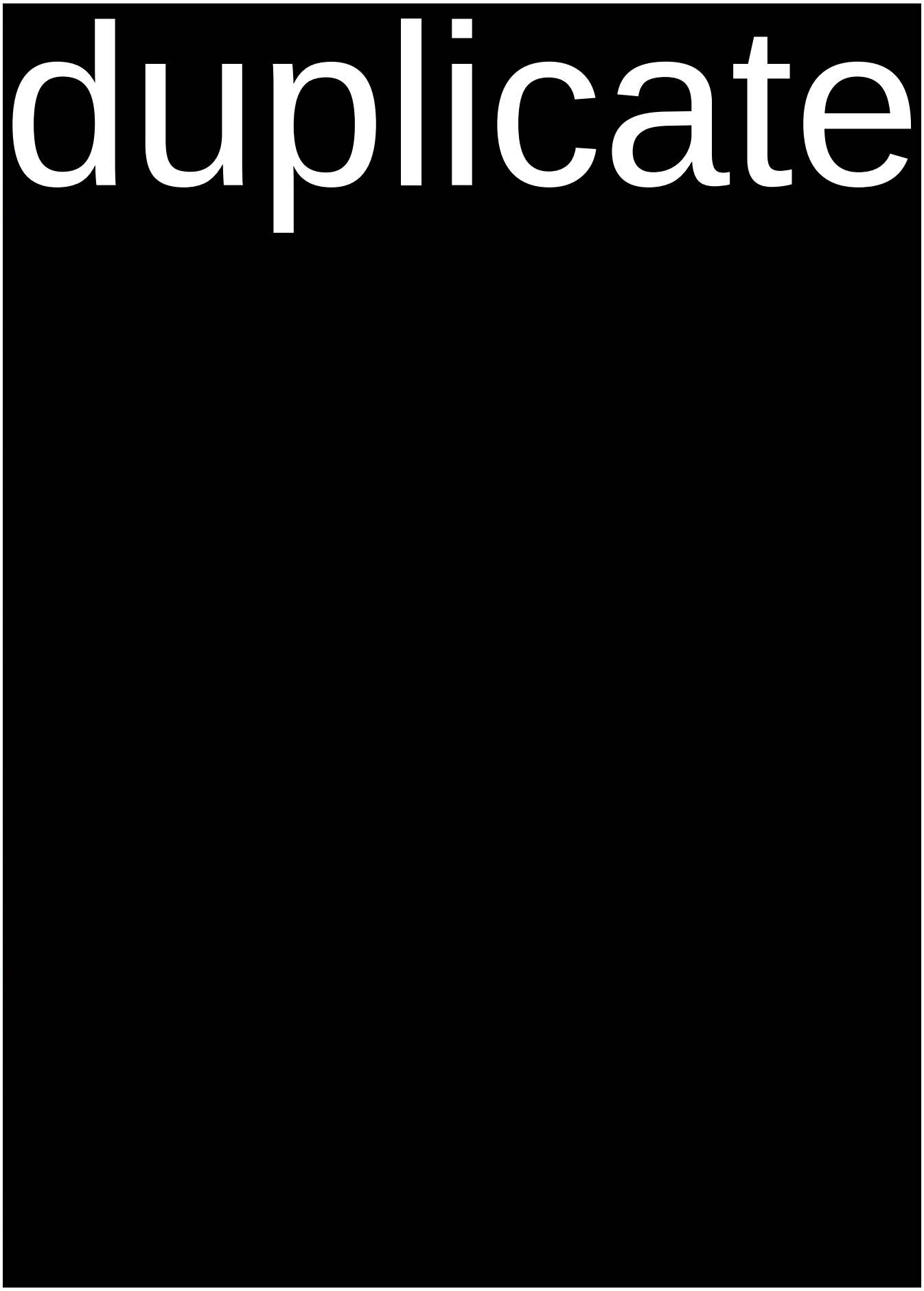
-----Original Message-----
From: Kirk, Matthew
Sent: Saturday, January 07, 2006 12:40 PM
To: Levinson, Katie; Allen, Michael; Miers, Harriet; Perino, Dana M.; Kavanaugh, Brett M.; 'Steve.Bradbury@usdoj.gov'; Mitnick, John M.
Cc: Fiddelke, Debbie S.
Subject: RE: (b) (5) Talkers.doc

I am happy to (b) (5) ,

Matt

-----Original Message-----
From: Levinson, Katie
Sent: Saturday, January 07, 2006 12:39 PM

duplicate



duplicate


duplicate

Bradbury, Steve

From: Bradbury, Steve
Sent: Tuesday, January 10, 2006 5:39 PM
To: 'Harriet_Miers@who.eop.gov'; William_K._Kelley@who.eop.gov; David_S._Addington@ovp.eop.gov; 'John_M._Mitnick@who.eop.gov'; 'John_B._Wiegmann@nsc.eop.gov'
Cc: 'Brett_M._Kavanaugh@who.eop.gov'; 'Brett_C._Gerry@who.eop.gov'
Subject: White Paper re NSA activities
Attachments: Surveillance Authorities_1_10 (1).doc

Attached is a current, revised draft of our white paper addressing more fully the legal basis for the NSA activities described by the President. We would like to finalize this white paper by the beginning of next week. Your comments are welcome.

Bradbury, Steve

From: Bradbury, Steve
Sent: Thursday, January 12, 2006 5:22 PM
To: 'Harriet_Miers@who.eop.gov'; David_S._Addington@ovp.eop.gov; William_K._Kelley@who.eop.gov; 'John_M._Mitnick@who.eop.gov'; 'John_B._Wiegmann@nsc.eop.gov'
Cc: 'Brett_C._Gerry@who.eop.gov'; 'Brett_M._Kavanaugh@who.eop.gov'
Subject: Draft white paper re NSA activities described by the President
Attachments: Surveillance Authorities_1_12_pm.doc

Attached is the current, revised draft of the white paper addressing the legal authorities supporting the NSA activities described by the President. Our intent is to finalize this paper by 1/16 for possible distribution by the AG early next week. Your comments are most welcome. Thx.

Gorsuch, Neil M

From:	Gorsuch, Neil M
Sent:	Monday, January 16, 2006 11:58 AM
To:	'Brett_C._Gerry@who.eop.gov'; Moschella, William; Scolinos, Tasia; McCallum, Robert (SMO); Sampson, Kyle; Roehrkasse, Brian; Harriet_Miers@who.eop.gov
Cc:	Elwood, John; David_S._Addington@ovp.eop.gov; Brett_M._Kavanaugh@who.eop.gov
Subject:	RE: USA Today update

(b) (5)

-----Original Message-----
From: Brett_C._Gerry@who.eop.gov [mailto:Brett_C._Gerry@who.eop.gov]
Sent: Monday, January 16, 2006 11:50 AM
To: Moschella, William; Scolinos, Tasia; McCallum, Robert (SMO); Gorsuch, Neil M; Sampson, Kyle; Roehrkasse, Brian; Harriet_Miers@who.eop.gov
Cc: Elwood, John; David_S._Addington@ovp.eop.gov; Brett_M._Kavanaugh@who.eop.gov
Subject: Re: USA Today update

(b) (5)

-----Original Message-----
From: Miers, Harriet <Harriet_Miers@who.eop.gov>
To: 'Neil.Gorsuch@usdoj.gov' <Neil.Gorsuch@usdoj.gov>; Robert.McCallum@usdoj.gov <Robert.McCallum@usdoj.gov>; Kyle.Sampson@usdoj.gov <Kyle.Sampson@usdoj.gov>; William.Moschella@usdoj.gov <William.Moschella@usdoj.gov>; Tasia.Scolinos@usdoj.gov <Tasia.Scolinos@usdoj.gov>; Brian.Roehrkasse@usdoj.gov <Brian.Roehrkasse@usdoj.gov>
CC: John.Elwood@usdoj.gov <John.Elwood@usdoj.gov>; Addington, David S. <David_S._Addington@ovp.eop.gov>; Gerry, Brett C. <Brett_C._Gerry@who.eop.gov>; Kavanaugh, Brett M. <Brett_M._Kavanaugh@who.eop.gov>
Sent: Mon Jan 16 11:30:43 2006
Subject: RE: USA Today update

I hate to add to the work here, but I asked Steve Hadley to review the draft and his doing so reminded me why we have staffing requirements. He had three comments that we need to consider, and through his comments pointed out the need for general staffing. So I am copying Brett Kavanaugh to make sure

he is aware of the development of this op ed. Steve's three thoughts were:

1. (b) (5) [redacted]

2. (b) (5) [redacted] I think Brett G and Brett K and I assume others have the specifics on this analysis.

3. (b) (5) [redacted]

-----Original Message-----
From: Neil.Gorsuch@usdoj.gov [mailto:Neil.Gorsuch@usdoj.gov]
Sent: Monday, January 16, 2006 11:08 AM
To: Neil.Gorsuch@usdoj.gov; Robert.McCallum@usdoj.gov; Kyle.Sampson@usdoj.gov; William.Moschella@usdoj.gov; Tasia.Scolinos@usdoj.gov; Brian.Roehrkasse@usdoj.gov
Cc: John.Elwood@usdoj.gov; Addington, David S.; Miers, Harriet; Gerry, Brett C.
Subject: RE: USA Today update

Brett Gerry had an excellent suggestion for the penultimate paragraph that both strengthens its message and reduces words (by 4). The suggested revision is attached for your consideration.

-----Original Message-----
From: Gorsuch, Neil M
Sent: Monday, January 16, 2006 10:27 AM
To: McCallum, Robert (SMO); Sampson, Kyle; Moschella, William; Scolinos, Tasia; Roehrkasse, Brian
Cc: 'Harriet_Miers@who.eop.gov'; 'Brett_C._Gerry@who.eop.gov'; 'David_S._Addington@ovp.eop.gov'; Elwood, John
Subject: RE: USA Today update

I must say that it's mighty tough to find any fat in John's excellent work. I have managed in the attached to eke some to get a (b) (5) version down to 377 words and pass it along for the group's consideration. It also seeks to incorporate Harriet's suggestions.
(Getting a (b) (5) version to 350 should be very easy, but it would be nice if we could (b) (5) [redacted]). NMG

-----Original Message-----
From: McCallum, Robert (SMO)
Sent: Monday, January 16, 2006 8:57 AM
To: Gorsuch, Neil M; Sampson, Kyle; Moschella, William; Scolinos, Tasia; Roehrkasse, Brian
Cc: 'Harriet_Miers@who.eop.gov'; 'Brett_C._Gerry@who.eop.gov'; 'David_S._Addington@ovp.eop.gov'; Elwood, John
Subject: FW: USA Today update

Copying Neil, Kyle, Tasia, Brian and Will with these edits. Robt.

-----Original Message-----
From: Harriet_Miers@who.eop.gov [mailto:Harriet_Miers@who.eop.gov]
Sent: Monday, January 16, 2006 7:38 AM
To: McCallum, Robert (SMO); Elwood, John
Cc: David_S._Addington@ovp.eop.gov; Brett_C._Gerry@who.eop.gov
Subject: RE: USA Today update

I have three general comments to the drafts which are very good. First, (b) (5) . I also think there should be (b) (5) . Finally, (b) (5)

-----Original Message-----
From: Robert.McCallum@usdoj.gov [mailto:Robert.McCallum@usdoj.gov]
Sent: Sunday, January 15, 2006 10:24 PM
To: John.Elwood@usdoj.gov; Neil.Gorsuch@usdoj.gov; Kyle.Sampson@usdoj.gov; Gerry, Brett C.; Addington, David S.; William.Moschella@usdoj.gov; Perino, Dana M.; Miers, Harriet
Cc: Tasia.Scolinos@usdoj.gov; Brian.Roehrkasse@usdoj.gov
Subject: RE: USA Today update

As per prior email to various folks, I will be in the office tomorrow am and can be reached by email, by direct dial at 514-7850, or through the DOJ command center. I will be reviewing the draft and be back in touch tomorrow am. Robt.

> -----Original Message-----
> From: Elwood, John
> Sent: Sunday, January 15, 2006 10:20 PM
> To: ' (Harriet_Miers@who.eop.gov)'; McCallum, Robert (SMO); Gorsuch,
> Neil M; Sampson, Kyle; 'Brett_C._Gerry@who.eop.gov';
> 'David_S._Addington@ovp.eop.gov'; 'Dana_M._Perino@who.eop.gov';
> Moschella, William
> Cc: Scolinos, Tasia; Roehrkasse, Brian
> Subject: USA Today update
>
> (b) (5)
I have gotten the (b) (5) version of the op-ed
> down to the current target (350 words).
>
> I've gotten the (b) (5) version of the op-ed down to 403 words.
> We're checking to see whether USA Today will extend the word count in
> view of the number and complexity of issues. If not, I'll find
> another 53 words that don't need to be said.
>
> I've attached copies of the (b) (5) op-eds to this
> e-mail. In case you're reading this on blackberry, I've cut and
> pasted the (b) (5) version into the body of the e-mail below. This

> incorporates all comments I've received so far.
>
> Thanks! << File: USA Today op-ed (v2.8) ((b) (5)).doc >> << File:
> USA Today op-ed (v2.8) ((b) (5)).doc >>
>
> DRAFT OP-ED==========
>

(b) (5)

(b) (5)

Scolinos, Tasia

From:	Scolinos, Tasia
Sent:	Monday, January 16, 2006 12:07 PM
To:	Gorsuch, Neil M; 'Harriet_Miers@who.eop.gov'; Moschella, William; McCallum, Robert (SMO); Sampson, Kyle; Roehrkasse, Brian
Cc:	Elwood, John; 'David_S._Addington@ovp.eop.gov'; 'Brett_C._Gerry@who.eop.gov'; 'Brett_M._Kavanaugh@who.eop.gov'
Subject:	Re: USA Today update

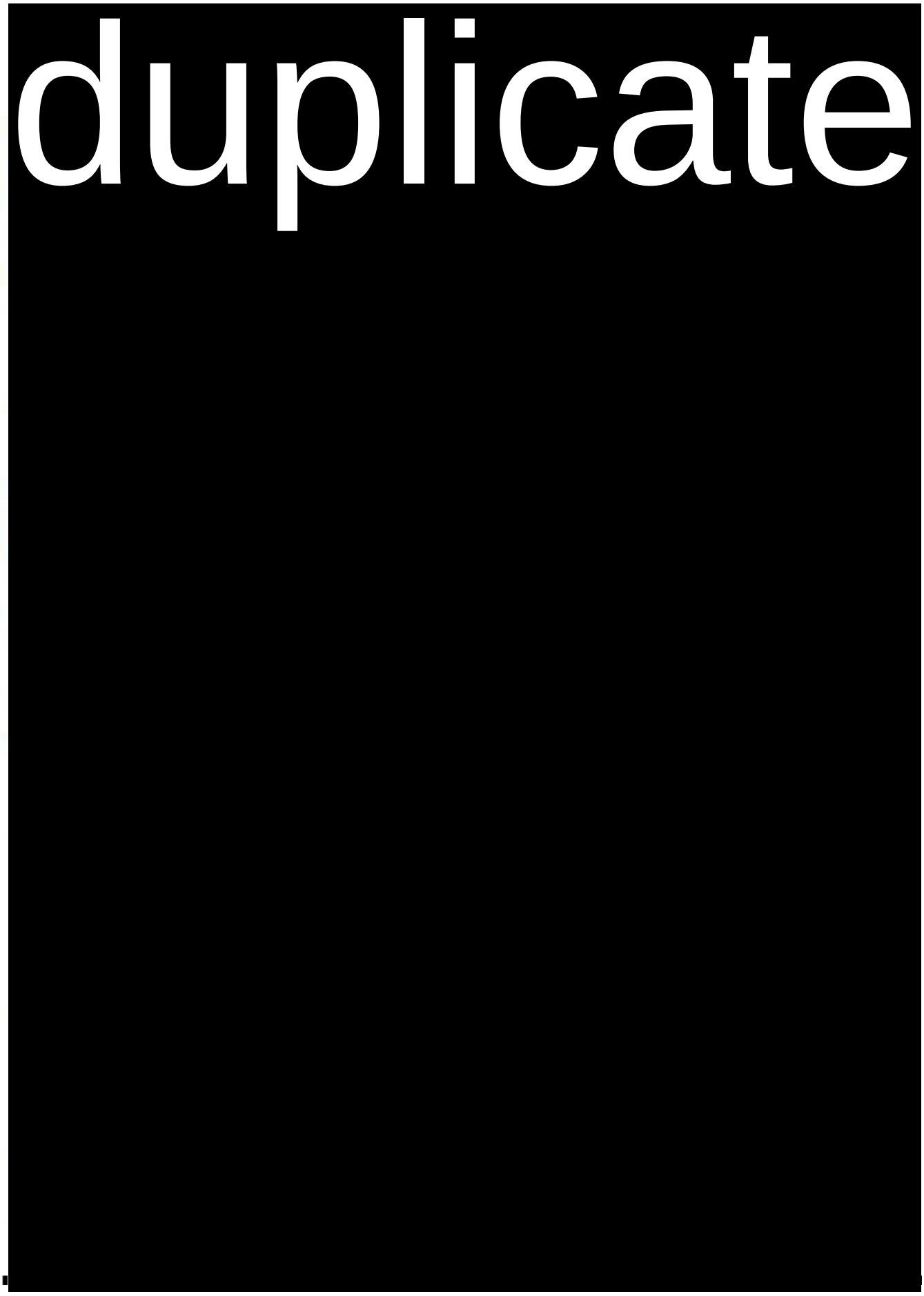
That is correct. We have directed reporters to them on this issue in the past and they are on the record with very strong statements supporting our interpretation.

Sent from my BlackBerry Wireless Handheld

-----Original Message-----
From: Gorsuch, Neil M <Neil.Gorsuch@SMOJMD.USDOJ.gov>
To: 'Harriet_Miers@who.eop.gov' <Harriet_Miers@who.eop.gov>; Moschella, William <William.Moschella@SMOJMD.USDOJ.gov>; Scolinos, Tasia <Tasia.Scolinos@SMOJMD.USDOJ.gov>; McCallum, Robert (SMO) <Robert.McCallum@SMOJMD.USDOJ.gov>; Sampson, Kyle <Kyle.Sampson@SMOJMD.USDOJ.gov>; Roehrkasse, Brian <Brian.Roehrkasse@SMOJMD.USDOJ.gov>
CC: Elwood, John <John.Elwood@SMOJMD.USDOJ.gov>; David_S._Addington@ovp.eop.gov <David_S._Addington@ovp.eop.gov>; Brett_C._Gerry@who.eop.gov <Brett_C._Gerry@who.eop.gov>; Brett_M._Kavanaugh@who.eop.gov <Brett_M._Kavanaugh@who.eop.gov>
Sent: Mon Jan 16 11:39:31 2006
Subject: RE: USA Today update

On #3, both Sen. Kyl and Graham are on record publicly stating that their legislation affects lawsuits "retroactively." Will and Tasia may be able to add more.

-----Original Message-----
From: Harriet_Miers@who.eop.gov [mailto:Harriet_Miers@who.eop.gov]
Sent: Monday, January 16, 2006 11:31 AM



duplicate

Roehrkasse, Brian

From: Roehrkasse, Brian
Sent: Monday, January 16, 2006 1:21 PM
To: Gorsuch, Neil M; McCallum, Robert (SMO); Elwood, John; Scolinos, Tasia; 'Brett_C._Gerry@who.eop.gov'; Moschella, William; 'Harriet_Miers@who.eop.gov'; 'David_S._Addington@ovp.eop.gov'; Sampson, Kyle; 'Brett_M._Kavanaugh@who.eop.gov'
Subject: Re: USA Today update

USA Today has decided to kill another element on their editorial page and will now grant us 430-440 words. This will also give us a little more time. Please circulate a final draft by no later 3:30.

Sent from my BlackBerry Wireless Handheld

-----Original Message-----
From: Gorsuch, Neil M <Neil.Gorsuch@SMOJMD.USDOJ.gov>
To: McCallum, Robert (SMO) <Robert.McCallum@SMOJMD.USDOJ.gov>; Elwood, John <John.Elwood@SMOJMD.USDOJ.gov>; Scolinos, Tasia <Tasia.Scolinos@SMOJMD.USDOJ.gov>; 'Brett_C._Gerry@who.eop.gov' <Brett_C._Gerry@who.eop.gov>; Roehrkasse, Brian <Brian.Roehrkasse@SMOJMD.USDOJ.gov>; Moschella, William <William.Moschella@SMOJMD.USDOJ.gov>; 'Harriet_Miers@who.eop.gov' <Harriet_Miers@who.eop.gov>; 'David_S._Addington@ovp.eop.gov' <David_S._Addington@ovp.eop.gov>; Sampson, Kyle <Kyle.Sampson@SMOJMD.USDOJ.gov>; 'Brett_M._Kavanaugh@who.eop.gov' <Brett_M._Kavanaugh@who.eop.gov>
Sent: Mon Jan 16 12:40:30 2006
Subject: RE: USA Today update

Will make sure these get in (not only do they clarify, they help reduce word count). John Elwood and Tasia Scolinos will pull the trigger here at DoJ after we get everyone's sign off at WH.

-----Original Message-----
From: McCallum, Robert (SMO)
Sent: Monday, January 16, 2006 12:34 PM
To: Gorsuch, Neil M; Elwood, John; Scolinos, Tasia; 'Brett_C._Gerry@who.eop.gov'; Roehrkasse, Brian; Moschella, William; 'Harriet_Miers@who.eop.gov'; 'David_S._Addington@ovp.eop.gov'; Sampson, Kyle; 'Brett_M._Kavanaugh@who.eop.gov'
Subject: RE: USA Today update

I like the revised draft. I have three suggested edits as follows:

[redacted] (b) (5) [redacted]

[redacted]

(b) (5)

Obviously, none are critical to my signing it. Who will pull the trigger on it in final? Robt.

-----Original Message-----
From: Gorsuch, Neil M
Sent: Monday, January 16, 2006 12:09 PM
To: Elwood, John; McCallum, Robert (SMO); Scolinos, Tasia; Brett_C._Gerry@who.eop.gov; Roehrkasse, Brian; McCallum, Robert (SMO); Moschella, William; Harriet_Miers@who.eop.gov; David_S._Addington@ovp.eop.gov; Sampson, Kyle; Brett_M._Kavanaugh@who.eop.gov
Subject: FW: USA Today update

At Brett and Harriet's suggestion, full version of a suggested draft, including Brett Gerry's great suggestion, follows in bb-friendly format below. It is 379 words. Per Brian R. of our press office, USA Today informs that it will "work with us" on words beyond the 350 limit it previously set, but the paper indicates that the sooner it has the document the more likely it will be able to work with us as other articles will come in later. Brian R. recommends getting a final to him by 2-ish. NMG

===

(b) (5)

[redacted] (b) (5)

-----Original Message-----
From: McCallum, Robert (SMO)
Sent: Monday, January 16, 2006 10:43 AM
To: Gorsuch, Neil M
Subject: RE: USA Today update

I thought yours was better than mine although great minds obviously think alike. [redacted] (b) (5)
Robt.

-----Original Message-----
From: Gorsuch, Neil M
Sent: Monday, January 16, 2006 10:41 AM
To: McCallum, Robert (SMO)
Subject: RE: USA Today update

Sorry, didn't see this before sending my draft! [redacted] (b) (5)

-----Original Message-----
From: McCallum, Robert (SMO)
Sent: Monday, January 16, 2006 10:24 AM
To: Scolinos, Tasia; Elwood, John; 'Harriet_Miers@who.eop.gov'
Cc: 'Brett_C._Gerry@who.eop.gov'; 'David_S._Addington@ovp.eop.gov'; Gorsuch, Neil M; Sampson, Kyle; Moschella, William; Roehrkasse, Brian
Subject: RE: USA Today update

Gentlepersons: I have made various edits below for your consideration, trying to incorporate Harriet's comments, cut some words, etc. [redacted] (b) (5)
No pride of authorship precludes rejection of these edits, other suggestions, etc. I am in the office for the day and can be reached by phone or email. Robt.

[redacted] (b) (5)

[redacted]

(b) (5)

[redacted]

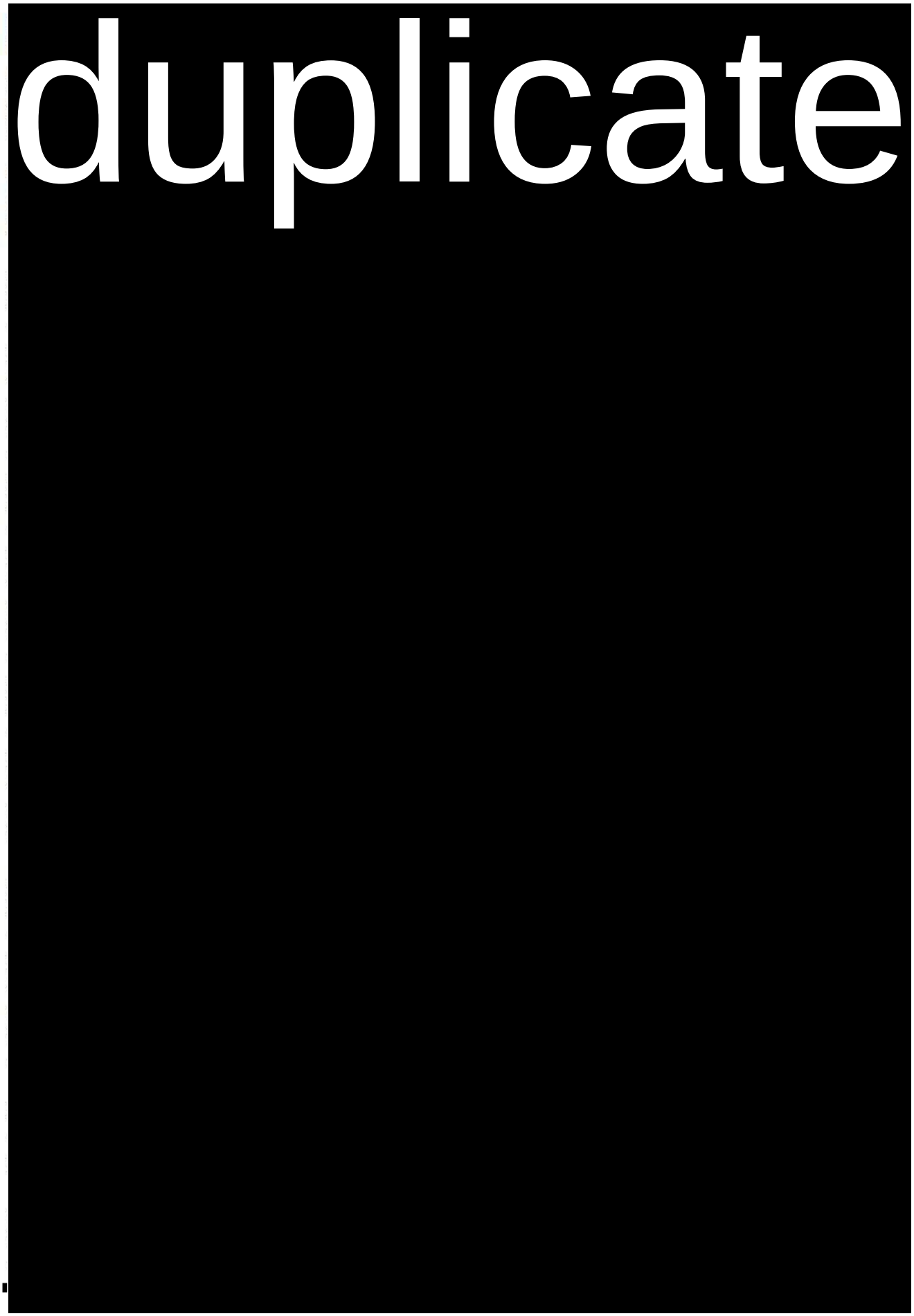
[redacted]

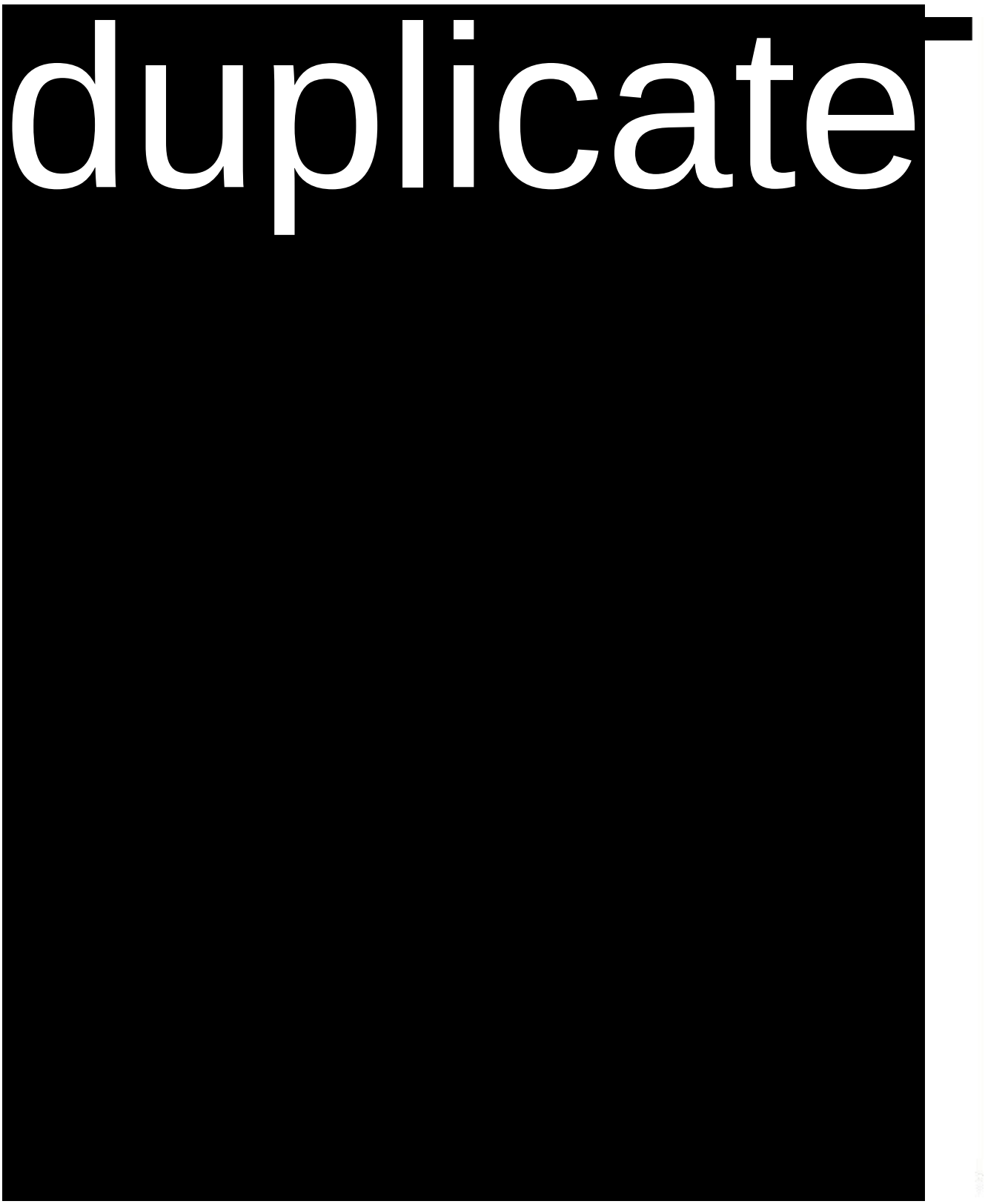
[redacted]

-----Original Message-----
From: McCallum, Robert (SMO)
Sent: Monday, January 16, 2006 8:57 AM

[redacted]

duplicate





McCallum, Robert (SMO)

From: McCallum, Robert (SMO)
Sent: Monday, January 16, 2006 2:06 PM
To: Gorsuch, Neil M; 'Brett_M._Kavanaugh@who.eop.gov'; 'Harriet_Miers@who.eop.gov'; 'Brett_C._Gerry@who.eop.gov'; Sampson, Kyle; Elwood, Courtney; Scolinos, Tasia; Roehrkasse, Brian; Moschella, William
Cc: Elwood, John
Subject: RE: LATEST version of USA Today

I like it and have no additional edits. Great work. Robt.

From: Gorsuch, Neil M
Sent: Monday, January 16, 2006 2:01 PM
To: 'Brett_M._Kavanaugh@who.eop.gov'; 'Harriet_Miers@who.eop.gov'; 'Brett_C._Gerry@who.eop.gov'; Sampson, Kyle; Elwood, Courtney; McCallum, Robert (SMO); Scolinos, Tasia; Roehrkasse, Brian; Moschella, William
Cc: Elwood, John
Subject: LATEST version of USA Today

Given that we now have 430 words to work with, John Elwood and I have sought to restore a few choice passages from earlier drafts you've seen (eg (b) (5)) without creating anything substantively "new." This version is at 429 words and is both attached and printed below for bb. Please let us know if there are any final changes as soon as possible. We need to get this to Brian by 3:30.

<< File: USA Today op-ed ((b) (5)) NMG 2.doc >>
==

(b) (5)

(b) (5)

Elwood, John

From: Elwood, John
Sent: Monday, January 16, 2006 3:56 PM
To: 'Brett_M._Kavanaugh@who.eop.gov'; Gorsuch, Neil M
Subject: RE: cutting 10 words ...

Not yet.

-----Original Message-----
From: Brett_M._Kavanaugh@who.eop.gov [mailto:Brett_M._Kavanaugh@who.eop.gov]
Sent: Monday, January 16, 2006 3:53 PM
To: Gorsuch, Neil M; Elwood, John
Subject: RE: cutting 10 words ...

Have you heard from her?

-----Original Message-----
From: Neil.Gorsuch@usdoj.gov [mailto:Neil.Gorsuch@usdoj.gov]
Sent: Monday, January 16, 2006 3:34 PM
To: John.Elwood@usdoj.gov; Kavanaugh, Brett M.
Subject: Re: cutting 10 words ...

Thanks, Brett.

-----Original Message-----
From: Brett_M._Kavanaugh@who.eop.gov <Brett_M._Kavanaugh@who.eop.gov>
To: Gorsuch, Neil M <Neil.Gorsuch@SMOJMD.USDOJ.gov>; Elwood, John
<John.Elwood@SMOJMD.USDOJ.gov>
Sent: Mon Jan 16 15:29:53 2006
Subject: RE: cutting 10 words ...

Checking now with HM.

-----Original Message-----
From: John.Elwood@usdoj.gov [mailto:John.Elwood@usdoj.gov]
Sent: Monday, January 16, 2006 3:16 PM
To: Neil.Gorsuch@usdoj.gov; Kavanaugh, Brett M.
Subject: RE: cutting 10 words ...

Brett:

We're supposed to get this to DOJ's Office of Public Affairs by 3:30.
Let me know if you or Harriet have any final comments. Thank you.

-----Original Message-----

-----Original Message-----
From: Brett_M._Kavanaugh@who.eop.gov
[mailto:Brett_M._Kavanaugh@who.eop.gov]
Sent: Monday, January 16, 2006 2:43 PM
To: Gorsuch, Neil M
Cc: Scolinos, Tasia; Elwood, John
Subject: RE: cutting 10 words ...

Waiting to get final word from Harriet. Thanks.

-----Original Message-----
From: Neil.Gorsuch@usdoj.gov [mailto:Neil.Gorsuch@usdoj.gov]
Sent: Monday, January 16, 2006 2:13 PM
To: Kavanaugh, Brett M.
Cc: John.Elwood@usdoj.gov; Tasia.Scolinos@usdoj.gov
Subject: RE: cutting 10 words ...

Brett, With Robert's ok we are (hopefully) finished on this end. We will wait to hear from you, however, before giving Tasia's shop the all clear. Thanks! NMG

Gorsuch, Neil M

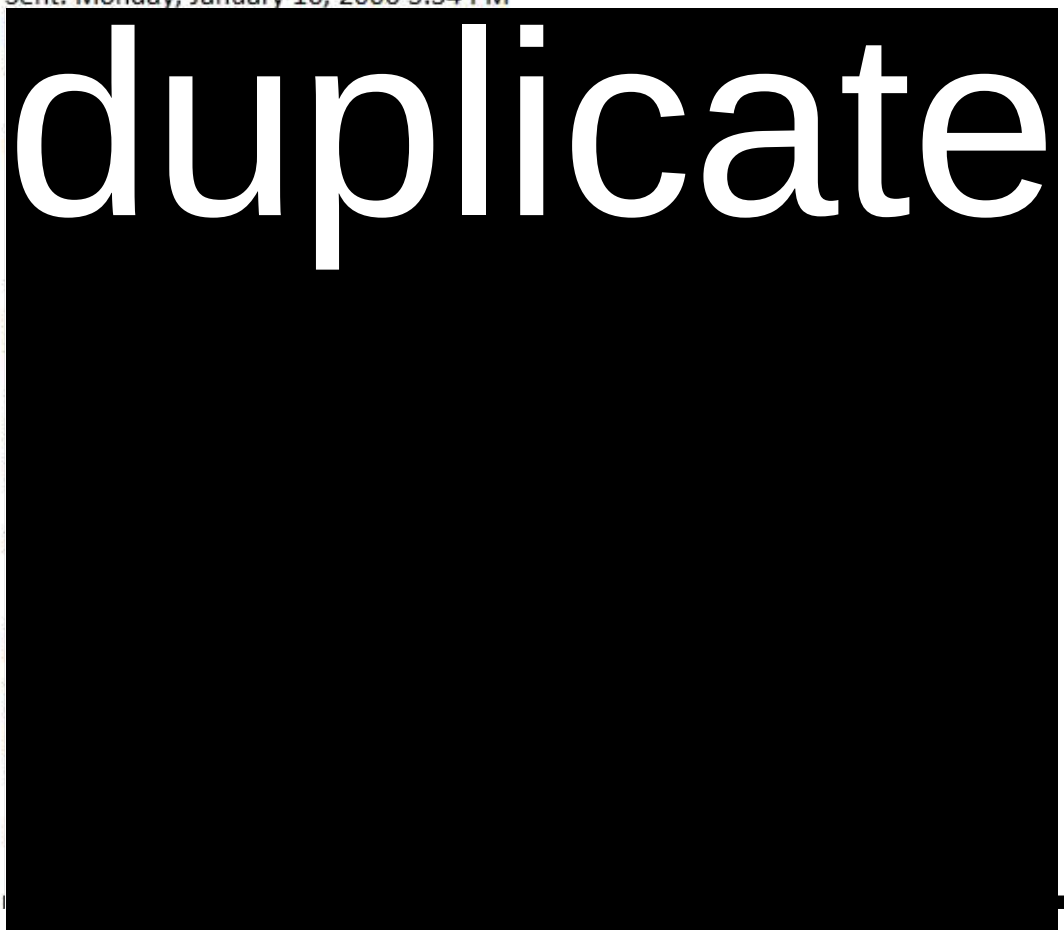
From: Gorsuch, Neil M
Sent: Monday, January 16, 2006 3:57 PM
To: 'Brett_M._Kavanaugh@who.eop.gov'; Elwood, John
Subject: Re: cutting 10 words ...

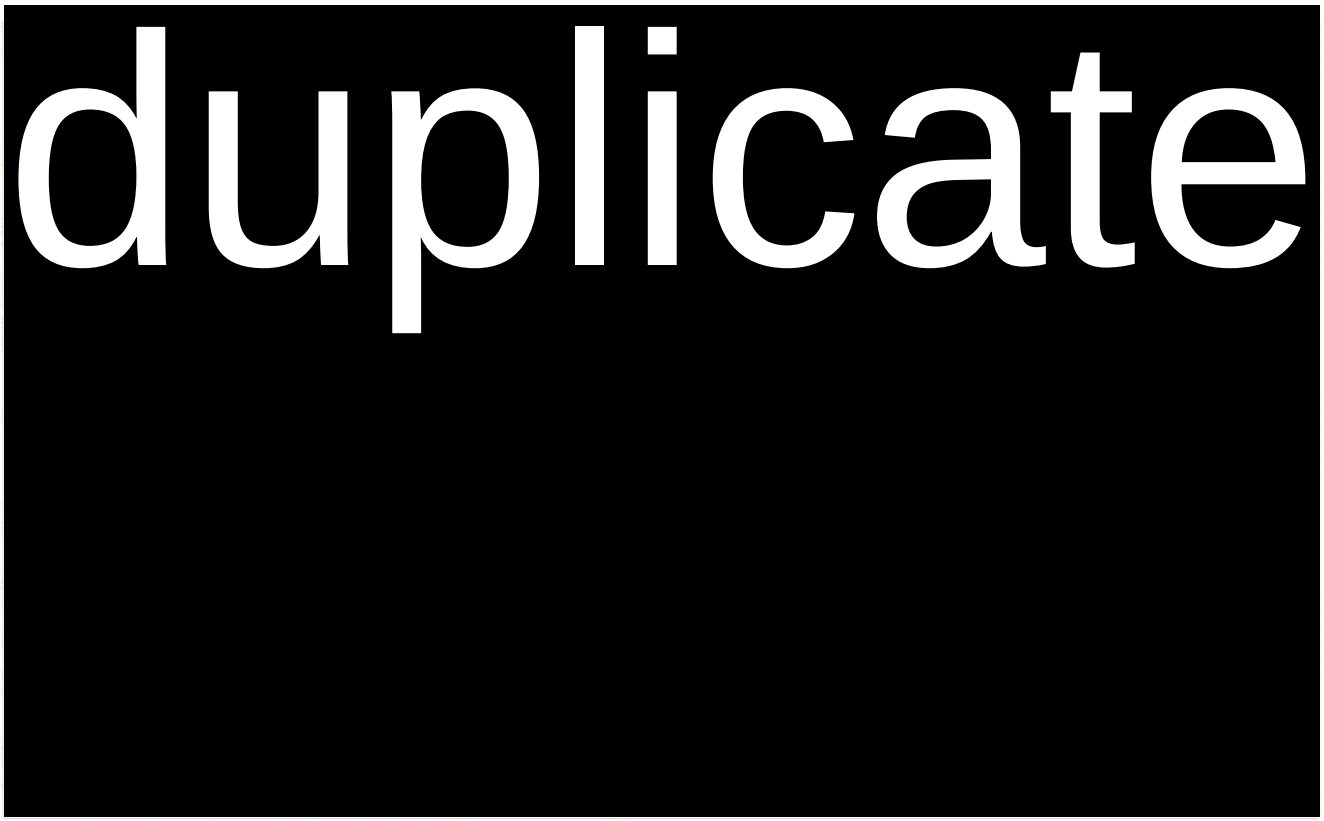
Thanks for helping push this across the finish line.

-----Original Message-----
From: Brett_M._Kavanaugh@who.eop.gov <Brett_M._Kavanaugh@who.eop.gov>
To: Gorsuch, Neil M <Neil.Gorsuch@SMOJMD.USDOJ.gov>; Elwood, John <John.Elwood@SMOJMD.USDOJ.gov>
Sent: Mon Jan 16 15:54:14 2006
Subject: RE: cutting 10 words ...

Good to go per Harriet.

-----Original Message-----
From: Neil.Gorsuch@usdoj.gov [mailto:Neil.Gorsuch@usdoj.gov]
Sent: Monday, January 16, 2006 3:34 PM





Elwood, John

From: Elwood, John
Sent: Monday, January 16, 2006 4:01 PM
To: 'Brett_M._Kavanaugh@who.eop.gov'; Gorsuch, Neil M
Subject: RE: cutting 10 words ...

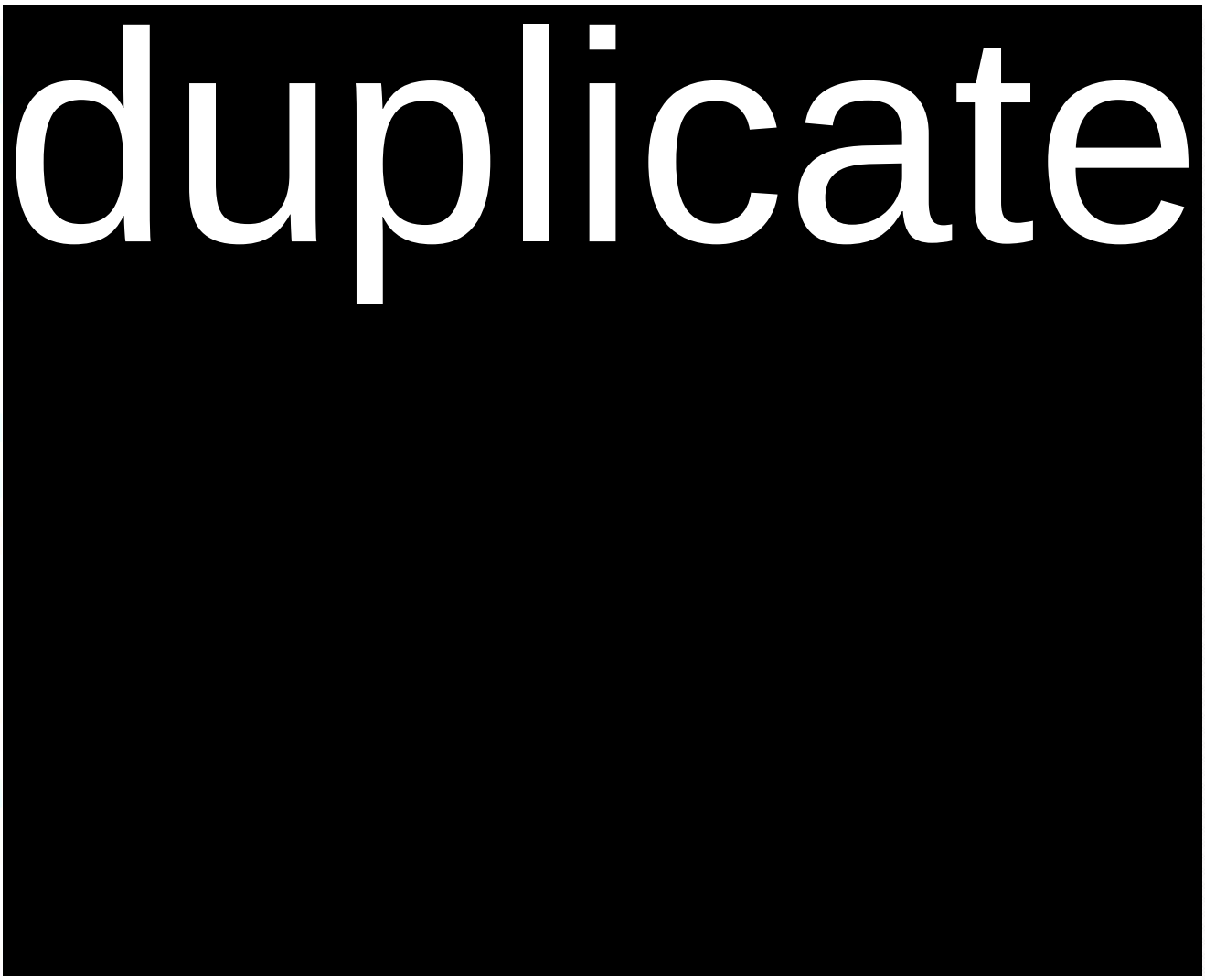
Will do.

-----Original Message-----
From: Brett_M._Kavanaugh@who.eop.gov [mailto:Brett_M._Kavanaugh@who.eop.gov]
Sent: Monday, January 16, 2006 3:58 PM
To: Gorsuch, Neil M; Elwood, John; Brett_M._Kavanaugh@who.eop.gov
Subject: RE: cutting 10 words ...

Got one more comment that [redacted] (b) (5) [redacted] Up to you.

-----Original Message-----
From: Kavanaugh, Brett M.
Sent: Monday, January 16, 2006 3:54 PM

[redacted]
duplicate
[redacted]



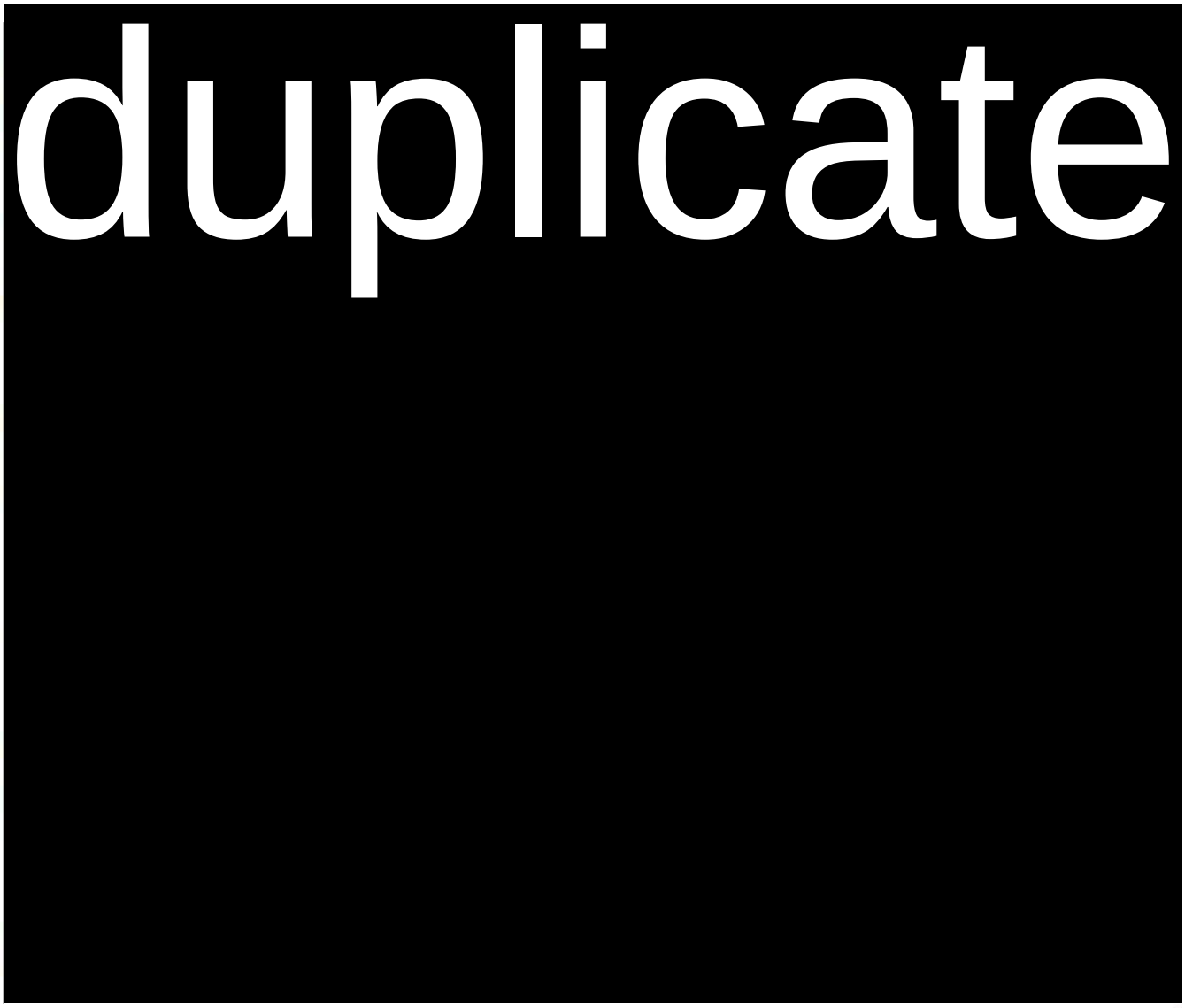
Elwood, John

From: Elwood, John
Sent: Monday, January 16, 2006 4:03 PM
To: 'Brett_M._Kavanaugh@who.eop.gov'; Gorsuch, Neil M
Subject: RE: cutting 10 words ...

Good catch. (b) (5)
.

-----Original Message-----
From: Brett_M._Kavanaugh@who.eop.gov [mailto:Brett_M._Kavanaugh@who.eop.gov]
Sent: Monday, January 16, 2006 3:58 PM

duplicate



Bradbury, Steve

From: Bradbury, Steve
Sent: Thursday, January 19, 2006 12:17 PM
To: 'benjamin.powell@dni.gov'; 'BellingerJB@state.gov'; 'hayneswj (b) (6) '; Dan_Bartlett@who.eop.gov; 'Harriet_Miers@who.eop.gov'; Raul_F._Yanes (b) (6) ; 'John_B._Wiegmann@nsc.eop.gov'; 'John_M._Mitnick@who.eop.gov' (b)(3) 50 USC § 3605 '; 'Brett_M._Kavanaugh@who.eop.gov'; 'Brett_C._Gerry@who.eop.gov'; William_K._Kelley@who.eop.gov
Cc: Sampson, Kyle; Scolinos, Tasia; Moschella, William; Roehrkasse, Brian
Subject: DOJ white paper on NSA activities
Attachments: White Paper on NSA Legal Authorities.pdf

Attached is an advance copy in PDF form of the DOJ white paper discussing the legal authorities for the NSA activities described by the President. The Attorney General will be sending this paper to Congress this afternoon and it will thereafter be publicly released.

U.S. Department of Justice

Washington, D.C. 20530

January 19, 2006

LEGAL AUTHORITIES SUPPORTING THE ACTIVITIES OF THE NATIONAL SECURITY AGENCY DESCRIBED BY THE PRESIDENT

As the President has explained, since shortly after the attacks of September 11, 2001, he has authorized the National Security Agency ("NSA") to intercept international communications into and out of the United States of persons linked to al Qaeda or related terrorist organizations. The purpose of these intercepts is to establish an early warning system to detect and prevent another catastrophic terrorist attack on the United States. This paper addresses, in an unclassified form, the legal basis for the NSA activities described by the President ("NSA activities").

SUMMARY

On September 11, 2001, the al Qaeda terrorist network launched the deadliest foreign attack on American soil in history. Al Qaeda's leadership repeatedly has pledged to attack the United States again at a time of its choosing, and these terrorist organizations continue to pose a grave threat to the United States. In response to the September 11th attacks and the continuing threat, the President, with broad congressional approval, has acted to protect the Nation from another terrorist attack. In the immediate aftermath of September 11th, the President promised that "[w]e will direct every resource at our command—every means of diplomacy, every tool of intelligence, every tool of law enforcement, every financial influence, and every weapon of war—to the destruction of and to the defeat of the global terrorist network." President Bush Address to a Joint Session of Congress (Sept. 20, 2001). The NSA activities are an indispensable aspect of this defense of the Nation. By targeting the international communications into and out of the United States of persons reasonably believed to be linked to al Qaeda, these activities provide the United States with an early warning system to help avert the next attack. For the following reasons, the NSA activities are lawful and consistent with civil liberties.

The NSA activities are supported by the President's well-recognized inherent constitutional authority as Commander in Chief and sole organ for the Nation in foreign affairs to conduct warrantless surveillance of enemy forces for intelligence purposes to detect and disrupt armed attacks on the United States. The President has the chief responsibility under the Constitution to protect America from attack, and the Constitution gives the President the authority necessary to fulfill that solemn responsibility. The President has made clear that he will exercise all authority available to him, consistent with the Constitution, to protect the people of the United States.

In the specific context of the current armed conflict with al Qaeda and related terrorist organizations, Congress by statute has confirmed and supplemented the President's recognized authority under Article II of the Constitution to conduct such warrantless surveillance to prevent further catastrophic attacks on the homeland. In its first legislative response to the terrorist attacks of September 11th, Congress authorized the President to "use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks" of September 11th in order to prevent "any future acts of international terrorism against the United States." Authorization for Use of Military Force, Pub. L. No. 107-40, § 2(a), 115 Stat. 224, 224 (Sept. 18, 2001) (reported as a note to 50 U.S.C.A. § 1541) ("AUMF"). History conclusively demonstrates that warrantless communications intelligence targeted at the enemy in time of armed conflict is a traditional and fundamental incident of the use of military force authorized by the AUMF. The Supreme Court's interpretation of the AUMF in *Hamdi v. Rumsfeld*, 542 U.S. 507 (2004), confirms that Congress in the AUMF gave its express approval to the military conflict against al Qaeda and its allies and thereby to the President's use of all traditional and accepted incidents of force in this current military conflict—including warrantless electronic surveillance to intercept enemy communications both at home and abroad. This understanding of the AUMF demonstrates Congress's support for the President's authority to protect the Nation and, at the same time, adheres to Justice O'Connor's admonition that "a state of war is not a blank check for the President," *Hamdi*, 542 U.S. at 536 (plurality opinion), particularly in view of the narrow scope of the NSA activities.

The AUMF places the President at the zenith of his powers in authorizing the NSA activities. Under the tripartite framework set forth by Justice Jackson in *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 635-38 (1952) (Jackson, J., concurring), Presidential authority is analyzed to determine whether the President is acting in accordance with congressional authorization (category I), whether he acts in the absence of a grant or denial of authority by Congress (category II), or whether he uses his own authority under the Constitution to take actions incompatible with congressional measures (category III). Because of the broad authorization provided in the AUMF, the President's action here falls within category I of Justice Jackson's framework. Accordingly, the President's power in authorizing the NSA activities is at its height because he acted "pursuant to an express or implied authorization of Congress," and his power "includes all that he possesses in his own right plus all that Congress can delegate." *Id*. at 635.

The NSA activities are consistent with the preexisting statutory framework generally applicable to the interception of communications in the United States—the Foreign Intelligence Surveillance Act ("FISA"), as amended, 50 U.S.C. §§ 1801-1862 (2000 & Supp. II 2002), and relevant related provisions in chapter 119 of title 18.[1] Although FISA generally requires judicial approval of electronic surveillance, FISA also contemplates that Congress may authorize such surveillance by a statute other than FISA. *See* 50 U.S.C. § 1809(a) (prohibiting any person from intentionally "engag[ing] . . . in electronic surveillance under color of law except as authorized

[1] Chapter 119 of title 18, which was enacted by Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended, 18 U.S.C. §§ 2510-2521 (2000 & West Supp. 2005), is often referred to as "Title III."

by statute"). The AUMF, as construed by the Supreme Court in *Hamdi* and as confirmed by the history and tradition of armed conflict, is just such a statute. Accordingly, electronic surveillance conducted by the President pursuant to the AUMF, including the NSA activities, is fully consistent with FISA and falls within category I of Justice Jackson's framework.

Even if there were ambiguity about whether FISA, read together with the AUMF, permits the President to authorize the NSA activities, the canon of constitutional avoidance requires reading these statutes in harmony to overcome any restrictions in FISA and Title III, at least as they might otherwise apply to the congressionally authorized armed conflict with al Qaeda. Indeed, were FISA and Title III interpreted to impede the President's ability to use the traditional tool of electronic surveillance to detect and prevent future attacks by a declared enemy that has already struck at the homeland and is engaged in ongoing operations against the United States, the constitutionality of FISA, as applied to that situation, would be called into very serious doubt. In fact, if this difficult constitutional question had to be addressed, FISA would be unconstitutional as applied to this narrow context. Importantly, the FISA Court of Review itself recognized just three years ago that the President retains constitutional authority to conduct foreign surveillance apart from the FISA framework, and the President is certainly entitled, at a minimum, to rely on that judicial interpretation of the Constitution and FISA.

Finally, the NSA activities fully comply with the requirements of the Fourth Amendment. The interception of communications described by the President falls within a well-established exception to the warrant requirement and satisfies the Fourth Amendment's fundamental requirement of reasonableness. The NSA activities are thus constitutionally permissible and fully protective of civil liberties.

BACKGROUND

A. THE ATTACKS OF SEPTEMBER 11, 2001

On September 11, 2001, the al Qaeda terrorist network launched a set of coordinated attacks along the East Coast of the United States. Four commercial jetliners, each carefully selected to be fully loaded with fuel for a transcontinental flight, were hijacked by al Qaeda operatives. Two of the jetliners were targeted at the Nation's financial center in New York and were deliberately flown into the Twin Towers of the World Trade Center. The third was targeted at the headquarters of the Nation's Armed Forces, the Pentagon. The fourth was apparently headed toward Washington, D.C., when passengers struggled with the hijackers and the plane crashed in Shanksville, Pennsylvania. The intended target of this fourth jetliner was evidently the White House or the Capitol, strongly suggesting that its intended mission was to strike a decapitation blow on the Government of the United States—to kill the President, the Vice President, or Members of Congress. The attacks of September 11th resulted in approximately 3,000 deaths—the highest single-day death toll from hostile foreign attacks in the Nation's history. These attacks shut down air travel in the United States, disrupted the Nation's financial markets and government operations, and caused billions of dollars in damage to the economy.

On September 14, 2001, the President declared a national emergency "by reason of the terrorist attacks at the World Trade Center, New York, New York, and the Pentagon, and the continuing and immediate threat of further attacks on the United States." Proclamation No. 7463, 66 Fed. Reg. 48,199 (Sept. 14, 2001). The same day, Congress passed a joint resolution authorizing the President "to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks" of September 11th, which the President signed on September 18th. AUMF § 2(a). Congress also expressly acknowledged that the attacks rendered it "necessary and appropriate" for the United States to exercise its right "to protect United States citizens both at home and abroad," and in particular recognized that "the President has authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States." *Id.* pmbl. Congress emphasized that the attacks "continue to pose an unusual and extraordinary threat to the national security and foreign policy of the United States." *Id.* The United States also launched a large-scale military response, both at home and abroad. In the United States, combat air patrols were immediately established over major metropolitan areas and were maintained 24 hours a day until April 2002. The United States also immediately began plans for a military response directed at al Qaeda's base of operations in Afghanistan. Acting under his constitutional authority as Commander in Chief, and with the support of Congress, the President dispatched forces to Afghanistan and, with the assistance of the Northern Alliance, toppled the Taliban regime.

As the President made explicit in his Military Order of November 13, 2001, authorizing the use of military commissions to try terrorists, the attacks of September 11th "created a state of armed conflict." Military Order § l(a), 66 Fed. Reg. 57,833 (Nov. 13, 2001). Indeed, shortly after the attacks, NATO—for the first time in its 46-year history—invoked article 5 of the North Atlantic Treaty, which provides that an "armed attack against one or more of [the parties] shall be considered an attack against them all." North Atlantic Treaty, Apr. 4, 1949, art. 5, 63 Stat. 2241, 2244, 34 U.N.T.S. 243, 246; *see also* Statement by NATO Secretary General Lord Robertson (Oct. 2, 2001), *available at* http://www.nato.int/docu/speech/2001/s011002a.htm ("[I]t has now been determined that the attack against the United States on 11 September was directed from abroad and shall therefore be regarded as an action covered by Article 5 of the Washington Treaty . . . ."). The President also determined in his Military Order that al Qaeda and related terrorists organizations "possess both the capability and the intention to undertake further terrorist attacks against the United States that, if not detected and prevented, will cause mass deaths, mass injuries, and massive destruction of property, and may place at risk the continuity of the operations of the United States Government," and concluded that "an extraordinary emergency exists for national defense purposes." Military Order, § l(c), (g), 66 Fed. Reg. at 57,833-34.

B. THE NSA ACTIVITIES

Against this unfolding background of events in the fall of 2001, there was substantial concern that al Qaeda and its allies were preparing to carry out another attack within the United States. Al Qaeda had demonstrated its ability to introduce agents into the United States undetected and to perpetrate devastating attacks, and it was suspected that additional agents were

likely already in position within the Nation's borders. As the President has explained, unlike a conventional enemy, al Qaeda has infiltrated "our cities and communities and communicated from here in America to plot and plan with bin Laden's lieutenants in Afghanistan, Pakistan and elsewhere." Press Conference of President Bush (Dec. 19, 2005), *available at* http://www.white-house.gov/news/releases/2005/12/20051219-2.html ("President's Press Conference"). To this day, finding al Qaeda sleeper agents in the United States remains one of the paramount concerns in the War on Terror. As the President has explained, "[t]he terrorists want to strike America again, and they hope to inflict even more damage than they did on September the 11th." *Id.*

The President has acknowledged that, to counter this threat, he has authorized the NSA to intercept international communications into and out of the United States of persons linked to al Qaeda or related terrorist organizations. The same day, the Attorney General elaborated and explained that in order to intercept a communication, there must be "a reasonable basis to conclude that one party to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda." Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence, *available at* http://www.whitehouse.gov/news/releases/2005/12/20051219-1.html (Dec. 19, 2005) (statement of Attorney General Gonzales). The purpose of these intercepts is to establish an early warning system to detect and prevent another catastrophic terrorist attack on the United States. The President has stated that the NSA activities "ha[ve] been effective in disrupting the enemy, while safeguarding our civil liberties." President's Press Conference.

The President has explained that the NSA activities are "critical" to the national security of the United States. *Id.* Confronting al Qaeda "is not simply a matter of [domestic] law enforcement"—we must defend the country against an enemy that declared war against the United States. *Id.* To "effectively detect enemies hiding in our midst and prevent them from striking us again . . . we must be able to act fast and to detect conversations [made by individuals linked to al Qaeda] so we can prevent new attacks." *Id.* The President pointed out that "a two-minute phone conversation between somebody linked to al Qaeda here and an operative overseas could lead directly to the loss of thousands of lives." *Id.* The NSA activities are intended to help "connect the dots" between potential terrorists. *Id.* In addition, the Nation is facing "a different era, a different war . . . people are changing phone numbers . . . and they're moving quick[ly]." *Id.* As the President explained, the NSA activities "enable[] us to move faster and quicker. And that's important. We've got to be fast on our feet, quick to detect and prevent." *Id.* "This is an enemy that is quick and it's lethal. And sometimes we have to move very, very quickly." *Id.* FISA, by contrast, is better suited "for long-term monitoring." *Id.*

As the President has explained, the NSA activities are "carefully reviewed approximately every 45 days to ensure that [they are] being used properly." *Id.* These activities are reviewed for legality by the Department of Justice and are monitored by the General Counsel and Inspector General of the NSA to ensure that civil liberties are being protected. *Id.* Leaders in Congress from both parties have been briefed more than a dozen times on the NSA activities.

C. THE CONTINUING THREAT POSED BY AL QAEDA

Before the September 11th attacks, al Qaeda had promised to attack the United States. In 1998, Osama bin Laden declared a "religious" war against the United States and urged that it was the moral obligation of all Muslims to kill U.S. civilians and military personnel. *See* Statement of Osama bin Laden, Ayman al-Zawahiri, et al., *Fatwah Urging Jihad Against Americans*, published in Al-Quds al-'Arabi (Feb. 23, 1998) ("To kill the Americans and their allies—civilians and military—is an individual duty for every Muslim who can do it in any country in which it is possible to do it, in order to liberate the al-Aqsa Mosque and the holy mosque from their grip, and in order for their armies to move out of all the lands of Islam, defeated and unable to threaten any Muslim."). Al Qaeda carried out those threats with a vengeance; they attacked the U.S.S. Cole in Yemen, the United States Embassy in Nairobi, and finally the United States itself in the September 11th attacks.

It is clear that al Qaeda is not content with the damage it wrought on September 11th. As recently as December 7, 2005, Ayman al-Zawahiri professed that al Qaeda "is spreading, growing, and becoming stronger," and that al Qaeda is "waging a great historic battle in Iraq, Afghanistan, Palestine, and even in the Crusaders' own homes." Ayman al-Zawahiri, videotape released on Al-Jazeera television network (Dec. 7, 2005). Indeed, since September 11th, al Qaeda leaders have repeatedly promised to deliver another, even more devastating attack on America. *See, e.g.*, Osama bin Laden, videotape released on Al-Jazeera television network (Oct. 24, 2004) (warning United States citizens of further attacks and asserting that "your security is in your own hands"); Osama bin Laden, videotape released on Al-Jazeera television network (Oct. 18, 2003) ("We, God willing, will continue to fight you and will continue martyrdom operations inside and outside the United States . . . ."); Ayman Al-Zawahiri, videotape released on the Al-Jazeera television network (Oct. 9, 2002) ("I promise you [addressing the 'citizens of the United States'] that the Islamic youth are preparing for you what will fill your hearts with horror"). Given that al Qaeda's leaders have repeatedly made good on their threats and that al Qaeda has demonstrated its ability to insert foreign agents into the United States to execute attacks, it is clear that the threat continues. Indeed, since September 11th, al Qaeda has staged several large-scale attacks around the world, including in Indonesia, Madrid, and London, killing hundreds of innocent people.

ANALYSIS

I. THE PRESIDENT HAS INHERENT CONSTITUTIONAL AUTHORITY TO ORDER WARRANTLESS FOREIGN INTELLIGENCE SURVEILLANCE

As Congress expressly recognized in the AUMF, "the President has authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States," AUMF pmbl., especially in the context of the current conflict. Article II of the Constitution vests in the President all executive power of the United States, including the power to act as Commander in Chief of the Armed Forces, *see* U.S. Const. art. II, § 2, and authority over the conduct of the Nation's foreign affairs. As the Supreme Court has explained, "[t]he President is the sole organ of the nation in its external relations, and its sole representative with

foreign nations." *United States v. Curtiss-Wright Export Corp.,* 299 U.S. 304, 319 (1936) (internal quotation marks and citations omitted). In this way, the Constitution grants the President inherent power to protect the Nation from foreign attack, *see, e.g.*, *The Prize Cases,* 67 U.S. (2 Black) 635, 668 (1863), and to protect national security information, *see, e.g.*, *Department of the Navy v. Egan,* 484 U.S. 518, 527 (1988).

To carry out these responsibilities, the President must have authority to gather information necessary for the execution of his office. The Founders, after all, intended the federal Government to be clothed with all authority necessary to protect the Nation. *See, e.g., The Federalist* No. 23, at 147 (Alexander Hamilton) (Jacob E. Cooke ed. 1961) (explaining that the federal Government will be "cloathed with all the powers requisite to the complete execution of its trust"); *id.* No. 41, at 269 (James Madison) ("Security against foreign danger is one of the primitive objects of civil society . . . . The powers requisite for attaining it must be effectually confided to the federal councils."). Because of the structural advantages of the Executive Branch, the Founders also intended that the President would have the primary responsibility and necessary authority as Commander in Chief and Chief Executive to protect the Nation and to conduct the Nation's foreign affairs. *See, e.g.*, *The Federalist* No. 70, at 471-72 (Alexander Hamilton); *see also Johnson v. Eisentrager,* 339 U.S. 763, 788 (1950) ("this [constitutional] grant of war power includes all that is necessary and proper for carrying these powers into execution") (citation omitted). Thus, it has been long recognized that the President has the authority to use secretive means to collect intelligence necessary for the conduct of foreign affairs and military campaigns. *See, e.g.*, *Chicago & S. Air Lines v. Waterman S.S. Corp.,* 333 U.S. 103, 111 (1948) ("The President, both as Commander-in-Chief and as the Nation's organ for foreign affairs, has available intelligence services whose reports are not and ought not to be published to the world."); *Curtiss-Wright,* 299 U.S. at 320 ("He has his confidential sources of information. He has his agents in the form of diplomatic, consular and other officials."); *Totten v. United States,* 92 U.S. 105, 106 (1876) (President "was undoubtedly authorized during the war, as commander-in-chief . . . to employ secret agents to enter the rebel lines and obtain information respecting the strength, resources, and movements of the enemy").

In reliance on these principles, a consistent understanding has developed that the President has inherent constitutional authority to conduct warrantless searches and surveillance within the United States for foreign intelligence purposes. Wiretaps for such purposes thus have been authorized by Presidents at least since the administration of Franklin Roosevelt in 1940. *See, e.g., United States v. United States District Court,* 444 F.2d 651, 669-71 (6th Cir. 1971) (reproducing as an appendix memoranda from Presidents Roosevelt, Truman, and Johnson). In a Memorandum to Attorney General Jackson, President Roosevelt wrote on May 21, 1940:

> You are, therefore, authorized and directed in such cases as you may approve, after investigation of the need in each case, to authorize the necessary investigation agents that they are at liberty to secure information by listening devices directed to the conversation or other communications of persons suspected of subversive activities against the Government of the United States, including suspected spies. You are requested furthermore to limit these investigations so conducted to a minimum and limit them insofar as

possible to aliens.

Id. at 670 (appendix A). President Truman approved a memorandum drafted by Attorney General Tom Clark in which the Attorney General advised that "it is as necessary as it was in 1940 to take the investigative measures" authorized by President Roosevelt to conduct electronic surveillance "in cases vitally affecting the domestic security." *Id*. Indeed, while FISA was being debated during the Carter Administration, Attorney General Griffin Bell testified that "the current bill recognizes no inherent power of the President to conduct electronic surveillance, and I want to interpolate here to say that *this does not take away the power [of] the President under the Constitution*." Foreign Intelligence Electronic Surveillance Act of 1978: Hearings on H.R. 5764, H.R. 9745, H.R. 7308, and H.R. 5632 Before the Subcomm. on Legislation of the House Comm. on Intelligence, 95th Cong., 2d Sess. 15 (1978) (emphasis added); *see also Katz v. United States*, 389 U.S. 347, 363 (1967) (White, J., concurring) ("Wiretapping to protect the security of the Nation has been authorized by successive Presidents."); *cf*. Amending the Foreign Intelligence Surveillance Act: Hearings Before the House Permanent Select Comm. on Intelligence,103d Cong. 2d Sess. 61 (1994) (statement of Deputy Attorney General Jamie S. Gorelick) ("[T]he Department of Justice believes, and the case law supports, that the President has inherent authority to conduct warrantless physical searches for foreign intelligence purposes . . . .").

The courts uniformly have approved this longstanding Executive Branch practice. Indeed, every federal appellate court to rule on the question has concluded that, even in peacetime, the President has inherent constitutional authority, consistent with the Fourth Amendment, to conduct searches for foreign intelligence purposes without securing a judicial warrant. *See In re Sealed Case,* 310 F.3d 717, 742 (Foreign Intel. Surv. Ct. of Rev. 2002) ("[A]ll the other courts to have decided the issue [have] held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information . . . . *We take for granted that the President does have that authority and, assuming that is so, FISA could not encroach on the President's constitutional power*.") (emphasis added); *accord, e.g., United States v. Truong Dinh Hung,* 629 F.2d 908 (4th Cir. 1980); *United States v. Butenko,* 494 F.2d 593 (3d Cir. 1974) (en banc); *United States v. Brown,* 484 F.2d 418 (5th Cir. 1973). *But cf. Zweibon v. Mitchell,* 516 F.2d 594 (D.C. Cir. 1975) (en banc) (dictum in plurality opinion suggesting that a warrant would be required even in a foreign intelligence investigation).

In *United States v. United States District Court,* 407 U.S. 297 (1972) (the "*Keith*" case), the Supreme Court concluded that the Fourth Amendment's warrant requirement applies to investigations of wholly *domestic* threats to security—such as domestic political violence and other crimes. But the Court in the *Keith* case made clear that it was not addressing the President's authority to conduct *foreign* intelligence surveillance without a warrant and that it was expressly reserving that question: "[T]he instant case requires no judgment on the scope of the President's surveillance power with respect to the activities of foreign powers, within or without this country." *Id.* at 308; *see also id.* at 321-22 & n.20 ("We have not addressed, and express no opinion as to, the issues which may be involved with respect to activities of foreign powers or their agents."). That *Keith* does not apply in the context of protecting against a foreign attack has been confirmed by the lower courts. After *Keith*, each of the three courts of appeals

that have squarely considered the question have concluded—expressly taking the Supreme Court's decision into account—that the President has inherent authority to conduct warrantless surveillance in the foreign intelligence context. *See, e.g.*, *Truong Dinh Hung,* 629 F.2d at 913-14; *Butenko*, 494 F.2d at 603; *Brown*, 484 F.2d 425-26.

From a constitutional standpoint, foreign intelligence surveillance such as the NSA activities differs fundamentally from the domestic security surveillance at issue in *Keith*. As the Fourth Circuit observed, the President has uniquely strong constitutional powers in matters pertaining to foreign affairs and national security. "Perhaps most crucially, the executive branch not only has superior expertise in the area of foreign intelligence, it is also constitutionally designated as the pre-eminent authority in foreign affairs." *Truong,* 629 F.2d at 914; *see id.* at 913 (noting that "the needs of the executive are so compelling in the area of foreign intelligence, unlike the area of domestic security, that a uniform warrant requirement would . . . unduly frustrate the President in carrying out his foreign affairs responsibilities"); *cf. Haig v. Agee,* 453 U.S. 280, 292 (1981) ("Matters intimately related to foreign policy and national security are rarely proper subjects for judicial intervention.").[2]

The present circumstances that support recognition of the President's inherent constitutional authority to conduct the NSA activities are considerably stronger than were the circumstances at issue in the earlier courts of appeals cases that recognized this power. All of the cases described above addressed inherent executive authority under the foreign affairs power to conduct surveillance in a peacetime context. The courts in these cases therefore had no occasion even to consider the fundamental authority of the President, as Commander in Chief, to gather intelligence in the context of an ongoing armed conflict in which the United States already had suffered massive civilian casualties and in which the intelligence gathering efforts at issue were specifically designed to thwart further armed attacks. Indeed, intelligence gathering is particularly important in the current conflict, in which the enemy attacks largely through clandestine activities and which, as Congress recognized, "pose[s] an unusual and extraordinary threat," AUMF pmbl.

Among the President's most basic constitutional duties is the duty to protect the Nation from armed attack. The Constitution gives him all necessary authority to fulfill that responsibility. The courts thus have long acknowledged the President's inherent authority to take action to protect Americans abroad, *see, e.g., Durand v. Hollins,* 8 F. Cas. 111, 112 (C.C.S.D.N.Y. 1860) (No. 4186), and to protect the Nation from attack, *see, e.g., The Prize Cases,* 67 U.S. at 668. *See generally Ex parte Quirin,* 317 U.S. 1, 28 (1942) (recognizing that

[2] *Keith* made clear that one of the significant concerns driving the Court's conclusion in the domestic security context was the inevitable connection between perceived threats to domestic security and political dissent. As the Court explained: "Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs. The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect 'domestic security.'" *Keith,* 407 U.S. at 314; *see also id.* at 320 ("Security surveillances are especially sensitive because of the inherent vagueness of the domestic security concept, the necessarily broad and continuing nature of intelligence gathering, and the temptation to utilize such surveillances to oversee political dissent."). Surveillance of domestic groups raises a First Amendment concern that generally is not present when the subjects of the surveillance are foreign powers or their agents.

the President has authority under the Constitution "to direct the performance of those functions which may constitutionally be performed by the military arm of the nation in time of war," including "important incident[s] to the conduct of war," such as "the adoption of measures by the military command . . . to repel and defeat the enemy"). As the Supreme Court emphasized in the *Prize Cases*, if the Nation is invaded, the President is "bound to resist force by force"; "[h]e must determine what degree of force the crisis demands" and need not await congressional sanction to do so. *The Prize Cases,* 67 U.S. at 670; *see also Campbell v. Clinton,* 203 F.3d 19, 27 (D.C. Cir. 2000) (Silberman, J., concurring) ("[T]he *Prize Cases* . . . stand for the proposition that the President has independent authority to repel aggressive acts by third parties even without specific congressional authorization, and courts may not review the level of force selected."); *id.* at 40 (Tatel, J., concurring) ("[T]he President, as commander in chief, possesses emergency authority to use military force to defend the nation from attack without obtaining prior congressional approval."). Indeed, "in virtue of his rank as head of the forces, [the President] has certain powers and duties with which Congress cannot interfere." *Training of British Flying Students in the United States,* 40 Op. Att'y Gen. 58, 61 (1941) (Attorney General Robert H. Jackson) (internal quotation marks omitted). In exercising his constitutional powers, the President has wide discretion, consistent with the Constitution, over the methods of gathering intelligence about the Nation's enemies in a time of armed conflict.

II. THE AUMF CONFIRMS AND SUPPLEMENTS THE PRESIDENT'S INHERENT POWER TO USE WARRANTLESS SURVEILLANCE AGAINST THE ENEMY IN THE CURRENT ARMED CONFLICT

In the Authorization for Use of Military Force enacted in the wake of September 11th, Congress confirms and supplements the President's constitutional authority to protect the Nation, including through electronic surveillance, in the context of the current post-September 11th armed conflict with al Qaeda and its allies. The broad language of the AUMF affords the President, at a minimum, discretion to employ the traditional incidents of the use of military force. The history of the President's use of warrantless surveillance during armed conflicts demonstrates that the NSA surveillance described by the President is a fundamental incident of the use of military force that is necessarily included in the AUMF.

A. THE TEXT AND PURPOSE OF THE AUMF AUTHORIZE THE NSA ACTIVITIES

On September 14, 2001, in its first legislative response to the attacks of September 11th, Congress gave its express approval to the President's military campaign against al Qaeda and, in the process, confirmed the well-accepted understanding of the President's Article II powers. *See* AUMF § 2(a).[3] In the preamble to the AUMF, Congress stated that "the President has authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States," AUMF pmbl., and thereby acknowledged the President's inherent constitutional authority to defend the United States. This clause "constitutes an extraordinarily

[3] America's military response began before the attacks of September 11th had been completed. *See The 9/11 Commission Report* 20 (2004). Combat air patrols were established and authorized "to engage inbound aircraft if they could verify that the aircraft was hijacked." *Id.* at 42.

sweeping recognition of independent presidential *constitutional* power to employ the war power to combat terrorism." Michael Stokes Paulsen, Youngstown *Goes to War,* 19 Const. Comment. 215, 252 (2002). This striking recognition of presidential authority cannot be discounted as the product of excitement in the immediate aftermath of September 11th, for the same terms were repeated by Congress more than a year later in the Authorization for Use of Military Force Against Iraq Resolution of 2002. Pub. L. No. 107-243, pmbl., 116 Stat. 1498, 1500 (Oct. 16, 2002) ("[T]he President has authority under the Constitution to take action in order to deter and prevent acts of international terrorism against the United States . . . ."). In the context of the conflict with al Qaeda and related terrorist organizations, therefore, Congress has acknowledged a broad executive authority to "deter and prevent" further attacks against the United States.

The AUMF passed by Congress on September 14, 2001, does not lend itself to a narrow reading. Its expansive language authorizes the President "to use *all necessary and appropriate force* against those nations, organizations, or persons *he determines* planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001." AUMF § 2(a) (emphases added). In the field of foreign affairs, and particularly that of war powers and national security, congressional enactments are to be broadly construed where they indicate support for authority long asserted and exercised by the Executive Branch. *See, e.g., Haig v. Agee*, 453 U.S. 280, 293-303 (1981); *United States ex rel. Knauff v. Shaughnessy*, 338 U.S. 537, 543-45 (1950); *cf. Loving v. United States,* 517 U.S. 748, 772 (1996) (noting that the usual "limitations on delegation [of congressional powers] do not apply" to authorizations linked to the Commander in Chief power); *Dames & Moore v. Regan*, 453 U.S. 654, 678-82 (1981) (even where there is no express statutory authorization for executive action, legislation in related field may be construed to indicate congressional acquiescence in that action). Although Congress's war powers under Article I, Section 8 of the Constitution empower Congress to legislate regarding the raising, regulation, and material support of the Armed Forces and related matters, rather than the prosecution of military campaigns, the AUMF indicates Congress's endorsement of the President's use of his constitutional war powers. This authorization transforms the struggle against al Qaeda and related terrorist organizations from what Justice Jackson called "a zone of twilight," in which the President and the Congress may have concurrent powers whose "distribution is uncertain," *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 637 (1952) (Jackson, J., concurring), into a situation in which the President's authority is at is maximum because "it includes all that he possesses in his own right plus all that Congress can delegate," *id.* at 635. With regard to these fundamental tools of warfare—and, as demonstrated below, warrantless electronic surveillance against the declared enemy is one such tool—the AUMF places the President's authority at its zenith under *Youngstown*.

It is also clear that the AUMF confirms and supports the President's use of those traditional incidents of military force against the enemy, wherever they may be—on United States soil or abroad. The nature of the September 11th attacks—launched on United States soil by foreign agents secreted in the United States—necessitates such authority, and the text of the AUMF confirms it. The operative terms of the AUMF state that the President is authorized to use force "in order to prevent any future acts of international terrorism against the United States," *id*., an objective which, given the recent attacks within the Nation's borders and the continuing use of air defense throughout the country at the time Congress acted, undoubtedly

contemplated the possibility of military action within the United States. The preamble, moreover, recites that the United States should exercise its rights "to protect United States citizens both *at home* and abroad." *Id*. pmbl. (emphasis added). To take action against those linked to the September 11th attacks involves taking action against individuals within the United States. The United States had been attacked on its own soil—not by aircraft launched from carriers several hundred miles away, but by enemy agents who had resided in the United States for months. A crucial responsibility of the President—charged by the AUMF and the Constitution—was and is to identify and attack those enemies, especially if they were in the United States, ready to strike against the Nation.

The text of the AUMF demonstrates in an additional way that Congress authorized the President to conduct warrantless electronic surveillance against the enemy. The terms of the AUMF not only authorized the President to "use all necessary and appropriate force" against those responsible for the September 11th attacks; it also authorized the President to "determine[]" the persons or groups responsible for those attacks and to take all actions necessary to prevent further attacks. AUMF § 2(a) ("the President is authorized to use all necessary and appropriate force against those nations, organizations, or persons *he determines* planned, authorized, committed, or aided the terrorist attacks that occurred on September 11th, 2001, or harbored such organizations or persons") (emphasis added). Of vital importance to the use of force against the enemy is locating the enemy and identifying its plans of attack. And of vital importance to identifying the enemy and detecting possible future plots was the authority to intercept communications to or from the United States of persons with links to al Qaeda or related terrorist organizations. Given that the agents who carried out the initial attacks resided in the United States and had successfully blended into American society and disguised their identities and intentions until they were ready to strike, the necessity of using the most effective intelligence gathering tools against such an enemy, including electronic surveillance, was patent. Indeed, Congress recognized that the enemy in this conflict poses an "unusual and extraordinary threat." AUMF pmbl.

The Supreme Court's interpretation of the scope of the AUMF in *Hamdi v. Rumsfeld*, 542 U.S. 507 (2004), strongly supports this reading of the AUMF. In *Hamdi*, five members of the Court found that the AUMF authorized the detention of an American within the United States, notwithstanding a statute that prohibits the detention of U.S. citizens "except pursuant to an Act of Congress," 18 U.S.C. § 4001(a). *See Hamdi*, 542 U.S. at 519 (plurality opinion); *id*. at 587 (Thomas, J., dissenting). Drawing on historical materials and "longstanding law-of-war principles," *id*. at 518-21, a plurality of the Court concluded that detention of combatants who fought against the United States as part of an organization "known to have supported" al Qaeda "is so fundamental and accepted an incident to war as to be an exercise of the 'necessary and appropriate force' Congress has authorized the President to use." *Id*. at 518; *see also id*. at 587 (Thomas, J., dissenting) (agreeing with the plurality that the joint resolution authorized the President to "detain those arrayed against our troops"); *accord Quirin*, 317 U.S. at 26-29, 38 (recognizing the President's authority to capture and try agents of the enemy in the United States even if they had never "entered the theatre or zone of active military operations"). Thus, even though the AUMF does not say anything expressly about detention, the Court nevertheless found that it satisfied section 4001(a)'s requirement that detention be congressionally authorized.

The conclusion of five Justices in *Hamdi* that the AUMF incorporates fundamental "incidents" of the use of military force makes clear that the absence of any specific reference to signals intelligence activities in the resolution is immaterial. *See Hamdi,* 542 U.S. at 519 ("[I]t is of no moment that the AUMF does not use specific language of detention.") (plurality opinion). Indeed, given the circumstances in which the AUMF was adopted, it is hardly surprising that Congress chose to speak about the President's authority in general terms. The purpose of the AUMF was for Congress to sanction and support the military response to the devastating terrorist attacks that had occurred just three days earlier. Congress evidently thought it neither necessary nor appropriate to attempt to catalog every specific aspect of the use of the forces it was authorizing and every potential preexisting statutory limitation on the Executive Branch. Rather than engage in that difficult and impractical exercise, Congress authorized the President, in general but intentionally broad terms, to use the traditional and fundamental incidents of war and to determine how best to identify and engage the enemy in the current armed conflict. Congress's judgment to proceed in this manner was unassailable, for, as the Supreme Court has recognized, even in normal times involving no major national security crisis, "Congress cannot anticipate and legislate with regard to every possible action the President may find it necessary to take." *Dames & Moore*, 453 U.S. at 678. Indeed, Congress often has enacted authorizations to use military force using general authorizing language that does not purport to catalogue in detail the specific powers the President may employ. The need for Congress to speak broadly in recognizing and augmenting the President's core constitutional powers over foreign affairs and military campaigns is of course significantly heightened in times of national emergency. *See Zemel v. Rusk,* 381 U.S. 1, 17 (1965) ("[B]ecause of the changeable and explosive nature of contemporary international relations . . . Congress—in giving the Executive authority over matters of foreign affairs—must of necessity paint with a brush broader than that it customarily wields in domestic areas.").

Hamdi thus establishes the proposition that the AUMF "clearly and unmistakably" authorizes the President to take actions against al Qaeda and related organizations that amount to "fundamental incident[s] of waging war." *Hamdi*, 542 U.S. at 519 (plurality opinion); *see also id*. at 587 (Thomas, J., dissenting). In other words, "*[t]he clear inference is that the AUMF authorizes what the laws of war permit*." Curtis A. Bradley & Jack L. Goldsmith, *Congressional Authorization and the War on Terrorism*, 118 Harv. L. Rev. 2048, 2092 (2005) (emphasis added). Congress is presumed to be aware of the Supreme Court's precedents. Indeed, Congress recently enacted legislation in response to the Court's decision in *Rasul v. Bush*, 542 U.S. 466 (2004)—which was issued the same day as the *Hamdi* decision—removing habeas corpus jurisdiction over claims filed on behalf of confined enemy combatants held at Guantanamo Bay. Congress, however, has not expressed any disapproval of the Supreme Court's commonsense and plain-meaning interpretation of the AUMF in *Hamdi*.[4]

[4] This understanding of the AUMF is consistent with Justice O'Connor's admonition that "a state of war is not a blank check for the President," *Hamdi*, 542 U.S. at 536 (plurality opinion). In addition to constituting a fundamental and accepted incident of the use of military force, the NSA activities are consistent with the law of armed conflict principle that the use of force be necessary and proportional. *See* Dieter Fleck, *The Handbook of Humanitarian Law in Armed Conflicts* 115 (1995). The NSA activities are proportional because they are minimally invasive and narrow in scope, targeting only the international communications of persons reasonably believed to be linked to al Qaeda, and are designed to protect the Nation from a devastating attack.

B. WARRANTLESS ELECTRONIC SURVEILLANCE AIMED AT INTERCEPTING ENEMY COMMUNICATIONS HAS LONG BEEN RECOGNIZED AS A FUNDAMENTAL INCIDENT OF THE USE OF MILITARY FORCE

The history of warfare—including the consistent practice of Presidents since the earliest days of the Republic—demonstrates that warrantless intelligence surveillance against the enemy is a fundamental incident of the use of military force, and this history confirms the statutory authority provided by the AUMF. Electronic surveillance is a fundamental tool of war that must be included in any natural reading of the AUMF's authorization to use "all necessary and appropriate force."

As one author has explained:

> It is *essential* in warfare for a belligerent to be as fully informed as possible about the enemy—his strength, his weaknesses, measures taken by him and measures contemplated by him. This applies not only to military matters, but . . . anything which bears on and is material to his ability to wage the war in which he is engaged. *The laws of war recognize and sanction this aspect of warfare.*

Morris Greenspan, *The Modern Law of Land Warfare* 325 (1959) (emphases added); *see also* Memorandum for Members of the House Permanent Select Comm. on Intel., from Jeffrey H. Smith, *Re: Legal Authorities Regarding Warrantless Surveillance of U.S. Persons* 6 (Jan. 3, 2006) ("Certainly, the collection of intelligence is understood to be necessary to the execution of the war."). Similarly, article 24 of the Hague Regulations of 1907 expressly states that "the employment of measures necessary for obtaining information about the enemy and the country [is] considered permissible." *See also* L. Oppenheim, *International Law* vol. II § 159 (7th ed. 1952) ("War cannot be waged without all kinds of information, about the forces and the intentions of the enemy . . . . To obtain the necessary information, it has always been considered lawful to employ spies . . . ."); Joseph R. Baker & Henry G. Crocker, *The Laws of Land Warfare* 197 (1919) ("Every belligerent has a right . . . to discover the signals of the enemy and . . . to seek to procure information regarding the enemy through the aid of secret agents."); *cf.* J.M. Spaight, *War Rights on Land* 205 (1911) ("[E]very nation employs spies; were a nation so quixotic as to refrain from doing so, it might as well sheathe its sword for ever. . . . Spies . . . are indispensably necessary to a general; and, other things being equal, that commander will be victorious who has the best secret service.") (internal quotation marks omitted).

In accordance with these well-established principles, the Supreme Court has consistently recognized the President's authority to conduct intelligence activities. *See, e.g., Totten v. United States,* 92 U.S. 105, 106 (1876) (recognizing President's authority to hire spies); *Tenet v. Doe*, 544 U.S. 1 (2005) (reaffirming *Totten* and counseling against judicial interference with such matters); *see also Chicago & S. Air Lines v. Waterman S.S. Corp.,* 333 U.S. 103, 111 (1948) ("The President, both as Commander-in-Chief and as the Nation's organ for foreign affairs, has available intelligence services whose reports neither are not and ought not to be published to the world."); *United States v. Curtiss-Wright Export Corp.,* 299 U.S. 304, 320 (1936) (The President "has his confidential sources of information. He has his agents in the form of diplomatic,

consular, and other officials."). Chief Justice John Marshall even described the gathering of intelligence as a military duty. *See Tatum v. Laird,* 444 F.2d 947, 952-53 (D.C. Cir. 1971) ("As Chief Justice John Marshall said of Washington, 'A general must be governed by his intelligence and must regulate his measures by his information. It is his duty to obtain correct information . . . . '") (quoting Foreword, U.S. Army Basic Field Manual, Vol. X, circa 1938), *rev'd on other grounds*, 408 U.S. 1 (1972).

The United States, furthermore, has a long history of wartime surveillance—a history that can be traced to George Washington, who "was a master of military espionage" and "made frequent and effective use of secret intelligence in the second half of the eighteenth century." Rhodri Jeffreys-Jones, *Cloak and Dollar: A History of American Secret Intelligence* 11 (2002); *see generally id*. at 11-23 (recounting Washington's use of intelligence); *see also Haig v. Agee*, 471 U.S. 159, 172 n.16 (1981) (quoting General Washington's letter to an agent embarking upon an intelligence mission in 1777: "The necessity of procuring good intelligence, is apparent and need not be further urged."). As President in 1790, Washington obtained from Congress a "secret fund" to deal with foreign dangers and to be spent at his discretion. Jeffreys-Jones, *supra*, at 22. The fund, which remained in use until the creation of the Central Intelligence Agency in the mid-twentieth century and gained "longstanding acceptance within our constitutional structure," *Halperin v. CIA,* 629 F.2d 144, 158-59 (D.C. Cir. 1980), was used "for all purposes to which a secret service fund should or could be applied for the public benefit," including "for persons sent publicly and secretly to search for important information, political or commercial," *id.* at 159 (quoting Statement of Senator John Forsyth, Cong. Debates 295 (Feb. 25, 1831)). *See also Totten,* 92 U.S. at 107 (refusing to examine payments from this fund lest the publicity make a "secret service" "impossible").

The interception of communications, in particular, has long been accepted as a fundamental method for conducting wartime surveillance. *See, e.g.*, Greenspan, *supra*, at 326 (accepted and customary means for gathering intelligence "include air reconnaissance and photography; ground reconnaissance; observation of enemy positions; *interception of enemy messages, wireless and other*; examination of captured documents; . . . and interrogation of prisoners and civilian inhabitants") (emphasis added). Indeed, since its independence, the United States has intercepted communications for wartime intelligence purposes and, if necessary, has done so within its own borders. During the Revolutionary War, for example, George Washington received and used to his advantage reports from American intelligence agents on British military strength, British strategic intentions, and British estimates of American strength. *See* Jeffreys-Jones, *supra*, at 13. One source of Washington's intelligence was intercepted British mail. *See* Central Intelligence Agency, *Intelligence in the War of Independence* 31, 32 (1997). In fact, Washington himself proposed that one of his Generals "contrive a means of opening [British letters] without breaking the seals, take copies of the contents, and then let them go on." *Id.* at 32 ("From that point on, Washington was privy to British intelligence pouches between New York and Canada."); *see generally* Final Report of the Select Committee to Study Governmental Operations with respect to Intelligence Activities (the "Church Committee"), S. Rep. No. 94-755, at Book VI, 9-17 (Apr. 23, 1976) (describing Washington's intelligence activities).

More specifically, warrantless electronic surveillance of wartime communications has been conducted in the United States since electronic communications have existed, *i.e.,* since at least the Civil War, when "[t]elegraph wiretapping was common, and an important intelligence source for both sides." G.J.A. O'Toole, *The Encyclopedia of American Intelligence and Espionage* 498 (1988). Confederate General J.E.B. Stuart even "had his own personal wiretapper travel along with him in the field" to intercept military telegraphic communications. Samuel Dash, et al., *The Eavesdroppers* 23 (1971); *see also* O'Toole, *supra*, at 121, 385-88, 496-98 (discussing Civil War surveillance methods such as wiretaps, reconnaissance balloons, semaphore interception, and cryptanalysis). Similarly, there was extensive use of electronic surveillance during the Spanish-American War. *See* Bruce W. Bidwell, *History of the Military Intelligence Division, Department of the Army General Staff:* 1775-1941, at 62 (1986). When an American expeditionary force crossed into northern Mexico to confront the forces of Pancho Villa in 1916, the Army "frequently intercepted messages of the regime in Mexico City or the forces contesting its rule." David Alvarez, *Secret Messages* 6-7 (2000). Shortly after Congress declared war on Germany in World War I, President Wilson (citing only his constitutional powers and the joint resolution declaring war) ordered the censorship of messages sent outside the United States via submarine cables, telegraph, and telephone lines. *See* Exec. Order No. 2604 (Apr. 28, 1917). During that war, wireless telegraphy "enabled each belligerent to tap the messages of the enemy." Bidwell, *supra*, at 165 (quoting statement of Col. W. Nicolai, former head of the Secret Service of the High Command of the German Army, *in* W. Nicolai, *The German Secret Service* 21 (1924)).

As noted in Part I, on May 21, 1940, President Roosevelt authorized warrantless electronic surveillance of persons suspected of subversive activities, including spying, against the United States. In addition, on December 8, 1941, the day after the attack on Pearl Harbor, President Roosevelt gave the Director of the FBI "temporary powers to direct all news censorship and to *control all other telecommunications traffic* in and out of the United States." Jack A. Gottschalk, *"Consistent with Security". . . . A History of American Military Press Censorship,* 5 Comm. & L. 35, 39 (1983) (emphasis added). *See* Memorandum for the Secretaries of War, Navy, State, and Treasury, the Postmaster General, and the Federal Communications Commission from Franklin D. Roosevelt (Dec. 8, 1941). President Roosevelt soon supplanted that temporary regime by establishing an office for conducting such electronic surveillance in accordance with the War Powers Act of 1941. *See* Pub. L. No. 77-354, § 303, 55 Stat. 838, 840-41 (Dec. 18, 1941); Gottschalk, 5 Comm. & L. at 40. The President's order gave the Government of the United States access to "communications by mail, cable, radio, or other means of transmission passing between the United States and any foreign country." *Id*. *See also* Exec. Order No. 8985, § 1, 6 Fed. Reg. 6625, 6625 (Dec. 19, 1941). In addition, the United States systematically listened surreptitiously to electronic communications as part of the war effort. *See* Dash, *Eavesdroppers* at 30. During World War II, signals intelligence assisted in, among other things, the destruction of the German U-boat fleet by the Allied naval forces, *see id.* at 27, and the war against Japan, *see* O'Toole, *supra*, at 32, 323-24. In general, signals intelligence "helped to shorten the war by perhaps two years, reduce the loss of life, and make inevitable an eventual Allied victory." Carl Boyd, *American Command of the Sea Through Carriers, Codes, and the Silent Service: World War II and Beyond* 27 (1995); *see also* Alvarez, *supra*, at 1 ("There can be little doubt that signals intelligence contributed significantly to the

military defeat of the Axis."). Significantly, not only was wiretapping in World War II used "extensively by military intelligence and secret service personnel in combat areas abroad," but also "by the FBI and secret service in this country." Dash, *supra*, at 30.

In light of the long history of prior wartime practice, the NSA activities fit squarely within the sweeping terms of the AUMF. The use of signals intelligence to identify and pinpoint the enemy is a traditional component of wartime military operations—or, to use the terminology of *Hamdi,* a "fundamental and accepted . . . incident to war," 542 U.S. at 518 (plurality opinion)—employed to defeat the enemy and to prevent enemy attacks in the United States. Here, as in other conflicts, the enemy may use public communications networks, and some of the enemy may already be in the United States. Although those factors may be present in this conflict to a greater degree than in the past, neither is novel. Certainly, both factors were well known at the time Congress enacted the AUMF. Wartime interception of international communications made by the enemy thus should be understood, no less than the wartime detention at issue in *Hamdi,* as one of the basic methods of engaging and defeating the enemy that Congress authorized in approving "*all* necessary and appropriate force" that the President would need to defend the Nation. AUMF § 2(a) (emphasis added).

* * *

Accordingly, the President has the authority to conduct warrantless electronic surveillance against the declared enemy of the United States in a time of armed conflict. That authority derives from the Constitution, and is reinforced by the text and purpose of the AUMF, the nature of the threat posed by al Qaeda that Congress authorized the President to repel, and the long-established understanding that electronic surveillance is a fundamental incident of the use of military force. The President's power in authorizing the NSA activities is at its zenith because he has acted "pursuant to an express or implied authorization of Congress." *Youngstown*, 343 U.S. at 635 (Jackson, J., concurring).

III. THE NSA ACTIVITIES ARE CONSISTENT WITH THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

The President's exercise of his constitutional authority to conduct warrantless wartime electronic surveillance of the enemy, as confirmed and supplemented by statute in the AUMF, is fully consistent with the requirements of the Foreign Intelligence Surveillance Act ("FISA").[5] FISA is a critically important tool in the War on Terror. The United States makes full use of the authorities available under FISA to gather foreign intelligence information, including authorities to intercept communications, conduct physical searches, and install and use pen registers and trap and trace devices. While FISA establishes certain procedures that must be followed for these authorities to be used (procedures that usually involve applying for and obtaining an order from a special court), FISA also expressly contemplates that a later legislative enactment could

[5] To avoid revealing details about the operation of the program, it is assumed for purposes of this paper that the activities described by the President constitute "electronic surveillance," as defined by FISA, 50 U.S.C. § 1801(f).

authorize electronic surveillance outside the procedures set forth in FISA itself. The AUMF constitutes precisely such an enactment. To the extent there is any ambiguity on this point, the canon of constitutional avoidance requires that such ambiguity be resolved in favor of the President's authority to conduct the communications intelligence activities he has described. Finally, if FISA could not be read to allow the President to authorize the NSA activities during the current congressionally authorized armed conflict with al Qaeda, FISA would be unconstitutional as applied in this narrow context.

A. THE REQUIREMENTS OF FISA

FISA was enacted in 1978 to regulate "electronic surveillance," particularly when conducted to obtain "foreign intelligence information," as those terms are defined in section 101 of FISA, 50 U.S.C. § 1801. As a general matter, the statute requires that the Attorney General approve an application for an order from a special court composed of Article III judges and created by FISA—the Foreign Intelligence Surveillance Court ("FISC"). *See* 50 U.S.C. §§ 1803-1804. The application must demonstrate, among other things, that there is probable cause to believe that the target is a foreign power or an agent of a foreign power. *See id.* § 1805(a)(3)(A). It must also contain a certification from the Assistant to the President for National Security Affairs or an officer of the United States appointed by the President with the advice and consent of the Senate and having responsibilities in the area of national security or defense that the information sought is foreign intelligence information and cannot reasonably be obtained by normal investigative means. *See id.* § 1804(a)(7). FISA further requires the Government to state the means that it proposes to use to obtain the information and the basis for its belief that the facilities at which the surveillance will be directed are being used or are about to be used by a foreign power or an agent of a foreign power. *See id.* § 1804(a)(4), (a)(8).

FISA was the first congressional measure that sought to impose restrictions on the Executive Branch's authority to engage in electronic surveillance for foreign intelligence purposes, an authority that, as noted above, had been repeatedly recognized by the federal courts. *See* Americo R. Cinquegrana, *The Walls (and Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978*, 137 U. Penn. L. Rev. 793, 810 (1989) (stating that the "status of the President's inherent authority" to conduct surveillance "formed the core of subsequent legislative deliberations" leading to the enactment of FISA). To that end, FISA modified a provision in Title III that previously had disclaimed any intent to have laws governing wiretapping interfere with the President's constitutional authority to gather foreign intelligence. Prior to the passage of FISA, section 2511(3) of title 18 had stated that "[n]othing contained in this chapter or in section 605 of the Communications Act of 1934 . . . shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities." 18 U.S.C. § 2511(3) (1970). FISA replaced that provision with an important, though more limited, preservation of authority for the President. *See* Pub. L. No. 95-511, § 201(b), (c), 92 Stat. 1783, 1797 (1978), codified at 18 U.S.C. § 2511(2)(f) (West Supp. 2005) (carving out from statutory regulation only the acquisition of intelligence information from "international or foreign communications" and

"foreign intelligence activities . . . involving a foreign electronic communications system" as long as they are accomplished "utilizing a means other than electronic surveillance as defined in section 101" of FISA). Congress also defined "electronic surveillance," 50 U.S.C. § 1801(f), carefully and somewhat narrowly.[6]

In addition, Congress addressed, to some degree, the manner in which FISA might apply after a formal declaration of war by expressly allowing warrantless surveillance for a period of fifteen days following such a declaration. Section 111 of FISA allows the President to "authorize electronic surveillance without a court order under this subchapter to acquire foreign intelligence information for a period not to exceed fifteen calendar days following a declaration of war by the Congress." 50 U.S.C. § 1811.

The legislative history of FISA shows that Congress understood it was legislating on fragile constitutional ground and was pressing or even exceeding constitutional limits in regulating the President's authority in the field of foreign intelligence. The final House Conference Report, for example, recognized that the statute's restrictions might well impermissibly infringe on the President's constitutional powers. That report includes the extraordinary acknowledgment that "[t]he conferees agree that the establishment by this act of exclusive means by which the President may conduct electronic surveillance does not foreclose a different decision by the Supreme Court." H.R. Conf. Rep. No. 95-1720, at 35, *reprinted in* 1978 U.S.C.C.A.N. 4048, 4064. But, invoking Justice Jackson's concurrence in the *Steel Seizure* case, the Conference Report explained that Congress intended in FISA to exert whatever power Congress constitutionally had over the subject matter to restrict foreign intelligence surveillance and to leave the President solely with whatever inherent constitutional authority he might be able to invoke against Congress's express wishes. *Id.* The Report thus explains that "[t]he intent of the conferees is to apply the standard set forth in Justice Jackson's concurring opinion in the Steel Seizure Case: 'When a President takes measures incompatible with the express or implied

---

[6] FISA's legislative history reveals that these provisions were intended to exclude certain intelligence activities conducted by the National Security Agency from the coverage of FISA. According to the report of the Senate Judiciary Committee on FISA, "this provision [referencing what became the first part of section 2511(2)(f)] is designed to make clear that the legislation does not deal with international signals intelligence activities as currently engaged in by the National Security Agency and electronic surveillance conducted outside the United States." S. Rep. No. 95-604, at 64 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3965. The legislative history also makes clear that the definition of "electronic surveillance" was crafted for the same reason. *See id*. at 33-34, 1978 U.S.C.C.A.N. at 3934-36. FISA thereby "adopts the view expressed by the Attorney General during the hearings that enacting statutory controls to regulate the National Security Agency and the surveillance of Americans abroad raises problems best left to separate legislation." *Id*. at 64, 1978 U.S.C.C.A.N. at 3965. Such legislation placing limitations on traditional NSA activities was drafted, but never passed. *See* National Intelligence Reorganization and Reform Act of 1978: Hearings Before the Senate Select Committee on Intelligence, 95th Cong., 2d Sess. 999-1007 (1978) (text of unenacted legislation). And Congress understood that the NSA surveillance that it intended categorically to exclude from FISA could include the monitoring of international communications into or out of the United States of U.S. citizens. The report specifically referred to the Church Committee report for its description of the NSA's activities, S. Rep. No. 95-604, at 64 n.63, 1978 U.S.C.C.A.N. at 3965-66 n.63, which stated that "the NSA intercepts messages passing over international lines of communication, some of which have one terminal within the United States. Traveling over these lines of communication, especially those with one terminal in the United States, are messages of Americans . . . ." S. Rep. 94-755, at Book II, 308 (1976). Congress's understanding in the legislative history of FISA that such communications could be intercepted outside FISA procedures is notable.

will of Congress, his power is at the lowest ebb, for then he can rely only upon his own constitutional power minus any constitutional power of Congress over the matter.'" *Id.* (quoting *Youngstown Sheet & Tube Co*. v. *Sawyer,* 343 U.S. 579, 637 (1952) (Jackson, J., concurring)); *see also* S. Rep. No. 95-604, at 64, *reprinted in* 1978 U.S.C.C.A.N. at 3966 (same); *see generally* Elizabeth B. Bazen et al., Congressional Research Service, *Re: Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information* 28-29 (Jan. 5, 2006). It is significant, however, that Congress did not decide conclusively to continue to push the boundaries of its constitutional authority in wartime. Instead, Congress reserved the question of the appropriate procedures to regulate electronic surveillance in time of war, and established a fifteen-day period during which the President would be permitted to engage in electronic surveillance without complying with FISA's express procedures and during which Congress would have the opportunity to revisit the issue. *See* 50 U.S.C. § 1811; H.R. Conf. Rep. No. 95-1720, at 34, *reprinted in* 1978 U.S.C.C.A.N. at 4063 (noting that the purpose of the fifteen-day period following a declaration of war in section 111 of FISA was to "allow time for consideration of any amendment to this act that may be appropriate during a wartime emergency").

B. FISA CONTEMPLATES AND ALLOWS SURVEILLANCE AUTHORIZED "BY STATUTE"

Congress did not attempt through FISA to prohibit the Executive Branch from using electronic surveillance. Instead, Congress acted to bring the exercise of that power under more stringent congressional control. *See, e.g.*, H. Conf. Rep. No. 95-1720, at 32, *reprinted in* 1978 U.S.C.C.A.N. 4048, 4064. Congress therefore enacted a regime intended to supplant the President's reliance on his own constitutional authority. Consistent with this overriding purpose of bringing the use of electronic surveillance under *congressional* control and with the commonsense notion that the Congress that enacted FISA could not bind future Congresses, FISA expressly contemplates that the Executive Branch may conduct electronic surveillance outside FISA's express procedures if and when a subsequent statute authorizes such surveillance.

Thus, section 109 of FISA prohibits any person from intentionally "engag[ing] . . . in electronic surveillance under color of law *except as authorized by statute*." 50 U.S.C. § 1809(a)(1) (emphasis added). Because FISA's prohibitory provision broadly exempts surveillance "authorized by statute," the provision demonstrates that Congress did not attempt to regulate through FISA electronic surveillance authorized by Congress through a subsequent enactment. The use of the term "statute" here is significant because it strongly suggests that *any* subsequent authorizing statute, not merely one that amends FISA itself, could legitimately authorize surveillance outside FISA's standard procedural requirements. *Compare* 18 U.S.C. § 2511(1) ("Except as otherwise specifically provided *in this chapter* any person who—(a) intentionally intercepts . . . any wire, oral, or electronic communication[] . . . shall be punished . . . .") (emphasis added); *id*. § 2511(2)(e) (providing a defense to liability to individuals "conduct[ing] electronic surveillance, . . . as authorized by *that Act [FISA]*") (emphasis added). In enacting FISA, therefore, Congress contemplated the possibility that the President might be permitted to conduct electronic surveillance pursuant to a later-enacted statute that did not

incorporate all of the procedural requirements set forth in FISA or that did not expressly amend FISA itself.

To be sure, the scope of this exception is rendered less clear by the conforming amendments that FISA made to chapter 119 of title 18—the portion of the criminal code that provides the mechanism for obtaining wiretaps for law enforcement purposes. Before FISA was enacted, chapter 119 made it a criminal offense for any person to intercept a communication except as specifically provided in that chapter. *See* 18 U.S.C. § 2511(1)(a), (4)(a). Section 201(b) of FISA amended that chapter to provide an exception from criminal liability for activities conducted pursuant to FISA. Specifically, FISA added 18 U.S.C. § 2511(2)(e), which provides that it is not unlawful for "an officer, employee, or agent of the United States . . . to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act." *Id.* § 2511(2)(e). Similarly, section 201(b) of FISA amended chapter 119 to provide that "procedures in this chapter [or chapter 121 (addressing access to stored wire and electronic communications and customer records)] and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted." *Id.* § 2511(2)(f) (West Supp. 2005).[7]

The amendments that section 201(b) of FISA made to title 18 are fully consistent, however, with the conclusion that FISA contemplates that a subsequent statute could authorize electronic surveillance outside FISA's express procedural requirements. Section 2511(2)(e) of title 18, which provides that it is "not unlawful" for an officer of the United States to conduct electronic surveillance "as authorized by" FISA, is best understood as a safe-harbor provision. Because of section 109, the protection offered by section 2511(2)(e) for surveillance "authorized by" FISA extends to surveillance that is authorized by any other statute and therefore excepted from the prohibition of section 109. In any event, the purpose of section 2511(2)(e) is merely to make explicit what would already have been implicit—that those authorized by statute to engage in particular surveillance do not act unlawfully when they conduct such surveillance. Thus, even if that provision had not been enacted, an officer conducting surveillance authorized by statute (whether FISA or some other law) could not reasonably have been thought to be violating Title III. Similarly, section 2511(2)(e) cannot be read to require a result that would be manifestly unreasonable—exposing a federal officer to criminal liability for engaging in surveillance authorized by statute, merely because the authorizing statute happens not to be FISA itself.

Nor could 18 U.S.C. § 2511(2)(f), which provides that the "procedures in this chapter . . . and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance . . . may be conducted," have been intended to trump the commonsense approach of section 109 and preclude a subsequent Congress from authorizing the President to engage in electronic surveillance through a statute other than FISA, using procedures other than those outlined in FISA or chapter 119 of title 18. The legislative history of section 2511(2)(f) clearly indicates an intent to prevent the President from engaging in surveillance except as

[7] The bracketed portion was added in 1986 amendments to section 2511(2)(f). *See* Pub. L. No. 99-508 § 101(b)(3), 100 Stat. 1848, 1850.

authorized by Congress, *see* H.R. Conf. Rep. No. 95-1720, at 32, *reprinted in* 1978 U.S.C.C.A.N. 4048, 4064, which explains why section 2511(2)(f) set forth all then-existing statutory restrictions on electronic surveillance. Section 2511(2)(f)'s reference to "exclusive means" reflected the state of statutory authority for electronic surveillance in 1978 and cautioned the President not to engage in electronic surveillance outside congressionally sanctioned parameters. It is implausible to think that, in attempting to limit the *President's* authority, Congress also limited its own future authority by barring subsequent Congresses from authorizing the Executive to engage in surveillance in ways not specifically enumerated in FISA or chapter 119, or by requiring a subsequent Congress specifically to amend FISA and section 2511(2)(f). There would be a serious question as to whether the Ninety-Fifth Congress could have so tied the hands of its successors. *See, e.g.*, *Fletcher v. Peck*, 10 U.S. (6 Cranch) 87, 135 (1810) (noting that "one legislature cannot abridge the powers of a succeeding legislature"); *Reichelderfer v. Quinn*, 287 U.S. 315, 318 (1932) ("[T]he will of a particular Congress . . . does not impose itself upon those to follow in succeeding years"); *Lockhart v. United States*, 126 S. Ct. 699, 703 (2005) (Scalia, J., concurring) (collecting precedent); 1 W. Blackstone, Commentaries on the Laws of England 90 (1765) ("Acts of parliament derogatory from the power of subsequent parliaments bind not"). In the absence of a clear statement to the contrary, it cannot be presumed that Congress attempted to abnegate its own authority in such a way.

Far from a clear statement of congressional intent to bind itself, there are indications that section 2511(2)(f) cannot be interpreted as requiring that *all* electronic surveillance and domestic interception be conducted under FISA's enumerated procedures or those of chapter 119 of title 18 until and unless those provisions are repealed or amended. Even when section 2511(2)(f) was enacted (and no subsequent authorizing statute existed), it could not reasonably be read to preclude all electronic surveillance conducted outside the procedures of FISA or chapter 119 of title 18. In 1978, use of a pen register or trap and trace device constituted electronic surveillance as defined by FISA. *See* 50 U.S.C. §§ 1801(f), (n). Title I of FISA provided procedures for obtaining court authorization for the use of pen registers to obtain foreign intelligence information. But the Supreme Court had, just prior to the enactment of FISA, held that chapter 119 of title 18 did not govern the use of pen registers. *See United States v. New York Tel. Co.*, 434 U.S. 159, 165-68 (1977). Thus, if section 2511(2)(f) were to be read to permit of no exceptions, the use of pen registers for purposes other than to collect foreign intelligence information would have been unlawful because such use would not have been authorized by the "exclusive" procedures of section 2511(2)(f), *i.e.*, FISA and chapter 119. But no court has held that pen registers could not be authorized outside the foreign intelligence context. Indeed, FISA appears to have recognized this issue by providing a defense to liability for any official who engages in electronic surveillance under a search warrant or court order. *See* 50 U.S.C. § 1809(b). (The practice when FISA was enacted was for law enforcement officers to obtain search warrants under the Federal Rules of Criminal Procedure authorizing the installation and use of pen registers. *See S. 1667, A Bill to Amend Title 18, United States Code, with Respect to the Interception of Certain Communications, Other Forms of Surveillance, and for Other Purposes: Hearing Before the Subcomm. On Patents, Copyrights and Trademarks of the Senate*

Comm. on the Judiciary, 99th Cong. 57 (1985) (prepared statement of James Knapp, Deputy Assistant Attorney General, Criminal Division)).[8]

In addition, section 2511(2)(a)(ii) authorizes telecommunications providers to assist officers of the Government engaged in electronic surveillance when the Attorney General certifies that "no warrant or court order is required by law [and] that all statutory requirements have been met." 18 U.S.C. § 2511(2)(a)(ii).[9] If the Attorney General can certify, in good faith, that the requirements of a subsequent statute authorizing electronic surveillance are met, service providers are affirmatively and expressly authorized to assist the Government. Although FISA does allow the Government to proceed without a court order in several situations, *see* 50 U.S.C. § 1805(f) (emergencies); *id.* § 1802 (certain communications between foreign governments), this provision specifically lists only Title III's emergency provision but speaks generally to Attorney General certification. That reference to Attorney General certification is consistent with the historical practice in which Presidents have delegated to the Attorney General authority to approve warrantless surveillance for foreign intelligence purposes. *See, e.g.*, *United States v. United States District Court,* 444 F.2d 651, 669-71 (6th Cir. 1971) (reproducing as an appendix memoranda from Presidents Roosevelt, Truman, and Johnson). Section 2511(2)(a)(ii) thus suggests that telecommunications providers can be authorized to assist with warrantless electronic surveillance when such surveillance is authorized by law outside FISA.

In sum, by expressly and broadly excepting from its prohibition electronic surveillance undertaken "as authorized by statute," section 109 of FISA permits an exception to the "procedures" of FISA referred to in 18 U.S.C. § 2511(2)(f) where authorized by another statute, even if the other authorizing statute does not specifically amend section 2511(2)(f).

C. THE AUMF IS A "STATUTE" AUTHORIZING SURVEILLANCE OUTSIDE THE CONFINES OF FISA

The AUMF qualifies as a "statute" authorizing electronic surveillance within the meaning of section 109 of FISA.

First, because the term "statute" historically has been given broad meaning, the phrase "authorized by statute" in section 109 of FISA must be read to include joint resolutions such as

---

[8] Alternatively, section 109(b) may be read to constitute a "procedure" in FISA or to incorporate procedures from sources other than FISA (such as the Federal Rules of Criminal Procedure or state court procedures), and in that way to satisfy section 2511(2)(f). But if section 109(b)'s defense can be so read, section 109(a) should also be read to constitute a procedure or incorporate procedures not expressly enumerated in FISA.

[9] Section 2511(2)(a)(ii) states:

> Notwithstanding any other law, providers of wire or electronic communication service, . . . are authorized by law to provide information, facilities, or technical assistance to persons authorized by law to intercept . . . communications or to conduct electronic surveillance, as defined [by FISA], if such provider . . . has been provided with . . . a certification in writing by [specified persons proceeding under Title III's emergency provision] or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specific assistance is required.

the AUMF. *See American Fed'n of Labor v. Watson*, 327 U. S. 582, 592-93 (1946) (finding the term "statute" as used in 28 U.S.C. § 380 to mean "a compendious summary of various enactments, by whatever method they may be adopted, to which a State gives her sanction"); Black's Law Dictionary 1410 (6th ed. 1990) (defining "statute" broadly to include any "formal written enactment of a legislative body," and stating that the term is used "to designate the legislatively created laws in contradistinction to court decided or unwritten laws"). It is thus of no significance to this analysis that the AUMF was enacted as a joint resolution rather than a bill. *See, e.g., Ann Arbor R.R. Co. v. United States*, 281 U.S. 658, 666 (1930) (joint resolutions are to be construed by applying "the rules applicable to legislation in general"); *United States ex rel. Levey v. Stockslager*, 129 U.S. 470, 475 (1889) (joint resolution had "all the characteristics and effects" of statute that it suspended); *Padilla ex rel. Newman v. Bush,* 233 F. Supp. 2d 564, 598 (S.D.N.Y 2002) (in analyzing the AUMF, finding that there is "no relevant constitutional difference between a bill and a joint resolution"), *rev'd sub nom. on other grounds, Rumsfeld v. Padilla*, 352 F.3d 695 (2d Cir. 2003), *rev'd*, 542 U.S. 426 (2004); *see also* Letter for the Hon. John Conyers, Jr., U.S. House of Representatives, from Prof. Laurence H. Tribe at 3 (Jan. 6, 2006) (term "statute" in section 109 of FISA "of course encompasses a joint resolution presented to and signed by the President").

Second, the longstanding history of communications intelligence as a fundamental incident of the use of force and the Supreme Court's decision in *Hamdi v. Rumsfeld* strongly suggest that the AUMF satisfies the requirement of section 109 of FISA for statutory authorization of electronic surveillance. As explained above, it is not necessary to demarcate the outer limits of the AUMF to conclude that it encompasses electronic surveillance targeted at the enemy. Just as a majority of the Court concluded in *Hamdi* that the AUMF authorizes detention of U.S. citizens who are enemy combatants without expressly mentioning the President's long-recognized power to detain, so too does it authorize the use of electronic surveillance without specifically mentioning the President's equally long-recognized power to engage in communications intelligence targeted at the enemy. And just as the AUMF satisfies the requirement in 18 U.S.C. § 4001(a) that no U.S. citizen be detained "except pursuant to an Act of Congress," so too does it satisfy section 109's requirement for statutory authorization of electronic surveillance.[10] In authorizing the President's use of force in response to the September 11th attacks, Congress did not need to comb through the United States Code looking for those restrictions that it had placed on national security operations during times of peace and designate with specificity each traditional tool of military force that it sought to authorize the President to use. There is no historical precedent for such a requirement: authorizations to use

[10] It might be argued that Congress dealt more comprehensively with electronic surveillance in FISA than it did with detention in 18 U.S.C. § 4001(a). Thus, although Congress prohibited detention "except pursuant to an Act of Congress," it combined the analogous prohibition in FISA (section 109(a)) with section 2511(2)(f)'s exclusivity provision. *See* Letter to the Hon. Bill Frist, Majority Leader, U.S. Senate, from Professor Curtis A. Bradley *et al.* at 5 n.6 (Jan. 9, 2006) (noting that section 4001(a) does not "attempt[] to create an exclusive mechanism for detention"). On closer examination, however, it is evident that Congress has regulated detention far more meticulously than these arguments suggest. Detention is the topic of much of the Criminal Code, as well as a variety of other statutes, including those providing for civil commitment of the mentally ill and confinement of alien terrorists. The existence of these statutes and accompanying extensive procedural safeguards, combined with the substantial constitutional issues inherent in detention, *see, e.g.*, *Hamdi*, 542 U.S. at 574-75 (Scalia, J., dissenting), refute any such argument.

military force traditionally have been couched in general language. Indeed, prior administrations have interpreted joint resolutions declaring war and authorizing the use of military force to authorize expansive collection of communications into and out of the United States.[11]

Moreover, crucial to the Framers' decision to vest the President with primary constitutional authority to defend the Nation from foreign attack is the fact that the Executive can act quickly, decisively, and flexibly as needed. For Congress to have a role in that process, it must be able to act with similar speed, either to lend its support to, or to signal its disagreement with, proposed military action. Yet the need for prompt decisionmaking in the wake of a devastating attack on the United States is fundamentally inconsistent with the notion that to do so Congress must legislate at a level of detail more in keeping with a peacetime budget reconciliation bill. In emergency situations, Congress must be able to use broad language that effectively sanctions the President's use of the core incidents of military force. That is precisely what Congress did when it passed the AUMF on September 14, 2001—just three days after the deadly attacks on America. The Capitol had been evacuated on September 11th, and Congress was meeting in scattered locations. As an account emerged of who might be responsible for these attacks, Congress acted quickly to authorize the President to use "all necessary and appropriate force" against the enemy that he determines was involved in the September 11th attacks. Under these circumstances, it would be unreasonable and wholly impractical to demand that Congress specifically amend FISA in order to assist the President in defending the Nation. Such specificity would also have been self-defeating because it would have apprised our adversaries of some of our most sensitive methods of intelligence gathering.[12]

Section 111 of FISA, 50 U.S.C. § 1811, which authorizes the President, "[n]otwithstanding any other law," to conduct "electronic surveillance without a court order under this subchapter to acquire foreign intelligence information for a period not to exceed fifteen calendar days following a declaration of war by Congress," does not require a different reading of the AUMF. *See also id.* § 1844 (same provision for pen registers); *id.* § 1829 (same provision for physical searches). Section 111 cannot reasonably be read as Congress's final word on electronic surveillance during wartime, thus permanently limiting the President in all

---

[11] As noted above, in intercepting communications, President Wilson relied on his constitutional authority and the joint resolution declaring war and authorizing the use of military force, which, as relevant here, provided "that the President [is] authorized and directed to employ the entire naval and military forces of the United States and the resources of the Government to carry on war against the Imperial German Government; and to bring the conflict to a successful termination all of the resources of the country are hereby pledged by the Congress of the United States." Joint Resolution of Apr. 6, 1917, ch. 1, 40 Stat. 1. The authorization did not explicitly mention interception of communications.

[12] Some have suggested that the Administration declined to seek a specific amendment to FISA allowing the NSA activities "because it was advised that Congress would reject such an amendment," Letter to the Hon. Bill Frist, Majority Leader, U.S. Senate, from Professor Curtis A. Bradley *et al.* 4 & n.4 (Jan. 9, 2005), and they have quoted in support of that assertion the Attorney General's statement that certain Members of Congress advised the Administration that legislative relief "would be difficult, if not impossible." *Id.* at 4 n.4. As the Attorney General subsequently indicated, however, the difficulty with such specific legislation was that it could not be enacted "without compromising the program." *See* Remarks by Homeland Security Secretary Chertoff and Attorney General Gonzales on the USA PATRIOT Act (Dec. 21, 2005), *available at* http://www.dhs.gov/dhspublic/display?content=5285.

circumstances to a mere fifteen days of warrantless military intelligence gathering targeted at the enemy following a declaration of war. Rather, section 111 represents Congress's recognition that it would likely have to return to the subject and provide additional authorization to conduct warrantless electronic surveillance outside FISA during time of war. The Conference Report explicitly stated the conferees' "inten[t] that this [fifteen-day] period will allow time for consideration of any amendment to this act that may be appropriate during a wartime emergency." H.R. Conf. Rep. No. 95-1720, at 34, *reprinted in* 1978 U.S.C.C.A.N. at 4063. Congress enacted section 111 so that the President could conduct warrantless surveillance while Congress considered supplemental wartime legislation.

Nothing in the terms of section 111 disables Congress from authorizing such electronic surveillance as a traditional incident of war through a broad, conflict-specific authorization for the use of military force, such as the AUMF. Although the legislative history of section 111 indicates that in 1978 some Members of Congress believed that any such authorization would come in the form of a particularized amendment to FISA itself, section 111 does not require that result. Nor could the Ninety-Fifth Congress tie the hands of a subsequent Congress in this way, at least in the absence of far clearer statutory language expressly requiring that result. *See supra*, pp. 21-22; *compare, e.g.*, War Powers Resolution, § 8, 50 U.S.C. § 1547(a) ("Authority to introduce United States Armed Forces into hostilities . . . shall not be inferred . . . from any provision of law . . . unless such provision specifically authorizes [such] introduction . . . and states that it is intended to constitute specific statutory authorization within the meaning of this chapter."); 10 U.S.C. § 401 (stating that any other provision of law providing assistance to foreign countries to detect and clear landmines shall be subject to specific limitations and may be construed as superseding such limitations "only if, and to the extent that, such provision specifically refers to this section and specifically identifies the provision of this section that is to be considered superseded or otherwise inapplicable"). An interpretation of section 111 that would disable Congress from authorizing broader electronic surveillance in that form can be reconciled neither with the purposes of section 111 nor with the well-established proposition that "one legislature cannot abridge the powers of a succeeding legislature." *Fletcher v. Peck*, 10 U.S. (6 Cranch) at 135; *see supra* Part II.B. For these reasons, the better interpretation is that section 111 was not intended to, and did not, foreclose Congress from using the AUMF as the legal vehicle for supplementing the President's existing authority under FISA in the battle against al Qaeda.

The contrary interpretation of section 111 also ignores the important differences between a formal declaration of war and a resolution such as the AUMF. As a historical matter, a formal declaration of war was no longer than a sentence, and thus Congress would not expect a declaration of war to outline the extent to which Congress authorized the President to engage in various incidents of waging war. Authorizations for the use of military force, by contrast, are typically more detailed and are made for the *specific purpose* of reciting the manner in which Congress has authorized the President to act. Thus, Congress could reasonably expect that an authorization for the use of military force would address the issue of wartime surveillance, while a declaration of war would not. Here, the AUMF declares that the Nation faces "an unusual and extraordinary threat," acknowledges that "the President has authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States," and

provides that the President is authorized "to use all necessary and appropriate force" against those "he determines" are linked to the September 11th attacks. AUMF pmbl., § 2. This sweeping language goes far beyond the bare terms of a declaration of war. *Compare*, *e.g.*, Act of Apr. 25, 1898, ch. 189, 30 Stat. 364 ("First. That war be, and the same is hereby declared to exist . . . between the United States of America and the Kingdom of Spain.").

Although legislation that has included a declaration of war has often also included an authorization of the President to use force, these provisions are separate and need not be combined in a single statute. *See*, *e.g.*, *id.* ("Second. That the President of the United States be, and he hereby is, directed and empowered to use the entire land and naval forces of the United States, and to call into the actual service of the United States the militia of the several states, *to such extent as may be necessary to carry this Act into effect*.") (emphasis added). Moreover, declarations of war have legal significance independent of any additional authorization of force that might follow. *See*, *e.g.*, Louis Henkin, *Foreign Affairs and the U.S. Constitution* 75 (2d ed. 1996) (explaining that a formal state of war has various legal effects, such as terminating diplomatic relations, and abrogating or suspending treaty obligations and international law rights and duties); *see also id.* at 370 n.65 (speculating that one reason to fight an undeclared war would be to "avoid the traditional consequences of declared war on relations with third nations or even . . . belligerents").

In addition, section 111 does not cover the vast majority of modern military conflicts. The last declared war was World War II. Indeed, the most recent conflict prior to the passage of FISA, Vietnam, was fought without a formal declaration of war. In addition, the War Powers Resolution, enacted less than five years before FISA, clearly recognizes the distinctions between formal declarations of war and authorizations of force and demonstrates that, if Congress had wanted to include such authorizations in section 111, it knew how to do so. *See, e.g.*, 50 U.S.C. § 1544(b) (attempting to impose certain consequences 60 days after reporting the initiation of hostilities to Congress "unless the Congress . . . has declared war *or has enacted a specific authorization for such use*" of military force) (emphasis added). It is possible that, in enacting section 111, Congress intended to make no provision for even the temporary use of electronic surveillance without a court order for what had become the legal regime for most military conflicts. A better reading, however, is that Congress assumed that such a default provision would be unnecessary because, if it had acted through an authorization for the use of military force, the more detailed provisions of that authorization would resolve the extent to which Congress would attempt to authorize, or withhold authorization for, the use of electronic surveillance.[13]

[13] Some have pointed to the specific amendments to FISA that Congress made shortly after September 11th in the USA PATRIOT Act, Pub. L. No. 107-56, §§ 204, 218, 115 Stat. 272, 281, 291 (2001), to argue that Congress did not contemplate electronic surveillance outside the parameters of FISA. *See* Memorandum for Members of the House Permanent Select Comm. on Intel. from Jeffrey H. Smith, *Re: Legal Authorities Regarding Warrantless Surveillance of U.S. Persons* 6-7 (Jan. 3, 2006). The USA PATRIOT Act amendments, however, do not justify giving the AUMF an unnaturally narrow reading. The USA PATRIOT Act amendments made important corrections in the general application of FISA; they were not intended to define the precise incidents of military force that would be available to the President in prosecuting the current armed conflict against al Qaeda and its allies. Many removed long-standing impediments to the effectiveness of FISA that had contributed to the

* * *

The broad text of the AUMF, the authoritative interpretation that the Supreme Court gave it in *Hamdi*, and the circumstances in which it was passed demonstrate that the AUMF is a statute authorizing electronic surveillance under section 109 of FISA. When the President authorizes electronic surveillance against the enemy pursuant to the AUMF, he is therefore acting at the height of his authority under *Youngstown*, 343 U.S. at 637 (Jackson, J., concurring).

D. THE CANON OF CONSTITUTIONAL AVOIDANCE REQUIRES RESOLVING IN FAVOR OF THE PRESIDENT'S AUTHORITY ANY AMBIGUITY ABOUT WHETHER FISA FORBIDS THE NSA ACTIVITIES

As explained above, the AUMF fully authorizes the NSA activities. Because FISA contemplates the possibility that subsequent statutes could authorize electronic surveillance without requiring FISA's standard procedures, the NSA activities are also consistent with FISA and related provisions in title 18. Nevertheless, some might argue that sections 109 and 111 of FISA, along with section 2511(2)(f)'s "exclusivity" provision and section 2511(2)(e)'s liability exception for officers engaged in FISA-authorized surveillance, are best read to suggest that FISA requires that subsequent authorizing legislation specifically amend FISA in order to free the Executive from FISA's enumerated procedures. As detailed above, this is not the better reading of FISA. But even if these provisions were ambiguous, any doubt as to whether the AUMF and FISA should be understood to allow the President to make tactical military decisions to authorize surveillance outside the parameters of FISA must be resolved to avoid the serious constitutional questions that a contrary interpretation would raise.

It is well established that the first task of any interpreter faced with a statute that may present an unconstitutional infringement on the powers of the President is to determine whether the statute may be construed to avoid the constitutional difficulty. "[I]f an otherwise acceptable

---

maintenance of an unnecessary "wall" between foreign intelligence gathering and criminal law enforcement; others were technical clarifications. *See In re Sealed Case,* 310 F.3d 717, 725-30 (Foreign Int. Surv. Ct. Rev. 2002). The "wall" had been identified as a significant problem hampering the Government's efficient use of foreign intelligence information well before the September 11th attacks and in contexts unrelated to terrorism. *See, e.g., Final Report of the Attorney General's Review Team on the Handling of the Los Alamos National Laboratory Investigation* 710, 729, 732 (May 2000); General Accounting Office, *FBI Intelligence Investigations: Coordination Within Justice on Counterintelligence Criminal Matters Is Limited* (GAO-01-780) 3, 31 (July 2001). Finally, it is worth noting that Justice Souter made a similar argument in *Hamdi* that the USA PATRIOT Act all but compelled a narrow reading of the AUMF. *See* 542 U.S. at 551 ("It is very difficult to believe that the same Congress that carefully circumscribed Executive power over alien terrorists on home soil [in the USA PATRIOT Act] would not have meant to require the Government to justify clearly its detention of an American citizen held on home soil incommunicado."). Only Justice Ginsburg joined this opinion, and the position was rejected by a majority of Justices.

Nor do later amendments to FISA undermine the conclusion that the AUMF authorizes electronic surveillance outside the procedures of FISA. Three months after the enactment of the AUMF, Congress enacted certain "technical amendments" to FISA which, *inter alia*, extended the time during which the Attorney General may issue an emergency authorization of electronic surveillance from 24 to 72 hours. *See* Intelligence Authorization Act for Fiscal Year 2002, Pub. L. No. 107-108, § 314, 115 Stat. 1394, 1402 (2001). These modifications to FISA do not in any way undermine Congress's previous authorization in the AUMF for the President to engage in electronic surveillance outside the parameters of FISA in the specific context of the armed conflict with al Qaeda.

construction of a statute would raise serious constitutional problems, and where an alternative interpretation of the statute is 'fairly possible,' we are obligated to construe the statute to avoid such problems." *INS v. St. Cyr,* 533 U.S. 289, 299-300 (2001) (citations omitted); *Ashwander v. TVA,* 297 U.S. 288, 345-48 (1936) (Brandeis, J., concurring). Moreover, the canon of constitutional avoidance has particular importance in the realm of national security, where the President's constitutional authority is at its highest. *See Department of the Navy v. Egan*, 484 U.S. 518, 527, 530 (1988); William N. Eskridge, Jr., *Dynamic Statutory Interpretation* 325 (1994) (describing "[s]uper-strong rule against congressional interference with the President's authority over foreign affairs and national security"). Thus, courts and the Executive Branch typically construe a general statute, even one that is written in unqualified terms, to be implicitly limited so as not to infringe on the President's Commander in Chief powers.

Reading FISA to prohibit the NSA activities would raise two serious constitutional questions, both of which must be avoided if possible: (1) whether the signals intelligence collection the President determined was necessary to undertake is such a core exercise of Commander in Chief control over the Armed Forces during armed conflict that Congress cannot interfere with it at all and (2) whether the particular restrictions imposed by FISA are such that their application would impermissibly impede the President's exercise of his constitutionally assigned duties as Commander in Chief. Constitutional avoidance principles require interpreting FISA, at least in the context of the military conflict authorized by the AUMF, to avoid these questions, if "fairly possible." Even if Congress intended FISA to use the full extent of its constitutional authority to "occupy the field" of "electronic surveillance," as FISA used that term, during peacetime, the legislative history indicates that Congress had not reached a definitive conclusion about its regulation during wartime. *See* H.R. Conf. Rep. No. 95-1720, at 34, *reprinted in* 1978 U.S.C.C.A.N. at 4063 (noting that the purpose of the fifteen-day period following a declaration of war in section 111 of FISA was to "allow time for consideration of any amendment to this act that may be appropriate during a wartime emergency"). Therefore, it is not clear that Congress, in fact, intended to test the limits of its constitutional authority in the context of wartime electronic surveillance.

Whether Congress may interfere with the President's constitutional authority to collect foreign intelligence information through interception of communications reasonably believed to be linked to the enemy poses a difficult constitutional question. As explained in Part I, it had long been accepted at the time of FISA's enactment that the President has inherent constitutional authority to conduct warrantless electronic surveillance for foreign intelligence purposes. Congress recognized at the time that the enactment of a statute purporting to eliminate the President's ability, even during peacetime, to conduct warrantless electronic surveillance to collect foreign intelligence was near or perhaps beyond the limit of Congress's Article I powers. The NSA activities, however, involve signals intelligence performed in the midst of a congressionally authorized armed conflict undertaken to prevent further hostile attacks on the United States. The NSA activities lie at the very core of the Commander in Chief power, especially in light of the AUMF's explicit authorization for the President to take *all* necessary and appropriate military action to stop al Qaeda from striking again. The constitutional principles at stake here thus involve not merely the President's well-established inherent

authority to conduct warrantless surveillance for foreign intelligence purposes during peacetime, but also the powers and duties expressly conferred on him as Commander in Chief by Article II.

Even outside the context of wartime surveillance of the enemy, the source and scope of Congress's power to restrict the President's inherent authority to conduct foreign intelligence surveillance is unclear. As explained above, the President's role as sole organ for the Nation in foreign affairs has long been recognized as carrying with it preeminent authority in the field of national security and foreign intelligence. The source of this authority traces to the Vesting Clause of Article II, which states that "[t]he executive Power shall be vested in a President of the United States of America." U.S. Const. art. II, § 1. The Vesting Clause "has long been held to confer on the President plenary authority to represent the United States and to pursue its interests outside the borders of the country, subject only to limits specifically set forth in the Constitution itself and to such statutory limitations as the Constitution permits Congress to impose by exercising one of its enumerated powers." *The President's Compliance with the "Timely Notification" Requirement of Section 501(b) of the National Security Act,* 10 Op. O.L.C. 159, 160-61 (1986) ("*Timely Notification Requirement Op.*").

Moreover, it is clear that some presidential authorities in this context are beyond Congress's ability to regulate. For example, as the Supreme Court explained in *Curtiss-Wright,* the President "*makes* treaties with the advice and consent of the Senate; but he alone negotiates. Into the field of negotiation the Senate cannot intrude; and Congress itself is powerless to invade it." 299 U.S. at 319. Similarly, President Washington established early in the history of the Republic the Executive's absolute authority to maintain the secrecy of negotiations with foreign powers, even against congressional efforts to secure information. *See id.* at 320-21. Recognizing presidential authority in this field, the Executive Branch has taken the position that "congressional legislation authorizing extraterritorial diplomatic and intelligence activities is superfluous, and . . . statutes infringing the President's inherent Article II authority would be unconstitutional." *Timely Notification Requirement Op.*, 10 Op. O.L.C. at 164.

There are certainly constitutional limits on Congress's ability to interfere with the President's power to conduct foreign intelligence searches, consistent with the Constitution, within the United States. As explained above, intelligence gathering is at the heart of executive functions. Since the time of the Founding it has been recognized that matters requiring secrecy—and intelligence in particular—are quintessentially executive functions. *See, e.g., The Federalist No. 64*, at 435 (John Jay) (Jacob E. Cooke ed. 1961) ("The convention have done well therefore in so disposing of the power of making treaties, that although the president must in forming them act by the advice and consent of the senate, yet he will be able to manage the business of intelligence in such manner as prudence may suggest."); *see also Timely Notification Requirement Op.*, 10 Op. O.L.C. at 165; *cf. New York Times Co. v. United States,* 403 U.S. 713, 729-30 (1971) (Stewart, J., concurring) ("[I]t is the constitutional duty of the Executive—as a matter of sovereign prerogative and not as a matter of law as the courts know law—through the promulgation and enforcement of executive regulations, to protect the confidentiality necessary to carry out its responsibilities in the field of international relations and national defense.").

Because Congress has rarely attempted to intrude in this area and because many of these questions are not susceptible to judicial review, there are few guideposts for determining exactly where the line defining the President's sphere of exclusive authority lies. Typically, if a statute is in danger of encroaching upon exclusive powers of the President, the courts apply the constitutional avoidance canon, if a construction avoiding the constitutional issue is "fairly possible." *See, e.g., Egan,* 484 U.S. at 527, 530. The only court that squarely has addressed the relative powers of Congress and the President in this field suggested that the balance tips decidedly in the President's favor. The Foreign Intelligence Surveillance Court of Review recently noted that all courts to have addressed the issue of the President's inherent authority have "held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information." *In re Sealed Case,* 310 F.3d 717, 742 (Foreign Intel. Surv. Ct. of Rev. 2002). On the basis of that unbroken line of precedent, the court "[took] for granted that the President does have that authority," and concluded that, "assuming that is so, FISA could not encroach on the President's constitutional power." *Id.*[14] Although the court did not provide extensive analysis, it is the only judicial statement on point, and it comes from the specialized appellate court created expressly to deal with foreign intelligence issues under FISA.

But the NSA activities are not simply exercises of the President's general foreign affairs powers. Rather, they are primarily an exercise of the President's authority as Commander in Chief during an armed conflict that Congress expressly has authorized the President to pursue. The NSA activities, moreover, have been undertaken specifically to prevent a renewed attack at the hands of an enemy that has already inflicted the single deadliest foreign attack in the Nation's history. The core of the Commander in Chief power is the authority to direct the Armed Forces in conducting a military campaign. Thus, the Supreme Court has made clear that the "President alone" is "constitutionally invested with the entire charge of hostile operations." *Hamilton v. Dillin,* 88 U.S. (21 Wall.) 73, 87 (1874); *The Federalist* No. 74, at 500 (Alexander Hamilton). "As commander-in-chief, [the President] is authorized to direct the movements of the naval and military forces placed by law at his command, and to employ them in the manner he may deem most effectual to harass and conquer and subdue the enemy." *Fleming v. Page,* 50 U.S. (9 How.) 603, 615 (1850). As Chief Justice Chase explained in 1866, although Congress has authority to legislate to support the prosecution of a war, Congress may not "*interfere[] with the command of the forces and the conduct of campaigns.* That power and duty belong to the President as commander-in-chief." *Ex parte Milligan,* 71 U.S. (4 Wall.) 2, 139 (1866) (Chase, C.J., concurring in judgment) (emphasis added).

The Executive Branch uniformly has construed the Commander in Chief and foreign affairs powers to grant the President authority that is beyond the ability of Congress to regulate. In 1860, Attorney General Black concluded that an act of Congress, if intended to constrain the President's discretion in assigning duties to an officer in the army, would be unconstitutional:

As commander-in-chief of the army it is your right to decide according to your

[14] In the past, other courts have declined to express a view on that issue one way or the other. *See, e.g., Butenko,* 494 F.2d at 601 ("We do not intimate, at this time, any view whatsoever as the proper resolution of the possible clash of the constitutional powers of the President and Congress.").

> own judgment what officer shall perform any particular duty, and as the supreme executive magistrate you have the power of appointment. Congress could not, if it would, take away from the President, or in anywise diminish the authority conferred upon him by the Constitution.

Memorial of Captain Meigs, 9 Op. Att'y Gen. 462, 468 (1860). Attorney General Black went on to explain that, in his view, the statute involved there could probably be read as simply providing "a recommendation" that the President could decline to follow at his discretion. *Id*. at 469-70.[15]

Supreme Court precedent does not support claims of congressional authority over core military decisions during armed conflicts. In particular, the two decisions of the Supreme Court that address a conflict between asserted wartime powers of the Commander in Chief and congressional legislation and that resolve the conflict in favor of Congress—*Little v. Barreme,* 6 U.S. (2 Cranch) 170 (1804), and *Youngstown Sheet & Tube Co. v. Sawyer,* 343 U.S. 579 (1952)—are both distinguishable from the situation presented by the NSA activities in the conflict with al Qaeda. Neither supports the constitutionality of the restrictions in FISA as applied here.

Barreme involved a suit brought to recover a ship seized by an officer of the U.S. Navy on the high seas during the so-called "Quasi War" with France in 1799. The seizure had been based upon the officer's orders implementing an act of Congress suspending commerce between the United States and France and authorizing the seizure of American ships bound *to* a French port. The ship in question was suspected of sailing *from* a French port. The Supreme Court held that the orders given by the President could not authorize a seizure beyond the terms of the

---

[15] Executive practice recognizes, consistent with the Constitution, some congressional control over the Executive's decisions concerning the Armed Forces. *See, e.g.*, U.S. Const. art. I, § 8, cl. 12 (granting Congress power "to raise and support Armies"). But such examples have not involved congressional attempts to regulate the actual conduct of a military campaign, and there is no comparable textual support for such interference. For example, just before World War II, Attorney General Robert Jackson concluded that the Neutrality Act prohibited President Roosevelt from selling certain armed naval vessels and sending them to Great Britain. *See Acquisition of Naval and Air Bases in Exchange for Over-Age Destroyers,* 39 Op. Att'y Gen. 484, 496 (1940). Jackson's apparent conclusion that Congress could control the President's ability to transfer war material does not imply acceptance of direct congressional regulation of the Commander in Chief's control of the means and methods of engaging the enemy in conflict. Similarly, in *Youngstown Sheet & Tube Co. v. Sawyer,* the Truman Administration readily conceded that, if Congress had prohibited the seizure of steel mills by statute, Congress's action would have been controlling. *See* Brief for Petitioner at 150, *Youngstown*, 343 U.S. 579 (1952) (Nos. 744 and 745). This concession implies nothing concerning congressional control over the methods of engaging the enemy.

Likewise, the fact that the Executive Branch has, at times, sought congressional ratification after taking unilateral action in a wartime emergency does not reflect a concession that the Executive lacks authority in this area. A decision to seek congressional support can be prompted by many motivations, including a desire for political support. In modern times, several administrations have sought congressional authorization for the use of military force while preserving the ability to assert the unconstitutionality of the War Powers Resolution. *See, e.g., Statement on Signing the Resolution Authorizing the Use of Military Force Against Iraq,* 1 Pub. Papers of George Bush 40 (1991) ("[M]y request for congressional support did not . . . constitute any change in the long-standing positions of the executive branch on either the President's constitutional authority to use the Armed Forces to defend vital U.S. interests or the constitutionality of the War Powers Resolution."). Moreover, many actions for which congressional support has been sought—such as President Lincoln's action in raising an Army in 1861—quite likely fall primarily under Congress's core Article I powers.

statute and therefore that the seizure of the ship not in fact bound *to* a French port was unlawful. *See* 6 U.S. at 177-78. Although some commentators have broadly characterized *Barreme* as standing for the proposition that Congress may restrict by statute the means by which the President can direct the Nation's Armed Forces to carry on a war, the Court's holding was limited in at least two significant ways. First, the operative section of the statute in question applied only to *American* merchant ships. *See id*. at 170 (quoting Act of February 9, 1799). Thus, the Court simply had no occasion to rule on whether, even in the limited and peculiar circumstances of the Quasi War, Congress could have placed some restriction on the orders the Commander in Chief could issue concerning direct engagements with enemy forces. Second, it is significant that the statute in *Barreme* was cast expressly, not as a limitation on the conduct of warfare by the President, but rather as regulation of a subject within the core of Congress's enumerated powers under Article I—the regulation of foreign commerce. *See* U.S. Const., art. I, § 8, cl. 3. The basis of Congress's authority to act was therefore clearer in *Barreme* than it is here.

Youngstown involved an effort by the President—in the face of a threatened work stoppage—to seize and to run steel mills. Congress had expressly considered the possibility of giving the President power to effect such a seizure during national emergencies. It rejected that option, however, instead providing different mechanisms for resolving labor disputes and mechanisms for seizing industries to ensure production vital to national defense.

For the Court, the connection between the seizure and the core Commander in Chief function of commanding the Armed Forces was too attenuated. The Court pointed out that the case did not involve authority over "day-to-day fighting in a theater of war." *Id.* at 587. Instead, it involved a dramatic extension of the President's authority over military operations to exercise control over an industry that was vital for producing equipment needed overseas. Justice Jackson's concurring opinion also reveals a concern for what might be termed foreign-to-domestic presidential bootstrapping. The United States became involved in the Korean conflict through President Truman's unilateral decision to commit troops to the defense of South Korea. The President then claimed authority, based upon this foreign conflict, to extend presidential control into vast sectors of the domestic economy. Justice Jackson expressed "alarm[]" at a theory under which "a President whose conduct of foreign affairs is so largely uncontrolled, and often even is unknown, can vastly enlarge his mastery over the internal affairs of the country by his own commitment of the Nation's armed forces to some foreign venture." *Id.* at 642.

Moreover, President Truman's action extended the President's authority into a field that the Constitution predominantly assigns to Congress. *See id*. at 588 (discussing Congress's commerce power and noting that "[t]he Constitution does not subject this lawmaking power of Congress to presidential or military supervision or control"); *see also id*. at 643 (Jackson, J., concurring) (explaining that Congress is given express authority to "'raise and *support* Armies'" and "'to *provide* and *maintain* a Navy'") (quoting U.S. Const. art. I, § 8, cls. 12, 13). Thus, *Youngstown* involved an assertion of executive power that not only stretched far beyond the

President's core Commander in Chief functions, but that did so by intruding into areas where Congress had been given an express, and apparently dominant, role by the Constitution.[16]

The present situation differs dramatically. The exercise of executive authority involved in the NSA activities is not several steps removed from the actual conduct of a military campaign. As explained above, it is an essential part of the military campaign. Unlike the activities at issue in *Youngstown*, the NSA activities are directed at the enemy, and not at domestic activity that might incidentally aid the war effort. And assertion of executive authority here does not involve extending presidential power into areas reserved for Congress. Moreover, the theme that appeared most strongly in Justice Jackson's concurrence in *Youngstown*—the fear of presidential bootstrapping—does not apply in this context. Whereas President Truman had used his inherent constitutional authority to commit U.S. troops, here Congress expressly provided the President sweeping authority to use "all necessary and appropriate force" to protect the Nation from further attack. AUMF § 2(a). There is thus no bootstrapping concern.

Finally, *Youngstown* cannot be read to suggest that the President's authority for engaging the enemy is less extensive inside the United States than abroad. To the contrary, the extent of the President's Commander in Chief authority necessarily depends on where the enemy is found and where the battle is waged. In World War II, for example, the Supreme Court recognized that the President's authority as Commander in Chief, as supplemented by Congress, included the power to capture and try agents of the enemy in the United States, even if they never had "entered the theatre or zone of active military operations." *Quirin,* 317 U.S. at 38.[17] In the present conflict, unlike in the Korean War, the battlefield was brought to the United States in the most literal way, and the United States continues to face a threat of further attacks on its soil. In short, therefore, *Youngstown* does not support the view that Congress may constitutionally prohibit the President from authorizing the NSA activities.

The second serious constitutional question is whether the particular restrictions imposed by FISA would impermissibly hamper the President's exercise of his constitutionally assigned duties as Commander in Chief. The President has determined that the speed and agility required to carry out the NSA activities successfully could not have been achieved under FISA.[18] Because the President also has determined that the NSA activities are necessary to the defense of

---

[16] *Youngstown* does demonstrate that the mere fact that Executive action might be placed in Justice Jackson's category III does not obviate the need for further analysis. Justice Jackson's framework therefore recognizes that Congress might impermissibly interfere with the President's authority as Commander in Chief or to conduct the Nation's foreign affairs.

[17] It had been recognized long before *Youngstown* that, in a large-scale conflict, the area of operations could readily extend to the continental United States, even when there are no major engagements of armed forces here. Thus, in the context of the trial of a German officer for spying in World War I, it was recognized that "[w]ith the progress made in obtaining ways and means for devastation and destruction, the territory of the United States was certainly within the field of active operations" during the war, particularly in the port of New York, and that a spy in the United States might easily have aided the "hostile operation" of U-boats off the coast. *United States ex reI. Wessels v. McDonald,* 265 F. 754, 764 (E.D.N.Y. 1920).

[18] In order to avoid further compromising vital national security activities, a full explanation of the basis for the President's determination cannot be given in an unclassified document.

the United States from a subsequent terrorist attack in the armed conflict with al Qaeda, FISA would impermissibly interfere with the President's most solemn constitutional obligation—to defend the United States against foreign attack.

Indeed, if an interpretation of FISA that allows the President to conduct the NSA activities were not "fairly possible," FISA would be unconstitutional as applied in the context of this congressionally authorized armed conflict. In that event, FISA would purport to *prohibit* the President from undertaking actions necessary to fulfill his constitutional obligation to protect the Nation from foreign attack in the context of a congressionally authorized armed conflict with an enemy that has already staged the most deadly foreign attack in our Nation's history. A statute may not "*impede* the President's ability to perform his constitutional duty," *Morrison v. Olson*, 487 U.S. 654, 691 (1988) (emphasis added); *see also id.* at 696-97, particularly not the President's most solemn constitutional obligation—the defense of the Nation. *See also In re Sealed Case*, 310 F.3d at 742 (explaining that "FISA could not encroach on the President's constitutional power").

Application of the avoidance canon would be especially appropriate here for several reasons beyond the acute constitutional crises that would otherwise result. First, as noted, Congress did not intend FISA to be the final word on electronic surveillance conducted during armed conflicts. Instead, Congress expected that it would revisit the subject in subsequent legislation. Whatever intent can be gleaned from FISA's text and legislative history to set forth a comprehensive scheme for regulating electronic surveillance during peacetime, that same intent simply does not extend to armed conflicts and declared wars.[19] Second, FISA was enacted during the Cold War, not during active hostilities with an adversary whose mode of operation is to blend in with the civilian population until it is ready to strike. These changed circumstances have seriously altered the constitutional calculus, one that FISA's enactors had already recognized might suggest that the statute was unconstitutional. Third, certain technological changes have rendered FISA still more problematic. As discussed above, when FISA was enacted in 1978, Congress expressly declined to regulate through FISA certain signals intelligence activities conducted by the NSA. *See supra*, at pp. 18-19 & n.6.[20] These same factors weigh heavily in favor of concluding that FISA would be unconstitutional as applied to the current conflict if the canon of constitutional avoidance could not be used to head off a collision between the Branches.

---

[19] FISA exempts the President from its procedures for fifteen days following a congressional declaration of war. *See* 50 U.S.C. § 1811. If an adversary succeeded in a decapitation strike, preventing Congress from declaring war or passing subsequent authorizing legislation, it seems clear that FISA could not constitutionally continue to apply in such circumstances.

[20] Since FISA's enactment in 1978, the means of transmitting communications has undergone extensive transformation. In particular, many communications that would have been carried by wire are now transmitted through the air, and many communications that would have been carried by radio signals (including by satellite transmissions) are now transmitted by fiber optic cables. It is such technological advancements that have broadened FISA's reach, not any particularized congressional judgment that the NSA's traditional activities in intercepting such international communications should be subject to FISA's procedures. A full explanation of these technological changes would require a discussion of classified information.

* * *

As explained above, FISA is best interpreted to allow a statute such as the AUMF to authorize electronic surveillance outside FISA's enumerated procedures. The strongest counterarguments to this conclusion are that various provisions in FISA and title 18, including section 111 of FISA and section 2511(2)(f) of title 18, together require that subsequent legislation must reference or amend FISA in order to authorize electronic surveillance outside FISA's procedures and that interpreting the AUMF as a statute authorizing electronic surveillance outside FISA procedures amounts to a disfavored repeal by implication. At the very least, however, interpreting FISA to allow a subsequent statute such as the AUMF to authorize electronic surveillance without following FISA's express procedures is "fairly possible," and that is all that is required for purposes of invoking constitutional avoidance. In the competition of competing canons, particularly in the context of an ongoing armed conflict, the constitutional avoidance canon carries much greater interpretative force.[21]

IV. THE NSA ACTIVITIES ARE CONSISTENT WITH THE FOURTH AMENDMENT

The Fourth Amendment prohibits "unreasonable searches and seizures" and directs that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and

---

[21] If the text of FISA were clear that nothing other than an amendment to FISA could authorize additional electronic surveillance, the AUMF would impliedly repeal as much of FISA as would prevent the President from using "all necessary and appropriate force" in order to prevent al Qaeda and its allies from launching another terrorist attack against the United States. To be sure, repeals by implication are disfavored and are generally not found whenever two statutes are "capable of co-existence." *Ruckelshaus v. Monsanto Co.,* 467 U.S. 986, 1018 (1984). Under this standard, an implied repeal may be found where one statute would "unduly interfere with" the operation of another. *Radzanower v. Touche Ross & Co.,* 426 U.S. 148, 156 (1976). The President's determination that electronic surveillance of al Qaeda outside the confines of FISA was "necessary and appropriate" would create a clear conflict between the AUMF and FISA. FISA's restrictions on the use of electronic surveillance would preclude the President from doing what the AUMF specifically authorized him to do: use all "necessary and appropriate force" to prevent al Qaeda from carrying out future attacks against the United States. The ordinary restrictions in FISA cannot continue to apply if the AUMF is to have its full effect; those constraints would "unduly interfere" with the operation of the AUMF.

Contrary to the recent suggestion made by several law professors and former government officials, the ordinary presumption against implied repeals is overcome here. *Cf.* Letter to the Hon. Bill Frist, Majority Leader, U.S. Senate, from Professor Curtis A. Bradley et al. at 4 (Jan. 9, 2006). First, like other canons of statutory construction, the canon against implied repeals is simply a presumption that may be rebutted by other factors, including conflicting canons. *Connecticut National Bank v. Germain,* 503 U.S. 249, 253 (1992); *see also Chickasaw Nation v. United States,* 534 U.S. 84, 94 (2001); *Circuit City Stores, Inc. v. Adams*, 532 U.S. 105, 115 (2001). Indeed, the Supreme Court has declined to apply the ordinary presumption against implied repeals where other canons apply and suggest the opposite result. *See Montana v. Blackfeet Tribe of Indians,* 471 U.S. 759, 765-66 (1985). Moreover, *Blackfeet* suggests that where the presumption against implied repeals would conflict with other, more compelling interpretive imperatives, it simply does not apply at all. *See* 471 U.S. at 766. Here, in light of the constitutional avoidance canon, which imposes the overriding imperative to use the tools of statutory interpretation to avoid constitutional conflicts, the implied repeal canon either would not apply at all or would apply with significantly reduced force. Second, the AUMF was enacted during an acute national emergency, where the type of deliberation and detail normally required for application of the canon against implied repeals was neither practical nor warranted. As discussed above, in these circumstances, Congress cannot be expected to work through every potential implication of the U.S. Code and to define with particularity each of the traditional incidents of the use of force available to the President.

particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. The touchstone for review of government action under the Fourth Amendment is whether the search is "reasonable." *See, e.g., Vernonia Sch. Dist. v. Acton,* 515 U.S. 646, 653 (1995).

As noted above, *see* Part I, all of the federal courts of appeals to have addressed the issue have affirmed the President's inherent constitutional authority to collect foreign intelligence without a warrant. *See In re Sealed Case,* 310 F.3d at 742. Properly understood, foreign intelligence collection in general, and the NSA activities in particular, fit within the "special needs" exception to the warrant requirement of the Fourth Amendment. Accordingly, the mere fact that no warrant is secured prior to the surveillance at issue in the NSA activities does not suffice to render the activities unreasonable. Instead, reasonableness in this context must be assessed under a general balancing approach, "'by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.'" *United States v. Knights*, 534 U.S. 112, 118-19 (2001) (quoting *Wyoming v. Houghton*, 526 U.S. 295, 300 (1999)). The NSA activities are reasonable because the Government's interest, defending the Nation from another foreign attack in time of armed conflict, outweighs the individual privacy interests at stake, and because they seek to intercept only international communications where one party is linked to al Qaeda or an affiliated terrorist organization.

A. THE WARRANT REQUIREMENT OF THE FOURTH AMENDMENT DOES NOT APPLY TO THE NSA ACTIVITIES

In "the criminal context," the Fourth Amendment reasonableness requirement "usually requires a showing of probable cause" and a warrant. *Board of Educ. v. Earls,* 536 U.S. 822, 828 (2002). The requirement of a warrant supported by probable cause, however, is not universal. Rather, the Fourth Amendment's "central requirement is one of reasonableness," and the rules the Court has developed to implement that requirement "[s]ometimes . . . require warrants." *Illinois v. McArthur*, 531 U.S. 326, 330 (2001); *see also, e.g.*, *Earls*, 536 U.S. at 828 (noting that the probable cause standard "is peculiarly related to criminal investigations and may be unsuited to determining the reasonableness of administrative searches where the Government seeks to prevent the development of hazardous conditions") (internal quotation marks omitted).

In particular, the Supreme Court repeatedly has made clear that in situations involving "special needs" that go beyond a routine interest in law enforcement, the warrant requirement is inapplicable. *See Vernonia,* 515 U.S. at 653 (there are circumstances "'when special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable'") (quoting *Griffin* v. *Wisconsin,* 483 U.S. 868, 873 (1987)); *see also McArthur,* 531 U.S. at 330 ("When faced with special law enforcement needs, diminished expectations of privacy, minimal intrusions, or the like, the Court has found that certain general, or individual, circumstances may render a warrantless search or seizure reasonable."). It is difficult to encapsulate in a nutshell all of the different circumstances the Court has found to qualify as "special needs" justifying warrantless searches. But one application in which the Court has found the warrant requirement inapplicable is in circumstances in which the Government faces

an increased need to be able to react swiftly and flexibly, or when there are at stake interests in public safety beyond the interests in ordinary law enforcement. One important factor in establishing "special needs" is whether the Government is responding to an emergency that goes beyond the need for general crime control. *See In re Sealed Case*, 310 F.3d at 745-46.

Thus, the Court has permitted warrantless searches of property of students in public schools, *see New Jersey v. T.L.O.*, 469 U.S. 325, 340 (1985) (noting that warrant requirement would "unduly interfere with the maintenance of the swift and informal disciplinary procedures needed in the schools"), to screen athletes and students involved in extracurricular activities at public schools for drug use, *see Vernonia*, 515 U.S. at 654-55; *Earls*, 536 U.S. at 829-38, to conduct drug testing of railroad personnel involved in train accidents, *see Skinner v. Railway Labor Executives' Ass'n,* 489 U.S. 602, 634 (1989), and to search probationers' homes, *see Griffin*, 483 U.S. 868. Many special needs doctrine and related cases have upheld *suspicionless* searches or seizures. *See, e.g., Illinois v. Lidster*, 540 U.S. 419, 427 (2004) (implicitly relying on special needs doctrine to uphold use of automobile checkpoint to obtain information about recent hit-and-run accident); *Earls*, 536 U.S. at 829-38 (suspicionless drug testing of public school students involved in extracurricular activities); *Michigan Dep't of State Police v. Sitz*, 496 U.S. 444, 449-55 (1990) (road block to check all motorists for signs of drunken driving); *United States* v. *Martinez-Fuerte*, 428 U.S. 543 (1976) (road block near the border to check vehicles for illegal immigrants); *cf. In re Sealed Case*, 310 F.3d at 745-46 (noting that suspicionless searches and seizures in one sense are a greater encroachment on privacy than electronic surveillance under FISA because they are not based on any particular suspicion, but "[o]n the other hand, wiretapping is a good deal more intrusive than an automobile stop accompanied by questioning"). To fall within the "special needs" exception to the warrant requirement, the purpose of the search must be distinguishable from ordinary general crime control. *See, e.g.*, *Ferguson v. Charleston*, 532 U.S. 67 (2001); *City of Indianapolis v. Edmond,* 531 U.S. 32, 41 (2000).

Foreign intelligence collection, especially in the midst of an armed conflict in which the adversary has already launched catastrophic attacks within the United States, fits squarely within the area of "special needs, beyond the normal need for law enforcement" where the Fourth Amendment's touchstone of reasonableness can be satisfied without resort to a warrant. *Vernonia*, 515 U.S. at 653. The Executive Branch has long maintained that collecting foreign intelligence is far removed from the ordinary criminal law enforcement action to which the warrant requirement is particularly suited. *See, e.g.*, Amending the Foreign Intelligence Surveillance Act: Hearings Before the House Permanent Select Comm. on Intelligence,103d Cong. 2d Sess. 62, 63 (1994) (statement of Deputy Attorney General Jamie S. Gorelick) ("[I]t is important to understand that the rules and methodology for criminal searches are inconsistent with the collection of foreign intelligence and would unduly frustrate the President in carrying out his foreign intelligence responsibilities. . . . [W]e believe that the warrant clause of the Fourth Amendment is inapplicable to such [foreign intelligence] searches."); *see also In re Sealed Case*, 310 F.3d 745. The object of foreign intelligence collection is securing information necessary to protect the national security from the hostile designs of foreign powers like al Qaeda and affiliated terrorist organizations, including the possibility of another foreign attack on the United States. In foreign intelligence investigations, moreover, the targets of surveillance

often are agents of foreign powers, including international terrorist groups, who may be specially trained in concealing their activities and whose activities may be particularly difficult to detect. The Executive requires a greater degree of flexibility in this field to respond with speed and absolute secrecy to the ever-changing array of foreign threats faced by the Nation.[22]

In particular, the NSA activities are undertaken to prevent further devastating attacks on our Nation, and they serve the highest government purpose through means other than traditional law enforcement.[23] The NSA activities are designed to enable the Government to act quickly and flexibly (and with secrecy) to find agents of al Qaeda and its affiliates—an international terrorist group which has already demonstrated a capability to infiltrate American communities without being detected—in time to disrupt future terrorist attacks against the United States. As explained by the Foreign Intelligence Surveillance Court of Review, the nature of the "emergency" posed by al Qaeda "takes the matter out of the realm of ordinary crime control." *In re Sealed Case*, 310 F.3d at 746. Thus, under the "special needs" doctrine, no warrant is required by the Fourth Amendment for the NSA activities.

B. THE NSA ACTIVITIES ARE REASONABLE

As the Supreme Court has emphasized repeatedly, "[t]he touchstone of the Fourth Amendment is reasonableness, and the reasonableness of a search is determined by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." *Knights*, 534 U.S. at 118-19 (quotation marks omitted); *see also Earls,* 536 U.S. at 829. The Supreme Court has found a search reasonable when, under the totality of the circumstances, the importance of the governmental interests outweighs the nature and quality of the intrusion on the individual's Fourth Amendment interests. *See Knights*, 534 U.S. at 118-22. Under the standard

---

[22] Even in the domestic context, the Supreme Court has recognized that there may be significant distinctions between wiretapping for ordinary law enforcement purposes and domestic national security surveillance. *See United States v. United States District Court,* 407 U.S. 297, 322 (1972) ("*Keith*") (explaining that "the focus of domestic [security] surveillance may be less precise than that directed against more conventional types of crime" because often "the emphasis of domestic intelligence gathering is on the prevention of unlawful activity or the enhancement of the Government's preparedness for some possible future crisis or emergency"); *see also United States v. Duggan*, 743 F.2d 59, 72 (2d Cir. 1984) (reading *Keith* to recognize that "the governmental interests presented in national security investigations differ substantially from those presented in traditional criminal investigations"). Although the Court in *Keith* held that the Fourth Amendment's warrant requirement does apply to investigations of purely *domestic* threats to national security—such as domestic terrorism, it suggested that Congress consider establishing a lower standard for such warrants than that set forth in Title III. *See id.* at 322-23 (advising that "different standards" from those applied to traditional law enforcement "may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of the Government for intelligence information and the protected rights of our citizens"). *Keith*'s emphasis on the need for flexibility applies with even greater force to surveillance directed at *foreign* threats to national security. *See* S. Rep. No. 95-701, at 16 ("Far more than in domestic security matters, foreign counterintelligence investigations are 'long range' and involve 'the interrelation of various sources and types of information.'") (quoting *Keith*, 407 U.S. at 322). And flexibility is particularly essential here, where the purpose of the NSA activities is to prevent another armed attack against the United States.

[23] This is not to say that traditional law enforcement has no role in protecting the Nation from attack. The NSA activities, however, are not directed at bringing criminals to justice but at detecting and preventing plots by a declared enemy of the United States to attack it again.

balancing of interests analysis used for gauging reasonableness, the NSA activities are consistent with the Fourth Amendment.

With respect to the individual privacy interests at stake, there can be no doubt that, as a general matter, interception of telephone communications implicates a significant privacy interest of the individual whose conversation is intercepted. The Supreme Court has made clear at least since *Katz v. United States,* 389 U.S. 347 (1967), that individuals have a substantial and constitutionally protected reasonable expectation of privacy that their telephone conversations will not be subject to governmental eavesdropping. Although the individual privacy interests at stake may be substantial, it is well recognized that a variety of governmental interests—including routine law enforcement and foreign-intelligence gathering—can overcome those interests.

On the other side of the scale here, the Government's interest in engaging in the NSA activities is the most compelling interest possible—securing the Nation from foreign attack in the midst of an armed conflict. One attack already has taken thousands of lives and placed the Nation in state of armed conflict. Defending the Nation from attack is perhaps the most important function of the federal Government—and one of the few express obligations of the federal Government enshrined in the Constitution. *See* U.S. Const. art. IV, § 4 ("The United States shall guarantee to every State in this Union a Republican Form of Government, *and shall protect each of them against Invasion . . . .*") (emphasis added); *The Prize Cases*, 67 U.S. (2 Black) 635, 668 (1863) ("If war be made by invasion of a foreign nation, the President is not only authorized but bound to resist force by force."). As the Supreme Court has declared, "[i]t is 'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation." *Haig v. Agee,* 453 U.S. 280, 307 (1981).

The Government's overwhelming interest in detecting and thwarting further al Qaeda attacks is easily sufficient to make reasonable the intrusion into privacy involved in intercepting one-end foreign communications where there is "a reasonable basis to conclude that one party to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda." Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence, *available at* http://www.whitehouse.gov/news/releases/2005/12/20051219-1.html (Dec. 19, 2005) (statement of Attorney General Gonzales); *cf. Edmond*, 531 U.S. at 44 (noting that "the Fourth Amendment would almost certainly permit an appropriately tailored roadblock set up to thwart an imminent terrorist attack" because "[t]he exigencies created by th[at] scenario[] are far removed" from ordinary law enforcement). The United States has already suffered one attack that killed thousands, disrupted the Nation's financial center for days, and successfully struck at the command and control center for the Nation's military. And the President has stated that the NSA activities are "critical" to our national security. Press Conference of President Bush (Dec. 19, 2005). To this day, finding al Qaeda sleeper agents in the United States remains one of the preeminent concerns of the war on terrorism. As the President has explained, "[t]he terrorists want to strike America again, and they hope to inflict even more damage than they did on September 11th." *Id.*

Of course, because the magnitude of the Government's interest here depends in part upon the threat posed by al Qaeda, it might be possible for the weight that interest carries in the balance to change over time. It is thus significant for the reasonableness of the NSA activities that the President has established a system under which he authorizes the surveillance only for a limited period, typically for 45 days. This process of reauthorization ensures a periodic review to evaluate whether the threat from al Qaeda remains sufficiently strong that the Government's interest in protecting the Nation and its citizens from foreign attack continues to outweigh the individual privacy interests at stake.

Finally, as part of the balancing of interests to evaluate Fourth Amendment reasonableness, it is significant that the NSA activities are limited to intercepting international communications where there is a reasonable basis to conclude that one party to the communication is a member or agent of al Qaeda or an affiliated terrorist organization. This factor is relevant because the Supreme Court has indicated that in evaluating reasonableness, one should consider the "efficacy of [the] means for addressing the problem." *Vernonia*, 515 U.S. at 663; *see also Earls,* 536 U.S. at 834 ("Finally, this Court must consider the nature and immediacy of the government's concerns and the efficacy of the Policy in meeting them."). That consideration does not mean that reasonableness requires the "least intrusive" or most "narrowly tailored" means for obtaining information. To the contrary, the Supreme Court has repeatedly rejected such suggestions. *See, e.g., Earls,* 536 U.S. at 837 ("[T]his Court has repeatedly stated that reasonableness under the Fourth Amendment does not require employing the least intrusive means, because the logic of such elaborate less-restrictive-alternative arguments could raise insuperable barriers to the exercise of virtually all search-and-seizure powers.") (internal quotation marks omitted); *Vernonia,* 515 U.S. at 663 ("We have repeatedly refused to declare that only the 'least intrusive' search practicable can be reasonable under the Fourth Amendment."). Nevertheless, the Court has indicated that some consideration of the efficacy of the search being implemented—that is, some measure of fit between the search and the desired objective—is relevant to the reasonableness analysis. The NSA activities are targeted to intercept international communications of persons reasonably believed to be members or agents of al Qaeda or an affiliated terrorist organization, a limitation which further strongly supports the reasonableness of the searches.

In sum, the NSA activities are consistent with the Fourth Amendment because the warrant requirement does not apply in these circumstances, which involve both "special needs" beyond the need for ordinary law enforcement and the inherent authority of the President to conduct warrantless electronic surveillance to obtain foreign intelligence to protect our Nation from foreign armed attack. The touchstone of the Fourth Amendment is reasonableness, and the NSA activities are certainly reasonable, particularly taking into account the nature of the threat the Nation faces.

CONCLUSION

For the foregoing reasons, the President—in light of the broad authority to use military force in response to the attacks of September 11th and to prevent further catastrophic attack expressly conferred on the President by the Constitution and confirmed and supplemented by

Congress in the AUMF—has legal authority to authorize the NSA to conduct the signals intelligence activities he has described. Those activities are authorized by the Constitution and by statute, and they violate neither FISA nor the Fourth Amendment.

BellingerJB@state.gov

From: BellingerJB@state.gov
Sent: Thursday, January 19, 2006 1:22 PM
To: (b)(3) 50 USC § 3024(m)(1) @dni.gov
Cc: Moschella, William; Scolinos, Tasia; Bradbury, Steve; Sampson, Kyle; Roehrkasse, Brian; Harriet_Miers@who.eop.gov; John_B._Wiegmann@nsc.eop.gov; John_M._Mitnick@who.eop.gov; (b)(3) 50 USC § 3605; Brett_C._Gerry@who.eop.gov; Raul_F._Yanes@ (b) (6) ; haynesw (b) (6) ; benjamin.powell@dni.gov; William_K._Kelley@who.eop.gov; Brett_M._Kavanaugh@who.eop.gov; Dan_Bartlett@who.eop.gov
Subject: RE: DOJ white paper on NSA activities

(b) (5) .

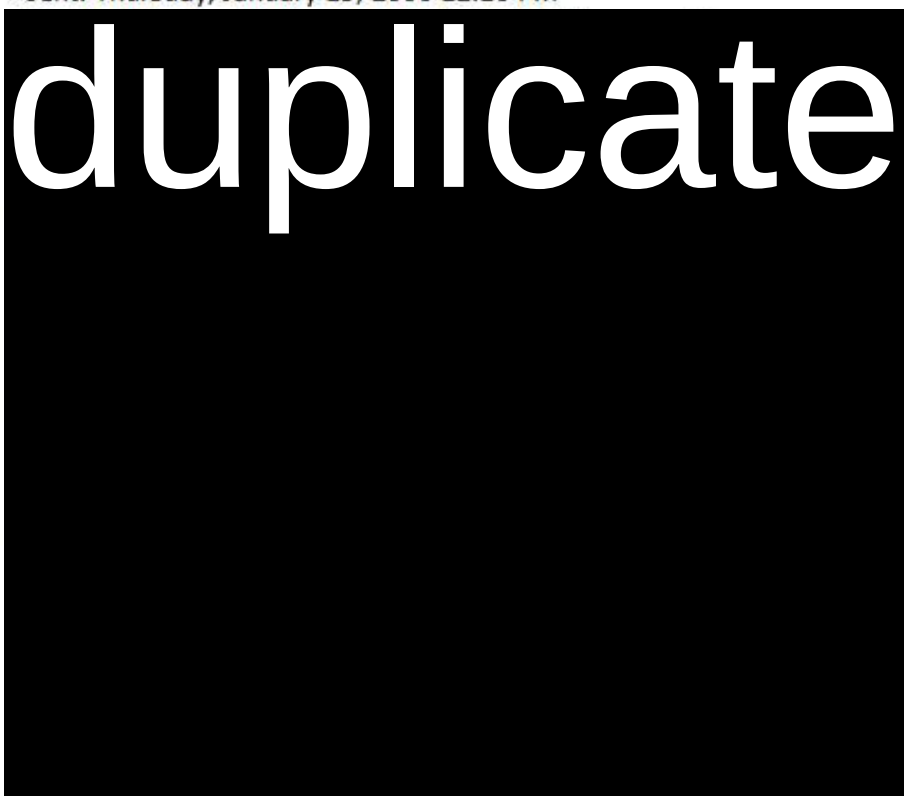
-----Original Message-----
From: Benjamin [mailto: (b)(3) 50 USC § 3024(m)(1) @dni.gov]
Sent: Thursday, January 19, 2006 1:20 PM
To: Bellinger, John B(Legal)
Cc: Steve.Bradbury@usdoj.gov; Harriet_Miers@who.eop.gov; John_B._Wiegmann@nsc.eop.gov; John_M._Mitnick@who.eop.gov; (b)(3) 50 USC § 3605; Brett_C._Gerry@who.eop.gov; Raul_F._Yanes@ (b) (6) ; haynesw (b) (6) ; benjamin.powell@dni.gov; William_K._Kelley@who.eop.gov; Brett_M._Kavanaugh@who.eop.gov; Dan_Bartlett@who.eop.gov; Kyle.Sampson@usdoj.gov; Tasia.Scolinos@usdoj.gov; William.Moschella@usdoj.gov; Brian.Roehrkasse@usdoj.gov
Subject: Re: DOJ white paper on NSA activities

John -- (b) (5) ? Ben

Bellinger, John B(Legal) wrote:

>Thanks Steve.
>
> (b) (5) .
>
(b) (5)
>
(b) (5)
>

>
>
>-----Original Message-----
>From: Steve.Bradbury@usdoj.gov [mailto:Steve.Bradbury@usdoj.gov]
>Sent: Thursday, January 19, 2006 12:16 PM



Harriet_Miers@who.eop.gov

From: Harriet_Miers@who.eop.gov
Sent: Sunday, January 22, 2006 4:31 PM
To: Brand, Rachel; Bradbury, Steve; (b)(3) 50 USC § 3024(m)(1) @dni.gov; Matthew_T._McDonald@who.eop.gov; Brett_C._Gerry@who.eop.gov; Brett_M._Kavanaugh@who.eop.gov; Brett_M._Kavanaugh@who.eop.gov
Subject: RE: comment

I will ask Matt by way of this email, (b) (5) . Perhaps we can turn the (b) (5) document around early tomorrow.

-----Original Message-----
From: Benjamin [mailto: (b)(3) 50 USC § 3024(m)(1) @dni.gov]
Sent: Sunday, January 22, 2006 4:26 PM
To: McDonald, Matthew T.; Gerry, Brett C.; rachel.brand@usdoj.gov; Miers, Harriet; Kavanaugh, Brett M.; Steve.Bradbury@usdoj.gov; Kavanaugh, Brett M.
Subject: comment

I think we can (b) (5) .

I would cite in particular the following:

(b) (5)

(b) (5)

Harriet_Miers@who.eop.gov

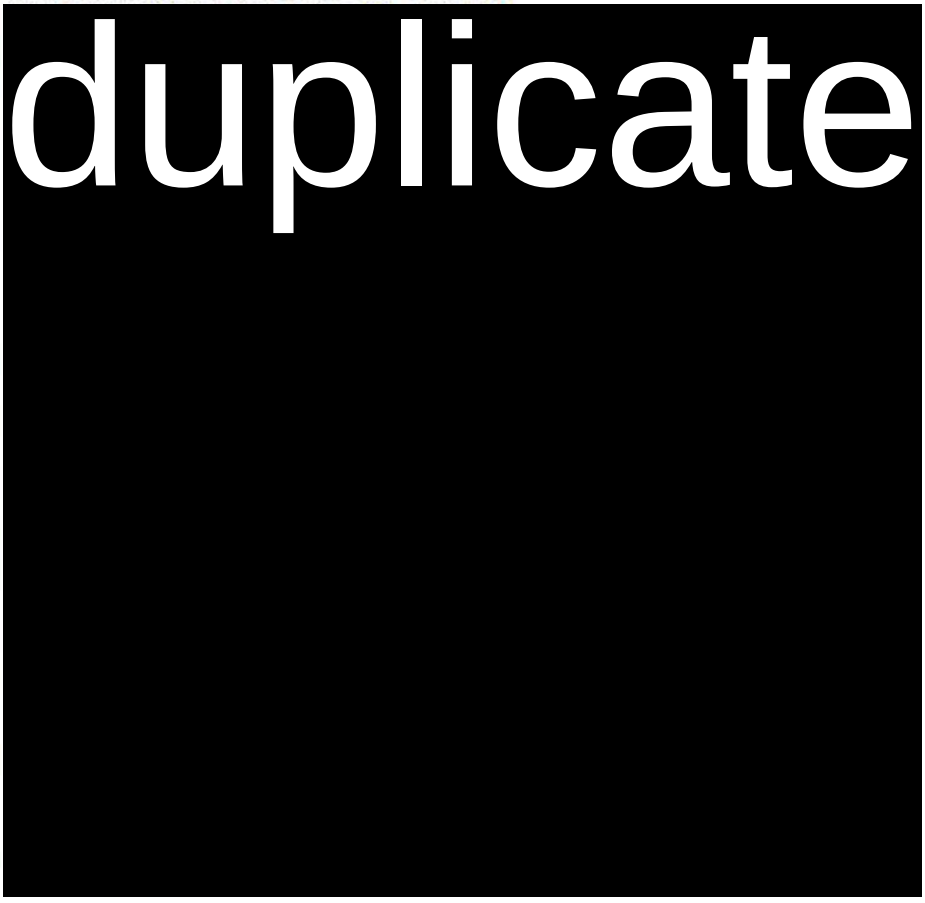
From: Harriet_Miers@who.eop.gov
Sent: Sunday, January 22, 2006 4:31 PM
To: Brand, Rachel; Bradbury, Steve; Matthew_T._McDonald@who.eop.gov; (b)(3) 50 USC § 3024(m)(1) @dni.gov; Brett_C._Gerry@who.eop.gov; Brett_M._Kavanaugh@who.eop.gov; Brett_M._Kavanaugh@who.eop.gov
Subject: RE: comment

Looks like it is ok!

-----Original Message-----
From: McDonald, Matthew T.
Sent: Sunday, January 22, 2006 4:27 PM
To: 'Benjamin'; Gerry, Brett C.; rachel.brand@usdoj.gov; Miers, Harriet; Kavanaugh, Brett M.; Steve.Bradbury@usdoj.gov; Kavanaugh, Brett M.
Subject: RE: comment

Perfect. We will add that.

-----Original Message-----
From: Benjamin [mailto:(b)(3) 50 USC § 3024(m)(1) @dni.gov]
Sent: Sunday, January 22, 2006 4:26 PM



(b)(3) 50 USC § 3024(m)(1) @dni.gov

From:	(b)(3) 50 USC § 3024(m)(1) @dni.gov
Sent:	Monday, January 23, 2006 9:26 AM
To:	Martinson, Wanda; Bradbury, Steve; Brand, Rachel; Sampson, Kyle; Elwood, Courtney; Dan_Bartlett@who.eop.gov; Brett_M._Kavanaugh@who.eop.gov; Harriet_Miers@who.eop.gov; William_K._Kelley@who.eop.gov; David_S._Addington@ovp.eop.gov; BellingerJB@state.gov; Michael_Drummond@who.eop.gov; Dana_M._Perino@who.eop.gov; Heather_M._Roebke@who.eop.gov; Michael_Allen@nsc.eop.gov; Shannen_W._Coffin@ovp.eop.gov; Brett_C._Gerry@who.eop.gov; (b)(3) 50 USC § 3024(m)(1) @dni.gov; Scott_McClellan@who.eop.gov; Matthew_T._McDonald@who.eop.gov; Christal_R._West@who.eop.gov; Candida_P._Wolff@who.eop.gov
Subject:	[Fwd: Final Version of the Speech]
Attachments:	tmp.htm; NatlPressClub--23Jan--0915.doc

final version prepared for delivery.

-------- Original Message --------
Subject: Final Version of the Speech
Date: Mon, 23 Jan 2006 09:16:26 -0500
From: (b)(3) 50 USC § 3024(m)(1) @dni.gov>
To: (b)(3) 50 USC § 3024(m)(1) @dni.gov>, (b)(3) 50 USC § 3024(m)(1) @dni.gov>, (b)(3) 50 USC § 3024(m)(1) @dni.gov>, (b)(3) 50 USC § 3024(m)(1) @dni.gov>, Benjamin Powell <benjamin.powell@dni.gov>, (b)(3) 50 USC § 3024(m)(1) @dni.gov>, (b)(3) 50 USC § 3024(m)(1) @dni.gov>

Principal Deputy Director of National Intelligence
Address to the National Press Club
23 January 2006

Good morning. I'm happy to be here to talk a bit about what American intelligence and especially NSA have been doing to defend the Nation.

I'm here today not only as Ambassador Negroponte's deputy in the Office of the Director of National Intelligence. I'm also here as the former Director of the National Security Agency, a post I took in March of 1999 and left only last spring.

Serious issues have been raised in recent weeks. And discussion of serious issues should be based on facts. There is a lot of information out there—some of it is frankly inaccurate, much of it is simply misunderstood. I'm here to tell the American people what NSA has been doing and why. And, perhaps more importantly, what it has not been doing.

Admittedly, this is a little hard to do while protecting our country's intelligence sources and methods. And people in my line of work generally don't like to talk about what they've done until it's a subject on the History Channel.

But let me make one thing very clear: as challenging as this might be, this is the speech I want to give. I much prefer being here with you today telling you about the things we have done when there hasn't been an attack on the US Homeland.

This is a far easier presentation to make than the ones I had to give four years ago—telling audiences like you *what we hadn't done* in the days and months leading up to the tragic events of September 11th. Today's story is not an easy one to tell in this kind of unclassified environment, but it is by far the brief I prefer to present.

We all have searing memories of the morning of September 11th. I know I do: making a decision to evacuate non-essential workers at NSA while the situation was still unclear; seeing the NSA counter terrorist shop in tears while black out curtains were being stapled to walls around their windows; like many of you, asking my wife to find our kids and then hanging up the phone on her.

Another memory comes from two days later when I addressed the NSA workforce to lay out our mission in a new environment. It was a short video talk beamed throughout our headquarters at Fort Meade and globally. Most of what I said was what anyone would expect. I tried to inspire. Our work was important and the Nation was relying on us. I tried to comfort. Look on the bright side I said to them: right now a quarter billion Americans wished they had your job…being able to go after the enemy. I ended the talk by trying to give perspective. I noted that all free peoples have had to balance the demands of

liberty with the demands of security. Historically we Americans had planted our flag well down the spectrum toward liberty. Here was our challenge. "We were going to keep America free," I said, "by making Americans feel safe again."

But to start the story with that Thursday, September 13th is misleading, because it is really near the end of the first reel of this movie. To understand that moment and that statement, you would have to know a little bit about what had happened to the National Security Agency in the preceding years.

NSA intercepts communications and it does so for only one purpose: to protect the lives, the liberties and the well being of the citizens of the United States from those who would do us harm. By the late 1990s, that job was becoming increasingly more difficult. The explosion of modern communications in terms of volume, variety and velocity threatened to overwhelm us.

The Agency took a lot of criticism in those days—that it was going deaf; that it was ossified in its thinking; that it had not and could not keep up with the changes in modern communications. All that was only reinforced when all the computer systems at Fort Meade went dark for three days in January of 2000 and we couldn't quickly or easily explain why.

Those were interesting times. As we were being criticized for being incompetent and going deaf, others seemed to be claiming that we were omniscient and reading your e-mails.

The Washington Post and New Yorker Magazine during that time incorrectly wrote that, "NSA has turned from eavesdropping on the Communists to eavesdropping on businesses and private citizens," and that, "NSA has the ability to extend its eavesdropping network without limits." We were also referred to as "a global spying network that can eavesdrop on every single phone call, fax, or e-mail, anywhere on the planet."

I used those quotes in a speech I gave at American University in February 2000. The great "urban legend" then was something called Echelon and the false accusation that NSA was using its capabilities to advance American corporate interests: signals intelligence for General Motors or something like that. With these kinds of charges, the turf back then feels familiar now: how could we prove a negative (that we weren't doing certain things) without revealing the appropriate things we were doing that kept America safe.

You see, NSA had (and has) an existential problem. In order to protect American lives and liberties it has to be two things: powerful in its capabilities and secretive in its methods. And we exist in a political culture that distrusts two things most of all: power and secrecy.

Modern communications didn't make this any easier. Gone were the days when "signals of interest" went along a dedicated microwave link between strategic rocket forces headquarters in Moscow to an ICBM base in western Siberia. By the late nineties, what NSA calls "targeted communications"—things like al Qa'ida communications—co-existed out there in a great global web with your phone calls and my e-mails. NSA needed the power to pick out the one and the discipline to leave the others alone.

So this question of security and liberty wasn't a new one for us in September 2001. We always have had this question: how do we balance the legitimate need for foreign intelligence with our responsibility to protect individual privacy rights? It is a question drilled into every employee of NSA from day one, and it shapes every decision about how NSA operates.

September 11th didn't change that. But it did change some things.

This ability to intercept communications, commonly referred to as Signals Intelligence (SIGINT), is a complex business with operational, technological and legal imperatives often intersecting and overlapping. There is routinely some freedom of action—within the law—to adjust operations. After the attacks I exercised some options I always had that collectively better prepared us to defend the Homeland.

Let me talk about this for a minute. Because a big gap in understanding is what's standard—what does NSA do routinely?

Where we set the threshold for what constituted "inherent foreign intelligence value" in reports involving a US person, for example, shapes the level of some of our collection and reporting. The American SIGINT system in the normal course of its foreign intelligence activities inevitably captures this kind of information—information to, from or about what we call a US person (by the way, that routinely includes anyone in the United States, citizen or not.) So, for example, because they were in the United States Mohammad Atta and his fellow 18 hijackers were presumed to be protected persons.

"Inherent foreign intelligence value" is one of the metrics we must use to ensure that we conform to the 4th Amendment's "reasonableness" standard when it comes to protecting the privacy of that person. If the US person information isn't relevant, the data is suppressed or what we call minimized. The individual is not mentioned, or if he is, he is referred to as US person number one. If the US person is actually the named terrorist, well, that could be a different matter.

The standard by which we decided that—the standard of what was relevant and valuable, and therefore what was reasonable—would understandably change as smoke billowed from two American cities and a Pennsylvania farm field, and we acted accordingly. To somewhat oversimplify

the question of inherent intelligence value—to just use an example—we had a different view of Zacarias Moussaoui's computer hard drive after the attacks than we had before.

This is not unlike what happened in other areas. Prior to September 11th airline passengers were screened in one way. After September 11th, we changed how we screened passengers. Similarly, although prior to September 11th certain communications weren't considered valuable intelligence, it became immediately clear after September 11 that intercepting and reporting these same communications were, in fact, critical to defending the homeland.

These decisions were easily within my authorities as Director of NSA under an executive order, known as Executive Order 12333, that was signed in 1981—an Executive Order that has governed NSA for nearly a quarter century.

Let me summarize: in the days after 9-11, NSA was using used its authorities and its judgment to appropriately respond to the most catastrophic attack on the Homeland in the history of the Nation.

That shouldn't be a headline, but as near as I can tell, these actions on my part have created some of the noise in recent press coverage. Let me be clear on this point--except that they involved NSA, these programs were not related to the authorization that the President has recently talked about. I asked to update the Congress on what NSA had been doing and I briefed the entire House Intelligence Committee on the 1st of October 2001 on what we had done under NSA's previously existing authorities.

As part of our adjustments, we also turned on the spigot of NSA reporting to FBI in an unprecedented way. We found that we were giving them too much data in too raw a form. We recognized it almost immediately—a question of weeks—and made adjustments.

This flow of data to the FBI has also become part of the current background noise. Despite reports in the press of "thousands of tips a month," our reporting has not even approached that kind of pace.

I actually find all of this a little odd. After all the findings of the 9-11 Commission and other bodies about the failure to *share* intelligence, I'm up here feeling like I have to explain pushing data to those who might be able to use it.

And it is the nature of intelligence that many tips lead nowhere but you have to go down some blind alleys to find the tips that pay off.

Beyond the authorities that I exercised under the standing executive order, as the war on terror has moved forward we have aggressively used FISA warrants. The Act and the Court have provided us with important tools and we

make full use of them. Published numbers show us using the Court at record rates and the results have been outstanding.

But the revolution in telecommunications technology has extended the actual impact of the FISA regime far beyond what Congress could ever have anticipated in 1978. And I don't think that anyone could make the claim that the FISA statute is optimized to deal with a 9/11 or to deal with a lethal enemy who likely already had combatants inside the United States.

I testified in open session to the House Intelligence Committee in April of the year 2000. At the time I created some looks of disbelief when I said that if Usama bin Ladin crossed the bridge from Niagara Falls, Ontario to Niagara Falls, New York, there were provisions of US law that would kick in, offer him protections and affect how NSA could now cover him. At the time I was just using this as a stark hypothetical. Seventeen months later this was about life and death.

So we now come to one additional piece of NSA's authorities: these are the activities whose existence the President confirmed several weeks ago. The authorization was based on an intelligence community assessment of a serious and continuing threat to the homeland. The lawfulness of the actual authorization was reviewed by lawyers at the Department of Justice and the White House and was approved by the Attorney General.

There is a certain sense of sufficiency here: authorized by the President, duly ordered, its lawfulness attested to by the Attorney General, and its content briefed to the Congressional leadership.

But we all have a personal responsibility. And in the end, NSA would have to implement this--and every operational decision the Agency makes is made with the full involvement of its legal office.

NSA professional career lawyers—and the Agency has a lot of them—have a well-deserved reputation. They're good. They know the law. And they don't let the Agency take many close pitches.

And so, even though I knew that program had been reviewed by the White House and the Department of Justice, I asked the three most senior and experienced lawyers in NSA. Our enemy in the global war on terrorism doesn't divide the United States from the rest of the world. The global telecommunications system doesn't make that distinction either. Our laws do—and should. How did these activities square with these facts? They reported back that they supported the lawfulness of the program—supported, not acquiesced. This was very important to me.

A veteran NSA lawyer, now retired, told me that a correspondent had suggested to him recently that all of the lawyers connected with this program had been very careful from the outset because they knew there would be a "day of reckoning." The NSA lawyer replied that that had not been the case. NSA had been so careful, he said—and I'm using his words here--because in this very focused, limited program NSA had to ensure that it dealt with privacy interests in an appropriate manner.

In other words, our lawyers weren't careful out of fear. They were careful out of a heartfelt and principled view that NSA operations had to be consistent with bedrock legal protections.

In early October 2001 I gathered key members of the NSA work force in our conference room and introduced our new operational authorities to them. With the historic culture at NSA being what it was (and is), I had to do this personally. I told them what we were going to do and why. I also told them that we were going to carry out the program and not go one step further. NSA's legal and operational leadership then went into the details of our new task.

The 9-11 Commission criticized our ability to link things happening in the United States with things that were happening elsewhere. In that light, there are no communications more important to the safety of the Homeland than those affiliated with al Qa'ida with one end in the United States. The President's authorization allows us to track this kind of call more comprehensively and more efficiently.

The trigger is quicker and a bit softer than it is for a FISA warrant but the intrusion into privacy is also limited—only international calls and only those we have a reasonable basis to believe involve al Qa'ida or one of its affiliates. The purpose of all of this is not to collect reams of intelligence but to detect and prevent attacks.

The Intelligence Community has neither the time, the resources, nor the legal authority to read communications that aren't likely to protect us, and NSA has no interest in doing so.

These are communications that we have reason to believe are al Qa'ida communications, a judgment made by the American intelligence professionals (not political appointees) most trained to understand al Qa'ida tactics, communications and aims.

Their work is actively overseen by the most intense oversight regime in the history of the National Security Agency. The Agency's conduct of the program is thoroughly reviewed by the NSA's General Counsel and Inspector General. The program has also been reviewed by the Department of Justice for compliance with the President's authorization.

Oversight also includes an aggressive training program to ensure that all activities are consistent with the letter and intent of the authorization and with the preservation of civil liberties.

Let me also talk for a minute about what this program is not. It is not a driftnet over Dearborn or Lackawanna or Fremont grabbing conversations that we then sort out by these alleged keyword searches or data mining tools or other devices that so-called experts keep talking about. This is targeted and focused.

This is not about intercepting conversations between people in the United States. This is *hot pursuit* of communications entering or leaving the United States involving someone we believe is associated with al Qa'ida.

We bring to bear all the technology we can to ensure that this is so. And if there were an anomaly and we discovered there had been an inadvertent intercept of a domestic-to-domestic call, that intercept would be destroyed and not reported but the incident—the inadvertent collection—would be recorded and reported. But that's a normal NSA procedure—for at least a quarter century.

And, as we always do when dealing with US person information, US identities are expunged when they are not essential to understanding the intelligence value of reports. Again, that's a normal NSA procedure.

So let me make this clear. When you are talking to your daughter away at State college, this program *cannot* intercept your conversations. And when she takes a semester abroad to complete her Arabic studies, this program *will* not intercept your conversations.

Let me emphasize one more thing that this program is not. Look, I know how hard it is to write a headline that is accurate, short and grabbing. But we should really shoot for all three attributes.

"Domestic Spying" doesn't really make it. One end of any call targeted under this program is always outside the United States. I have flown a lot in this country and I've taken hundreds of *domestic* flights. I have never boarded a domestic flight in this country and landed in Waziristan.

In the same way—and I am speaking illustratively here—if NSA had intercepted al Qa'ida ops chief Khalid Sheik Mohammed in Karachi talking to Mohammed Atta in Laurel, Maryland in say July of 2001…if NSA had done that and the results had been made public, I'm convinced that the crawler on all the 7/24 news networks would not have been: NSA domestic spying!

Had this program been in effect prior to 9-11, it is my professional judgment that we would have detected some of the 9-11 al Qa'ida operatives in the United States, and we would have identified them as such.

I've said earlier that this program has been successful. Clearly not every lead pans out, from this or any other source, but this program has given us information that we would not otherwise have been able to get. It's impossible for me to talk about this more in any public way without alerting our enemies to our tactics or what we have learned. I can't give details without increasing the danger to Americans. On one level I wish that I could, but I can't.

Our enemy has made his intentions clear. He has declared war on us. Since September 11th al Qa'ida and its affiliates have continued to announce their intention and continue to act on their clearly stated goal of attacking America. They have succeeded against our friends in London, Madrid, Bali, Amman, Istanbul and elsewhere. They desperately want to succeed against us.

The 9-11 Commission told us that "Bin Laden and Islamist terrorists mean exactly what they say: to them America is the font of all evil, the 'head of the snake', and it must be converted or destroyed." Bin Laden reminded us of this intention as recently as last Thursday.

The people at NSA, and the rest of the Intelligence Community, are committed to defend us against this evil and to do it in a way consistent with our values.

[We know that we can only do our jobs if we have the trust of the American people. And we can only have your trust if we are careful about how we use our tools and resources. That sense of care is part of the fabric of the intelligence community—it helps defines who we are.]

I recently went out to Fort Meade to talk to the work force involved in this program. They know what they have contributed and they know the care with which it has been done. Even in today's heated environment, the only concern expressed to me was continuing their work in the defense of the nation, and doing so in a manner that honors the law and the Constitution.

As I was talking with them I looked out over their heads to see a large sign fixed to one of the pillars that breaks up their office space. The sign is visible from almost all of the work area. It's yellow with bold black letters. The title is readable from 50 feet: "What Constitutes a US Person." And that is followed by an explanation of the criteria.

That has always been the fundamental tenet of privacy for NSA. And here it was, in the center of a room, guiding the actions of a workforce determined to prevent another attack on the United States.

Security and liberty. The people at NSA know what their job is.

I know what my job is, too. I learned a lot from NSA and its culture during my time there. But I come from a culture, too. I have been a military officer for nearly 37 years and from the start I have taken an oath to protect and defend the Constitution of the United States. I would never violate that Constitution nor would I abuse the rights of the American people. As Director I was the one responsible to ensure that this program was limited in its scope and disciplined in its application.

American intelligence and especially American SIGINT is the front line of defense in dramatically changed circumstances, circumstances in which—if we fail to do our job well and completely—more Americans will almost certainly die. The speed of operations, the ruthlessness of our enemy, the pace of modern communications has called on us to do things and do them in ways never before required. We have worked hard to find innovative ways to protect the American people and the liberties we hold dear. And in doing so we have not forgotten who we are.

final version prepared for delivery.

duplicate

(b)(3) 50 USC § 3024(m)(1) **@dni.gov**

From: (b)(3) 50 USC § 3024(m)(1) @dni.gov
Sent: Monday, January 23, 2006 7:37 PM
To: Bradbury, Steve; Sampson, Kyle; Brett_C._Gerry@who.eop.gov; Brett_M._Kavanaugh@who.eop.gov; William_K._Kelley@who.eop.gov; Harriet_Miers@who.eop.gov; David_S._Addington@ovp.eop.gov
Subject: know AG speech is being revised (b) (5)

one point that I think may resonate in a speech is (b) (5)

So one "take away" could be (b) (5)

just a thought for your consideration. . . no response needed..

Bradbury, Steve

From:	Bradbury, Steve
Sent:	Monday, January 23, 2006 9:50 PM
To:	'(b)(3) 50 USC § 3024(m)(1), (b)(6)'; Sampson, Kyle; Elwood, Courtney; Scolinos, Tasia
Cc:	(b)(3) 50 USC § 3024(m)(1) @dni.gov; (b)(3) 50 USC § 3024(m)(1) @dni.gov; (b)(3) 50 USC § 3024(m)(1) @dni.gov; (b)(3) 50 USC § 3024(m)(1) @dni.gov; Brett_C._Gerry@who.eop.gov; (b)(6) Michael Hayden (personal); (b)(3) 50 USC § 3024(m)(1) @dni.gov; 'Brett_M._Kavanaugh@who.eop.gov'; Dan_Bartlett@who.eop.gov; Moschella, William; McNeil, Tucker (OPA); Nichols, Grant W; Bradbury, Steve
Subject:	Draft 7 of AG speech
Attachments:	NSA Speech Draft 7_1 23pm.doc

Here's the new version of the AG's speech, incorporating all comments, including AG and WH comments, received by 9:45 pm. Very important for General Hayden to review closely and provide any comments he may have, if possible, by 8:00 am. The AG is scheduled to give the speech at 10:30 in the morning. Thx

(b)(6) Michael Hayden (personal)

From: (b)(6) Michael Hayden (personal)

Sent: Monday, January 23, 2006 10:26 PM

To: Scolinos, Tasia; Bradbury, Steve; Sampson, Kyle; Elwood, Courtney; (b)(3) 50 USC § 3024(m)(1), (b)(6)

Cc: Moschella, William; McNeil, Tucker (OPA); Nichols, Grant W; (b)(3) 50 USC § 3024(m)(1)@dni.gov; (b)(3) 50 USC § 3024(m)(1)@dni.gov; (b)(3) 50 USC § 3024(m)(1)@dni.gov; (b)(3) 50 USC § 3024(m)(1)@dni.gov; Dan_Bartlett@who.eop.gov; Brett_M._Kavanaugh@who.eop.gov; Brett_C._Gerry@who.eop.gov

Subject: Re: Draft 7 of AG speech

Attachments: tmp.htm

Got it. I'll take a look.

MVH

Got it. I'll take a look.

MVH

(b)(3) 50 USC § 3024(m)(1) @dni.gov

From: (b)(3) 50 USC § 3024(m)(1) @dni.gov
Sent: Tuesday, January 24, 2006 12:02 AM
To: Bradbury, Steve; (b)(3) 50 USC § 3024(m)(1), (b)(6)
Cc: McNeil, Tucker (OPA); Nichols, Grant W; (b)(3) 50 USC § 3024(m)(1) @dni.gov; (b)(3) 50 USC § 3024(m)(1) @dni.gov; (b)(3) 50 USC § 3024(m)(1) @dni.gov; Brett_M._Kavanaugh@who.eop.gov; Brett_C._Gerry@who.eop.gov
Subject: Re: Draft 7 of AG speech

Steve - looks good to me. A few very minor nits I can provide in morning and you probably will have already caught them anyways.

Have not spoken to general about draft 7 so this does not reflect his input.

----- Original Message -----
From: "Steve.Bradbury@usdoj.gov" [Steve.Bradbury@usdoj.gov]
Sent: 01/23/2006 09:50 PM

duplicate

Bradbury, Steve

From:	Bradbury, Steve
Sent:	Tuesday, January 24, 2006 10:05 AM
To:	'Harriet_Miers@who.eop.gov'; 'Brett_C._Gerry@who.eop.gov'; 'Brett_M._Kavanaugh@who.eop.gov'
Cc:	'Benjamin.Powell@DNI.gov'; 'William_K._Kelley@who.eop.gov'
Subject:	Fw: AS PREPARED FOR DELIVERY: NSA Speech
Attachments:	NSA Speech - as prepared for delivery.doc
Importance:	High

-----Original Message-----
From: Nichols, Grant W <Grant.W.Nichols@SMOJMD.USDOJ.gov>
To: Sampson, Kyle <Kyle.Sampson@SMOJMD.USDOJ.gov>; Elwood, Courtney <Courtney.Elwood@SMOJMD.USDOJ.gov>; Roper, Matt M <Matt.M.Roper@SMOJMD.USDOJ.gov>; Nowacki, John <John.Nowacki@SMOJMD.USDOJ.gov>; Peterson, Evan <Evan.Peterson@SMOJMD.USDOJ.gov>; Bradbury, Steve <Steve.Bradbury@SMOJMD.USDOJ.gov>
CC: Scolinos, Tasia <Tasia.Scolinos@SMOJMD.USDOJ.gov>; Roehrkasse, Brian <Brian.Roehrkasse@SMOJMD.USDOJ.gov>; McNeil, Tucker (OPA) <Tucker.McNeil@SMOJMD.USDOJ.gov>; Sours, Raquel <Raquel.Sours@SMOJMD.USDOJ.gov>
Sent: Tue Jan 24 09:51:00 2006
Subject: AS PREPARED FOR DELIVERY: NSA Speech

Topic: NSA Speech
Date: Tuesday, January 24, 2006 -- 10:30 AM

Please let me know if you have any questions. Thank you.

Grant
(202) 514-5611 - office
(b) (6) - cell

PREPARED REMARKS FOR
ATTORNEY GENERAL ALBERTO R. GONZALES
AT
THE GEORGETOWN UNIVERSITY LAW CENTER

"Intercepting Al Qaeda: A Lawful and Necessary Tool for Protecting America"

WASHINGTON, D.C.
TUESDAY, JANUARY 24th, 2006

Thank you, Dean.

Just after dawn on September 11th, 2001, I flew out of Dulles Airport less than an hour before the departure from the same airport of American Airlines Flight 77, the plane that was hijacked and crashed into the Pentagon later that morning. When I arrived in Norfolk, Virginia, to give a speech, the North Tower of the World Trade Center had been hit. By the end of my remarks, both the North and South Towers stood shrouded in smoke and flames with many desperate people jumping to their deaths, some 90 stories below. I spent much of the rest of that horrible day trying to get back to Washington to assist the President in my role as White House Counsel.

Everyone has a story from that morning. Up and down the East Coast, men and women were settling into their desks, coming home from a graveyard shift, or taking their children to school. And across the rest of the country, Americans were waking up to smoldering ruins and the images of ash covered faces. We remember where we were, what we were doing … and how we felt on that terrible morning, as 3,000 innocent men, women, and children died, without warning, without being able

to look into the faces of their loved ones and say goodbye . . . all killed just for being Americans.

The open wounds so many of us carry from that day are the backdrop to the current debate about the National Security Agency's terrorist surveillance program. This program, described by the President, is focused on international communications where experienced intelligence experts have reason to believe that at least one party to the communication is a member or agent of al Qaeda or a terrorist organization affiliated with al Qaeda. This program is reviewed and reauthorized by the President approximately every 45 days. The leadership of Congress, including the leaders of the Intelligence Committees of both Houses of Congress, have been briefed about this program more than a dozen times since 2001.

A word of caution here. This remains a highly classified program. It remains an important tool in protecting America. So my remarks today speak only to those activities confirmed publicly by the President, and not to other purported activities described in press reports. These press accounts are in almost every case, in one way or another, misinformed, confusing, or wrong. And unfortunately, they have caused concern over the potential breadth of what the President has actually authorized.

It seems that everyone who has heard of the President's actions has an opinion – as well we should regarding matters of national security, separation of powers, and civil liberties. Of course, a few critics are interested only in political gains. Other doubters hope the President will do everything he can to protect our country, but they worry about the appropriate checks upon a Commander in Chief's ability to monitor the enemy in a time of war.

Whatever your opinion, this much is clear: No one is above the law. We are all bound by the Constitution, and no matter the pain and anger we feel from the attacks, we must all abide by the Constitution. During my confirmation hearing, I said that, quote, "we are very, very mindful of Justice O'Connor's statement in the 2004 Hamdi decision that a state of war is not a blank check for the President of the United States with respect to the rights of American citizens. I understand that and I agree with that." Close quote. The President takes seriously his obligations to protect the American people and to protect the Constitution, and he is committed to upholding both of those obligations.

I've noticed that through all of the noise on this topic, very few have asked that the terrorist surveillance program be stopped. The American people are, however, asking two important questions: Is this program necessary? And is it lawful? The answer to each is yes.

****

The question of necessity rightly falls to our nation's military leaders. You've heard the President declare: We are a nation at war.

And in this war, our military employs a wide variety of tools and weapons to defeat the enemy. General Mike Hayden, Principal Deputy Director of National Intelligence and former Director of the NSA, laid out yesterday why a terrorist surveillance program that allows us to quickly collect important information about our enemy is so vital and necessary to the War on Terror.

The conflict against al Qaeda is, in fundamental respects, a war of information. We cannot build walls thick enough, fences high enough, or systems strong enough to keep our enemies out of our open and welcoming country. Instead, as the bipartisan 9/11 and WMD Commissions have urged, we must understand better who they are and what they're doing – we have to collect more dots, if you will, before we can "connect the dots." This program to surveil al Qaeda is a necessary weapon as we fight to detect and prevent another attack before it happens. I feel confident that is what the American people expect … and it's what the terrorist surveillance program provides.

As General Hayden explained yesterday, many men and women who shoulder the daily burden of preventing another terrorist attack here at home are convinced of the necessity of this surveillance program.

****

Now, the legal authorities. As Attorney General, I am primarily concerned with the legal basis for these necessary military activities. I expect that as lawyers and law students, you are too.

The Attorney General of the United States is the chief legal advisor for the Executive Branch. Accordingly, from the outset, the Justice Department thoroughly examined this program against al Qaeda, and concluded that the President is acting within his power in authorizing it. These activities are lawful. The Justice Department is not alone in reaching that conclusion. Career lawyers at the NSA and the NSA's Inspector General have

been intimately involved in reviewing the program and ensuring its legality.

The terrorist surveillance program is firmly grounded in the President's constitutional authorities. No other public official – no mayor, no governor, no member of Congress -- is charged by the Constitution with the primary responsibility for protecting the safety of all Americans – and the Constitution gives the President all authority necessary to fulfill this solemn duty.

It has long been recognized that the President's constitutional powers include the authority to conduct warrantless surveillance aimed at detecting and preventing armed attacks on the United States. Presidents have uniformly relied on their inherent power to gather foreign intelligence for reasons both diplomatic and military, and the federal courts have consistently upheld this longstanding practice.

If this is the case in ordinary times, it is even more so in the present circumstances of our armed conflict with al Qaeda and its allies. The terrorist surveillance program was authorized in response to the deadliest foreign attack on American soil, and it is designed solely to prevent the next attack. After all, the goal of our enemy is to blend in with our civilian population in order to plan and carry out future attacks within America. We cannot forget that the 9/11 hijackers were in our country, living in our communities.

The President's authority to take military action—including the use of communications intelligence targeted at the enemy—does not come merely from his inherent constitutional powers. It comes directly from Congress as well.

Just a few days after the events of September 11th, Congress enacted a joint resolution to support and authorize a military response to the attacks on American soil. In this resolution, the Authorization for Use of Military Force, Congress did two important things. First, it expressly recognized the President's "authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States." Second, it supplemented that authority by authorizing the President to, quote, "use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks" in order to prevent further attacks on the United States.

The Resolution means that the President's authority to use military force against those terrorist groups is at its maximum because he is acting with the express authorization of Congress. Thus, were we to employ the three-part framework of Justice Jackson's concurring opinion in the Youngstown Steel Seizure case, the President's authority falls within Category One, and is at its highest. He is acting "pursuant to an express or implied authorization of Congress," and the President's authority "includes all that he possesses in his own right [under the Constitution] plus all that Congress can" confer on him.

In 2004, the Supreme Court considered the scope of the Force Resolution in the Hamdi case. There, the question was whether the President had the authority to detain an American citizen as an enemy combatant for the duration of the hostilities.

In that case, the Supreme Court confirmed that the expansive language of the Resolution —"*all* necessary and appropriate force"—ensures that the congressional

authorization extends to traditional incidents of waging war. And, just like the detention of enemy combatants approved in *Hamdi*, the use of communications intelligence to prevent enemy attacks is a fundamental and well-accepted incident of military force.

This fact is borne out by history. This Nation has a long tradition of wartime enemy surveillance—a tradition that can be traced to George Washington, who made frequent and effective use of secret intelligence, including the interception of mail between the British and Americans.

And for as long as electronic communications have existed, the United States has conducted surveillance of those communications during wartime—all without judicial warrant. In the Civil War, for example, telegraph wiretapping was common, and provided important intelligence for both sides. In World War I, President Wilson ordered the interception of all cable communications between the United States and Europe; he inferred the authority to do so from the Constitution and from a general congressional authorization to use military force that did not mention anything about such surveillance. So too in World War II; the day after the attack on Pearl Harbor, President Roosevelt authorized the interception of all communications traffic into and out of the United States. The terrorist surveillance program, of course, is far more focused, since it involves only the interception of international communications that are linked to al Qaeda or its allies.

Some have suggested that the Force Resolution did not authorize intelligence collection inside the United States. That contention cannot be squared with the reality of the 9/11 attacks, which gave rise to the Resolution, and with the language of the

authorization itself, which calls on the President to protect Americans both "at home and abroad" and to take action to prevent further terrorist attacks "against the United States." It's also contrary to the history of wartime surveillance, which has often involved the interception of enemy communications into and out of the United States.

Against this backdrop, the NSA's focused terrorist surveillance program falls squarely within the broad authorization of the Resolution even though, as some have argued, the Resolution does not expressly mention surveillance. The Resolution also doesn't mention detention of enemy combatants. But we know from the Supreme Court's decision in *Hamdi* that such detention is authorized. Justice O'Connor reasoned: "Because detention to prevent a combatant's return to the battlefield is a fundamental incident of waging war…Congress has clearly and unmistakably authorized detention in the narrow circumstances considered here."

As Justice O'Connor recognized, it does not matter that the Force Resolution nowhere specifically refers to the detention of U.S. citizens as enemy combatants. Nor does it matter that individual Members of Congress may not have specifically intended to authorize such detention. The same is true of electronic surveillance. It is a traditional incident of war and, thus, as Justice O'Connor said, it is "of no moment" that the Resolution does not explicitly mention this activity.

These omissions are not at all surprising. In enacting the Force Resolution, Congress made no attempt to catalog every aspect of the use of force it was authorizing.

Instead, following the model of past military force authorizations, Congress—in general, but broad, terms—confirmed the President's authority to use all traditional and legitimate incidents of military force to identify and defeat the enemy. In doing so, Congress must be understood to have intended that the use of electronic surveillance against the enemy is a fundamental component of military operations.

****

Some contend that even if the President has constitutional authority to engage in the surveillance of our enemy in a time of war, that authority has been constrained by Congress with the passage in 1978 of the Foreign Intelligence Surveillance Act. Generally, FISA requires the government to obtain an order from a special FISA court before conducting electronic surveillance. It is clear from the legislative history of FISA that there were concerns among Members of Congress about the constitutionality of FISA itself.

For purposes of this discussion, because I cannot discuss operational details, I'm going to assume here that intercepts of al Qaeda communications under the terrorist surveillance program fall within the definition of "electronic surveillance" in FISA.

The FISA Court of Review, the special court of appeals charged with hearing appeals of decisions by the FISA court, stated in 2002 that, quote, "[w]e take for granted that the President does have that [inherent] authority" and, "assuming that is so, FISA could not encroach on the President's constitutional power." We do not have to decide whether, when we are at war and there is a vital need for the terrorist

surveillance program, FISA unconstitutionally encroaches – or places an unconstitutional constraint upon – the President's Article II powers. We can avoid that tough question because Congress gave the President the Force Resolution, and that statute removes any possible tension between what Congress said in 1978 in FISA and the President's constitutional authority today.

Let me explain by focusing on certain aspects of FISA that have attracted a lot of attention and generated a lot of confusion in the last few weeks.

First, FISA, of course, allows Congress to respond to new threats through separate legislation. FISA bars persons from intentionally "engag[ing] . . . in electronic surveillance under color of law *except as authorized by statute*." For the reasons I have already discussed, the Force Resolution provides the relevant statutory authorization for the terrorist surveillance program. *Hamdi* makes it clear that the broad language in the Resolution can satisfy a requirement for specific statutory authorization set forth in another law.

***Hamdi* involved a statutory prohibition on all detention of U.S. citizens except as authorized "pursuant to an Act of Congress." Even though the detention of a U.S. citizen involves a deprivation of liberty, and even though the Force Resolution says nothing on its face about detention of U.S. citizens, a majority of the members of the Court nevertheless concluded that the Resolution satisfied the statutory requirement. The same is true, I submit, for the prohibition on warrantless electronic surveillance in FISA.**

You may have heard about the provision of FISA that allows the President to conduct warrantless surveillance for 15 days following a declaration of war. That provision shows that Congress knew that warrantless surveillance would be essential in wartime. But no one could reasonably suggest that all such critical military surveillance in a time of war would end after only 15 days.

Instead, the legislative history of this provision makes it clear that Congress elected NOT TO DECIDE how surveillance might need to be conducted in the event of a particular armed conflict. Congress expected that it would revisit the issue in light of events and likely would enact a special authorization during that 15-day period. That is exactly what happened three days after the attacks of 9/11, when Congress passed the Force Resolution, permitting the President to exercise "all necessary and appropriate" incidents of military force.

Thus, it is simply not the case that Congress in 1978 anticipated all the ways that the President might need to act in times of armed conflict to protect the United States. FISA, by its own terms, was not intended to be the last word on these critical issues.

Second, some people have argued that, by their terms, Title III and FISA are the "exclusive means" for conducting electronic surveillance. It is true that the law says that Title III and FISA are "the exclusive means by which electronic surveillance . . . may be conducted." But, as I have said before, FISA itself says elsewhere that the government cannot engage in electronic surveillance "except as authorized by statute." It is noteworthy that, FISA did not say "the government cannot engage in electronic surveillance 'except as authorized by FISA

and Title III.'" No, it said, except as authorized by statute -- any statute. And, in this case, that other statute is the Force Resolution.

Even if some might think that's not the only way to read the statute, in accordance with long recognized canons of construction, FISA must be interpreted in harmony with the Force Resolution to allow the President, as Commander in Chief during time of armed conflict, to take the actions necessary to protect the country from another catastrophic attack. So long as such an interpretation is "fairly possible," the Supreme Court has made clear that it must be adopted, in order to avoid the serious constitutional issues that would otherwise be raised.

Third, I keep hearing, "Why not FISA?" "Why didn't the President get orders from the FISA court approving these NSA intercepts of al Qaeda communications?"

We have to remember that we're talking about a wartime foreign intelligence program. It is an "early warning system" with only one purpose: To detect and prevent the next attack on the United States from foreign agents hiding in our midst. It is imperative for national security that we can detect RELIABLY, IMMEDIATELY, and WITHOUT DELAY whenever communications associated with al Qaeda enter or leave the United States. That may be the only way to alert us to the presence of an al Qaeda agent in our country and to the existence of an unfolding plot.

Consistent with the wartime intelligence nature of this program, the optimal way to achieve the necessary speed and agility is to leave the decisions about particular intercepts to the judgment of professional intelligence officers, based on the best

available intelligence information. They can make that call quickly. If, however, those same intelligence officers had to navigate through the FISA process for each of these intercepts, that would necessarily introduce a significant factor of DELAY, and there would be critical holes in our early warning system.

Some have pointed to the provision in FISA that allows for so-called "emergency authorizations" of surveillance for 72 hours without a court order. There's a serious misconception about these emergency authorizations. People should know that we do not approve emergency authorizations without knowing that we will receive court approval within 72 hours. FISA requires the Attorney General to determine IN ADVANCE that a FISA application for that particular intercept will be fully supported and will be approved by the court before an emergency authorization may be granted. That review process can take precious time.

Thus, to initiate surveillance under a FISA emergency authorization, it is not enough to rely on the best judgment of our intelligence officers alone. Those intelligence officers would have to get the sign-off of lawyers at the NSA that all provisions of FISA have been satisfied, then lawyers in the Department of Justice would have to be similarly satisfied, and finally as Attorney General, I would have to be satisfied that the search meets the requirements of FISA. And we would have to be prepared to follow up with a full FISA application within the 72 hours.

A typical FISA application involves a substantial process in its own right: The work of several lawyers; the preparation of a legal brief and supporting declarations; the approval of a Cabinet-level officer; a certification from the National Security

Adviser, the Director of the FBI, or another designated Senate-confirmed officer; and, finally, of course, the approval of an Article III judge.

We all agree that there should be appropriate checks and balances on our branches of government. The FISA process makes perfect sense in almost all cases of foreign intelligence monitoring in the United States. Although technology has changed dramatically since FISA was enacted, FISA remains a vital tool in the War on Terror, and one that we are using to its fullest and will continue to use against al Qaeda and other foreign threats. But as the President has explained, the terrorist surveillance program operated by the NSA requires the maximum in speed and agility, since even a very short delay may make the difference between success and failure in preventing the next attack. And we cannot afford to fail.

****

Finally, let me explain why the NSA's terrorist surveillance program fully complies with the Fourth Amendment, which prohibits unreasonable searches and seizures.

The Fourth Amendment has never been understood to require warrants in all circumstances. For instance, before you get on an airplane, or enter most government buildings, you and your belongings may be searched without a warrant. There are also searches at the border or when you've been pulled over at a checkpoint designed to identify folks driving while under the influence. Those searches do not violate the Fourth Amendment because they involve "special needs" beyond routine law enforcement. The Supreme Court has repeatedly held that these

circumstances make such a search reasonable even without a warrant.

The terrorist surveillance program is subject to the checks of the Fourth Amendment, and it clearly fits within this "special needs" category. This is by no means a novel conclusion. The Justice Department during the Clinton Administration testified in 1994 that the President has inherent authority under the Constitution to conduct foreign intelligence searches of the private homes of U.S. citizens in the United States without a warrant, and that such warrantless searches are permissible under the Fourth Amendment.

The key question, then, under the Fourth Amendment is not whether there was a warrant, but whether the search was reasonable. This requires balancing privacy with the government's interests – and ensuring that we maintain appropriate safeguards. We've done that here.

No one takes lightly the concerns that have been raised about the interception of communications inside the United States. But this terrorist surveillance program involves intercepting the international communications of persons reasonably believed to be members or agents of al Qaeda or affiliated terrorist organizations. This surveillance is narrowly focused and fully consistent with the traditional forms of enemy surveillance found to be necessary in all previous armed conflicts. The authorities are reviewed approximately every 45 days to ensure that the al Qaeda threat to the national security of this nation continues to exist. Moreover, the standard applied − "reasonable basis to believe" − is essentially the same as the traditional Fourth Amendment probable cause standard. As the

Supreme Court has stated, "The substance of all the definitions of probable cause is a reasonable ground for belief of guilt."

If we conduct this *reasonable* surveillance – while taking special care to preserve civil liberties as we have – we can all continue to enjoy our rights and freedoms for generations to come.

****

I close with a reminder that just last week, al Jazeera aired an audio tape in which Osama bin Laden promised a new round of attacks on the United States. Bin Laden said the proof of his promise is, and I quote, "the explosions you have seen in the capitals of European nations." He continued, quote, "The delay in similar operations happening in America has not been because of failure to break through your security measures. The operations are under preparation and you will see them in your homes the minute they are through with preparations." Close quote.

We've seen and heard these types of warnings before. And we've seen what the result of those preparations can be – thousands of our fellow citizens who perished in the attacks of 9/11.

This Administration has chosen to act now to prevent the next attack, rather than wait until it is too late. This Administration has chosen to utilize every necessary and lawful tool at its disposal. It is hard to imagine a President who wouldn't elect to use these tools in defense of the American people – in fact, I think it would be irresponsible to do otherwise.

The terrorist surveillance program is both necessary and lawful. Accordingly, the President has done with this lawful authority the only responsible thing: use it. He has exercised, and will continue to exercise, his authority to protect Americans and the cherished freedoms of the American people.

Thank you. May God continue to bless the United States of America.

###

(b)(3) 50 USC § 3024(m)(1) @dni.gov

From: (b)(3) 50 USC § 3024(m)(1) @dni.gov
Sent: Thursday, January 26, 2006 2:25 PM
To: Brand, Rachel; Bradbury, Steve; Sampson, Kyle; Michael_Allen@nsc.eop.gov; (b)(3) 50 USC § 3024(m)(1), (b)(6); (b)(3) 50 USC § 3024(m)(1) @dni.gov; (b)(3) 50 USC § 3024(m)(1) @dni.gov; William_K._Kelley@who.eop.gov; David_S._Addington@ovp.eop.gov; Raul_F._Yanes@ (b) (6) ; (b)(3) 50 USC § 3024(m)(1) @dni.gov; Brett_M._Kavanaugh@who.eop.gov; Shannen_W._Coffin@ovp.eop.gov; Dana_M._Perino@who.eop.gov
Subject: Posner
Attachments: tmp.htm; tmp.gif; tmp.gif; tmp.gif; tmp.gif; tmp.gif; tmp.gif; tmp.gif

fyi.

<http://www.tnr.com/sam/public/click.mhtml/498/0>

<http://www.tnr.com/>

WHAT IF WIRETAPPING WORKS?

Wire Trap
by Richard A. Posner
Post date: 01.26.06
Issue date: 02.06.06

he revelation by The New York Times that the National Security Agency (NSA) is conducting a secret program of electronic surveillance outside the framework of the Foreign Intelligence Surveillance Act (fisa) has sparked a hot debate in the press and in the blogosphere. But there is something odd about the debate: It is aridly legal. Civil libertarians contend that the program is illegal, even unconstitutional; some want President Bush impeached for breaking the law. The administration and its defenders have responded that the program is perfectly legal; if it does violate fisa (the administration denies that it does), then, to that extent, the law is unconstitutional. This legal debate is complex, even esoteric. But, apart from a handful of not very impressive anecdotes (did the NSA program really prevent the Brooklyn Bridge from being destroyed by blowtorches?), there has been little discussion of the program's concrete value as a counterterrorism measure or of the inroads it has or has not made on liberty or privacy.

Not only are these questions more important to most people than the legal questions; they are fundamental to those questions. Lawyers who are busily debating legality without first trying to assess the consequences of the program have put the cart before the horse. Law in

the United States is not a Platonic abstraction but a flexible tool of social policy. In analyzing all but the simplest legal questions, one is well advised to begin by asking what social policies are at stake. Suppose the NSA program is vital to the nation's defense, and its impingements on civil liberties are slight. That would not prove the program's legality, because not every good thing is legal; law and policy are not perfectly aligned. But a conviction that the program had great merit would shape and hone the legal inquiry. We would search harder for grounds to affirm its legality, and, if our search were to fail, at least we would know how to change the law--or how to change the program to make it comply with the law--without destroying its effectiveness. Similarly, if the program's contribution to national security were negligible--as we learn, also from the Times, that some FBI personnel are indiscreetly whispering--and it is undermining our civil liberties, this would push the legal analysis in the opposite direction.

Ronald Dworkin, the distinguished legal philosopher and constitutional theorist, wrote in The New York Review of Books in the aftermath of the September 11 attacks that "we cannot allow our Constitution and our shared sense of decency to become a suicide pact." He would doubtless have said the same thing about fisa. If you approach legal issues in that spirit rather than in the spirit of ruat caelum fiat iusticia (let the heavens fall so long as justice is done), you will want to know how close to suicide a particular legal interpretation will bring you before you decide whether to embrace it. The legal critics of the surveillance program have not done this, and the defenders have for the most part been content to play on the critics' turf.

ashington, D.C., which happens to be the home of The New Republic, could be destroyed by an atomic bomb the size of a suitcase. Portions of the city could be rendered uninhabitable, perhaps for decades, merely by the explosion of a conventional bomb that had been coated with radioactive material. The smallpox virus--bioengineered to make it even more toxic and the vaccine against it ineffectual, then aerosolized and sprayed in a major airport--could kill millions of people. Our terrorist enemies have the will to do such things. They may soon have the means as well. Access to weapons of mass destruction is becoming ever easier. With the September 11 attacks now more than four years in the past, forgetfulness and complacency are the order of the day. Are we safer today, or do we just feel safer? The terrorist leaders, scattered by our invasion of Afghanistan and by our stepped-up efforts at counterterrorism (including the NSA program), may even now be regrouping and preparing an attack that will produce destruction on a scale to dwarf September 11. Osama bin Laden's latest audiotape claims that Al Qaeda is planning new attacks on the United States.

The next terrorist attack (if there is one) will likely be mounted, as the last one was, from within the United States but orchestrated by

leaders safely ensconced abroad. So suppose the NSA learns the phone number of a suspected terrorist in a foreign country. If the NSA just wants to listen to his calls to others abroad, fisa doesn't require a warrant. But it does if either (a) one party to the call is in the United States and the interception takes place here or (b) the party on the U.S. side of the conversation is a "U.S person"--primarily either a citizen or a permanent resident. If both parties are in the United States, no warrant can be issued; interception is prohibited. The problem with fisa is that, in order to get a warrant, the government must have grounds to believe the "U.S. person" it wishes to monitor is a foreign spy or a terrorist. Even if a person is here on a student or tourist visa, or on no visa, the government can't get a warrant to find out whether he is a terrorist; it must already have a reason to believe he is one.

As far as an outsider can tell, the NSA program is designed to fill these gaps by conducting warrantless interceptions of communications in which one party is in the United States (whether or not he is a "U.S. person") and the other party is abroad and suspected of being a terrorist. But there may be more to the program. Once a phone number in the United States was discovered to have been called by a terrorist suspect abroad, the NSA would probably want to conduct a computer search of all international calls to and from that local number for suspicious patterns or content. A computer search does not invade privacy or violate fisa, because a computer program is not a sentient being. But, if the program picked out a conversation that seemed likely to have intelligence value and an intelligence officer wanted to scrutinize it, he would come up against fisa's limitations. One can imagine an even broader surveillance program, in which all electronic communications were scanned by computers for suspicious messages that would then be scrutinized by an intelligence officer, but, again, he would be operating outside the framework created by fisa.

The benefits of such programs are easy to see. At worst, they might cause terrorists to abandon or greatly curtail their use of telephone, e-mail, and other means of communicating electronically with people in the United States. That would be a boon to us, because it is far more difficult for terrorist leaders to orchestrate an attack when communicating by courier. At best, our enemies might continue communicating electronically in the mistaken belief that, through use of code words or electronic encryption, they could thwart the NSA.

So the problem with fisa is that the surveillance it authorizes is unusable to discover who is a terrorist, as distinct from eavesdropping on known terrorists--yet the former is the more urgent task. Even to conduct fisa-compliant surveillance of non-U.S. persons, you have to know beforehand whether they are agents of a terrorist group, when what you really want to know is who those agents are.

Fisa's limitations are borrowed from law enforcement. When crimes are

committed, there are usually suspects, and electronic surveillance can be used to nail them. In counterterrorist intelligence, you don't know whom to suspect--you need surveillance to find out. The recent leaks from within the FBI, expressing skepticism about the NSA program, reflect the FBI's continuing inability to internalize intelligence values. Criminal investigations are narrowly focused and usually fruitful. Intelligence is a search for the needle in the haystack. FBI agents don't like being asked to chase down clues gleaned from the NSA's interceptions, because 99 out of 100 (maybe even a higher percentage) turn out to lead nowhere. The agents think there are better uses of their time. Maybe so. But maybe we simply don't have enough intelligence officers working on domestic threats.

have no way of knowing how successful the NSA program has been or will be, though, in general, intelligence successes are underreported, while intelligence failures are fully reported. What seems clear is that fisa does not provide an adequate framework for counterterrorist intelligence. The statute was enacted in 1978, when apocalyptic terrorists scrambling to obtain weapons of mass destruction were not on the horizon. From a national security standpoint, the statute might as well have been enacted in 1878 to regulate the interception of telegrams. In the words of General Michael Hayden, director of NSA on September 11 and now the principal deputy director of national intelligence, the NSA program is designed to "detect and prevent," whereas "fisa was built for long-term coverage against known agents of an enemy power."

In the immediate aftermath of the September 11 attacks, Hayden, on his own initiative, expanded electronic surveillance by NSA without seeking fisa warrants. The United States had been invaded. There was fear of follow-up attacks by terrorists who might already be in the country. Hayden's initiative was within his military authority. But, if a provision of fisa that allows electronic surveillance without a warrant for up to 15 days following a declaration of war is taken literally (and I am not opining on whether it should or shouldn't be; I am not offering any legal opinions), Hayden was supposed to wait at least until September 14 to begin warrantless surveillance. That was the date on which Congress promulgated the Authorization for Use of Military Force, which the administration considers a declaration of war against Al Qaeda. Yet the need for such surveillance was at its most acute on September 11. And, if a war is raging inside the United States on the sixteenth day after an invasion begins and it is a matter of military necessity to continue warrantless interceptions of enemy communications with people in the United States, would anyone think the 15-day rule prohibitive?

We must not ignore the costs to liberty and privacy of intercepting phone calls and other electronic communications. No one wants strangers eavesdropping on his personal conversations. And wiretapping programs

have been abused in the past. But, since the principal fear most people have of eavesdropping is what the government might do with the information, maybe we can have our cake and eat it, too: Permit surveillance intended to detect and prevent terrorist activity but flatly forbid the use of information gleaned by such surveillance for any purpose other than to protect national security. So, if the government discovered, in the course of surveillance, that an American was not a terrorist but was evading income tax, it could not use the discovery to prosecute him for tax evasion or sue him for back taxes. No such rule currently exists. But such a rule (if honored) would make more sense than requiring warrants for electronic surveillance.

Once you grant the legitimacy of surveillance aimed at detection rather than at gathering evidence of guilt, requiring a warrant to conduct it would be like requiring a warrant to ask people questions or to install surveillance cameras on city streets. Warrants are for situations where the police should not be allowed to do something (like search one's home) without particularized grounds for believing that there is illegal activity going on. That is too high a standard for surveillance designed to learn rather than to prove.

Richard A. Posner <http://www.tnr.com/showBio.mhtml?pid=62> is a federal circuit judge and the author of the forthcoming Uncertain Shield: The U.S. Intelligence System in the Throes of Reform.

RELATED LINKS

Character Flaw <http://www.tnr.com/doc.mhtml?i=20060123&s=trb012306> Bush's new humility <http://www.tnr.com/tnrd.mhtml>

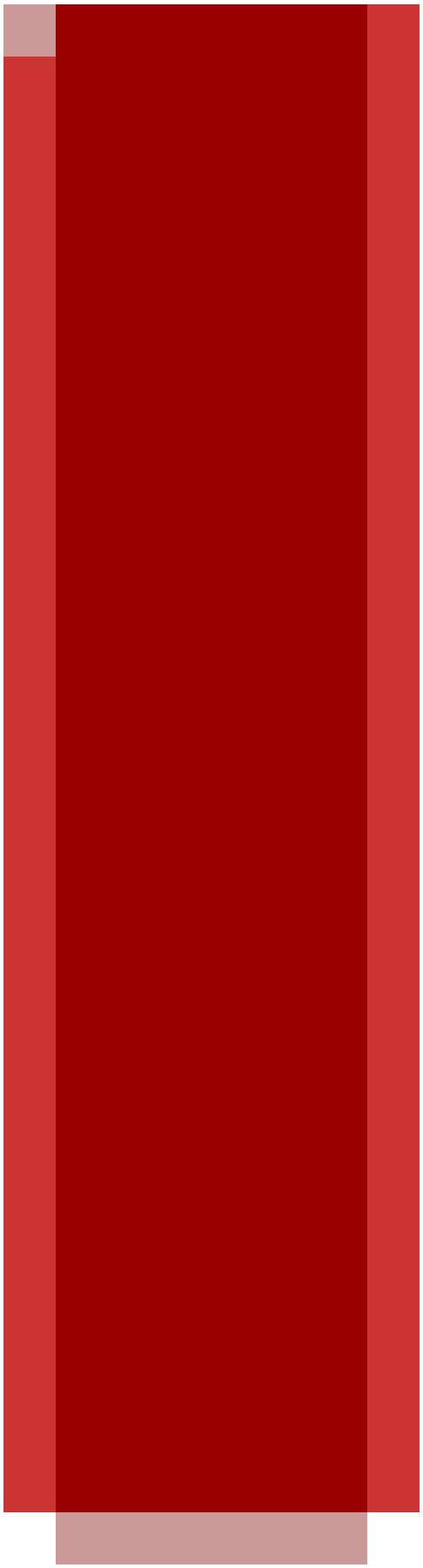
The Insider <http://www.tnr.com/doc.mhtml?i=w060102&s=lizza010606> Bush and the GOP scandals <http://www.tnr.com/tnrd.mhtml> web only

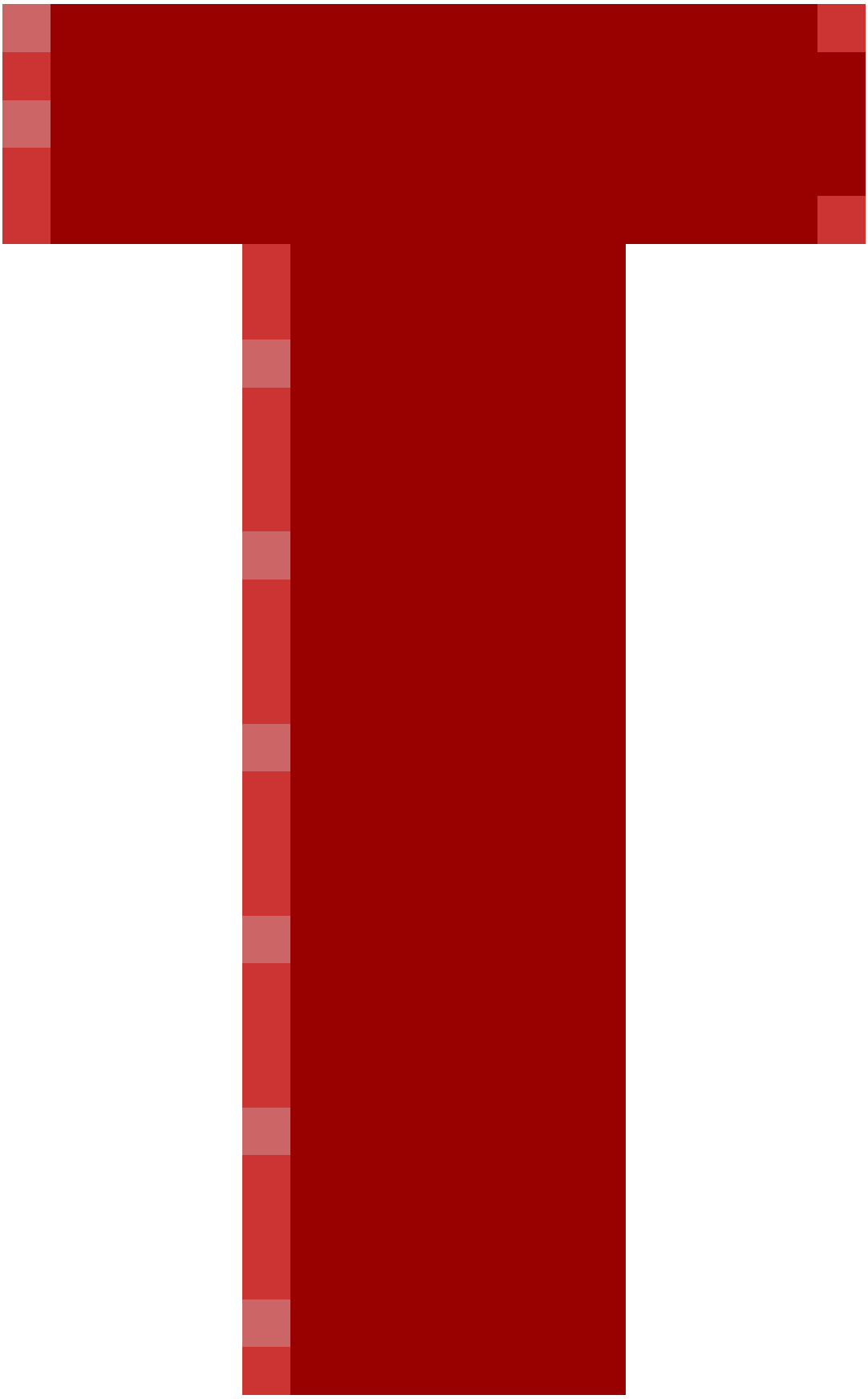
Rebel Quelled <http://www.tnr.com/doc.mhtml?i=20060116&s=lizza011606> Suddenly, Bush just wants to be liked

Spy Crimes <http://www.tnr.com/doc.mhtml?i=20060116&s=editorial011606> The president's domestic wiretapping program is illegal

Breakfast at Epiphanies
<http://www.tnr.com/doc.mhtml?i=w051205&s=frank120705>
Bush officials are frequently misunderstood. Allow them to clarify web only

Con Text <http://www.tnr.com/doc.mhtml?i=w051114&s=lizza111505> Bush's new strategy for defending the war? Take Democratic quotes out of context <http://www.tnr.com/tnrd.mhtml> web only





THE NEW REPUBLIC ONLINE

Searching for the perfect mix.

MORTGAGE BANKERS ASSOCIATION®
investing in communities

How do homes, retail spaces, office buildings, public spaces and rental apartments combine to create the ideal neighborhood?

By providing the capital to create just the right mix.

fyi.

 The New Republic Online

WHAT IF WIRETAPPING WORKS?

Wire Trap

by Richard A. Posner

Post date: 01.26.06
Issue date: 02.06.06

<!--[if !vml]--><!--[endif]-->he revelation by *The New York Times* that the National Security Agency (NSA) is conducting a secret program of electronic surveillance outside the framework of the Foreign Intelligence Surveillance Act (fisa) has sparked a hot debate in the press and in the blogosphere. But there is something odd about the debate: It is aridly legal. Civil libertarians contend that the program is illegal, even unconstitutional; some want President Bush impeached for breaking the law. The administration and its defenders have responded that the program is perfectly legal; if it does violate fisa (the administration denies that it does), then, to that extent, the law is unconstitutional. This legal debate is complex, even esoteric. But, apart from a handful of not very impressive anecdotes (did the NSA program really prevent the Brooklyn Bridge from being destroyed by *blowtorches*?), there has been little discussion of the program's concrete value as a counterterrorism measure or of the inroads it has or has not made on liberty or privacy.

Not only are these questions more important to most people than the legal questions; they are fundamental to those questions. Lawyers who are busily debating legality without first trying to assess the consequences of the program have put the cart before the horse. Law in the United States is not a Platonic abstraction but a flexible tool of social policy. In analyzing all but the simplest legal questions, one is well advised to begin by asking what social policies are at stake. Suppose the NSA program is vital to the nation's defense, and its impingements on civil liberties are slight. That would not prove the program's legality, because not every good thing is legal; law and policy are not perfectly aligned. But a conviction that the program had great merit would shape and hone the legal inquiry. We would search harder for grounds to affirm its legality, and, if our search were to fail, at least we would know how to change the law--or how to change the program to make it comply with the law--without destroying its effectiveness. Similarly, if the program's contribution to national security were negligible--as we learn, also from the *Times*, that some FBI personnel are indiscreetly whispering--and it is undermining our civil liberties, this would push the legal analysis in the opposite direction.

Ronald Dworkin, the distinguished legal philosopher and constitutional theorist, wrote in *The New York Review of Books* in the aftermath of the September 11 attacks that "we cannot allow our Constitution and our shared sense of decency to become a suicide pact." He would doubtless have said the same thing about fisa. If you approach legal issues in that spirit rather than in the spirit of *ruat caelum fiat iusticia* (let the heavens fall so long as justice is done), you will want to know how close to suicide a particular legal interpretation will bring you before you decide whether to embrace it. The legal critics of the surveillance program have not done this, and the defenders have for the most part been content to play on the critics' turf.

<!--[if !vml]--><!--[endif]-->ashington, D.C., which happens to be the home of The New Republic, could be destroyed by an atomic bomb the size of a suitcase. Portions of the city could be rendered uninhabitable, perhaps for decades, merely by the explosion of a conventional bomb that had been coated with radioactive material. The smallpox virus--bioengineered to make it even more toxic and the vaccine against it ineffectual, then aerosolized and sprayed in a major airport--could kill millions of people. Our terrorist enemies have the will to do such things. They may soon have the means as well. Access to weapons of mass destruction is becoming ever easier. With the September 11 attacks now more than four years in the past, forgetfulness and complacency are the order of the day. Are we safer today, or do we just feel safer? The terrorist leaders, scattered by our invasion of Afghanistan and by our stepped-up efforts at counterterrorism (including the NSA program), may even now be regrouping and preparing an attack that will produce destruction on a scale to dwarf September 11. Osama bin Laden's latest audiotape claims that Al Qaeda is planning new attacks on the United States.

The next terrorist attack (if there is one) will likely be mounted, as the last one was, from within the United States but orchestrated by leaders safely ensconced abroad. So suppose the NSA learns the phone number of a suspected terrorist in a foreign country. If the NSA just wants to listen to his calls to others abroad, fisa doesn't require a warrant. But it does if either (a) one party to the call is in the United States and the interception takes place here or (b) the party on the U.S. side of the conversation is a "U.S person"--primarily either a citizen or a permanent resident. If both parties are in the United States, *no* warrant can be issued; interception is prohibited. The problem with fisa is that, in order to get a warrant, the government must have grounds to believe the "U.S. person" it wishes to monitor is a foreign spy or a terrorist. Even if a person is here on a student or tourist visa, or on no visa, the government can't get a warrant to find out whether he is a terrorist; it must already have a reason to believe he is one.

As far as an outsider can tell, the NSA program is designed to fill these gaps by conducting warrantless interceptions of communications in which one party is in the United States (whether or not he is a "U.S. person") and the other party is abroad and suspected of being a terrorist. But there may be more to the program. Once a phone number in the United States was discovered to have been called by a terrorist suspect abroad, the NSA would probably want to conduct a computer search of all international calls to and from that local number for suspicious patterns or content. A computer search does not invade privacy or violate fisa, because a computer program is not a sentient being. But, if the program picked out a conversation that seemed likely to have intelligence value and an intelligence officer wanted to scrutinize it, he would come up against fisa's limitations. One can imagine an even broader surveillance program, in which *all* electronic communications were scanned by computers for suspicious messages that would then be scrutinized by an intelligence officer, but, again, he would be operating outside the framework created by fisa.

The benefits of such programs are easy to see. At worst, they might cause terrorists to abandon or greatly curtail their use of telephone, e-mail, and other means of communicating electronically with people in the United States. That would be a boon to us, because it is far more difficult for terrorist leaders to orchestrate an attack when communicating by courier. At best, our enemies might continue communicating electronically in the mistaken belief that, through use of code words or electronic encryption, they could thwart the NSA.

So the problem with fisa is that the surveillance it authorizes is unusable to discover who is a terrorist, as distinct from eavesdropping on known terrorists--yet the former is the more urgent task. Even to conduct fisa-compliant surveillance of non-U.S. persons, you have to know beforehand whether they are agents of a terrorist group, when what you really want to know is who those agents are.

Fisa's limitations are borrowed from law enforcement. When crimes are committed, there are usually suspects, and electronic surveillance can be used to nail them. In counterterrorist intelligence, you don't know whom to suspect--you need surveillance to find out. The recent leaks from within the FBI, expressing skepticism about the NSA program, reflect the FBI's continuing inability to internalize intelligence values. Criminal investigations are narrowly focused and usually fruitful. Intelligence is a search for the needle in the haystack. FBI agents don't like being asked to chase down clues gleaned from the NSA's interceptions, because 99 out of 100 (maybe even a higher percentage) turn out to lead nowhere. The agents think there are better uses of their time. Maybe so. But maybe we simply don't have enough

intelligence officers working on domestic threats.

<!--[if !vml]--><!--[endif]-->have no way of knowing how successful the NSA program has been or will be, though, in general, intelligence successes are underreported, while intelligence failures are fully reported. What seems clear is that fisa does not provide an adequate framework for counterterrorist intelligence. The statute was enacted in 1978, when apocalyptic terrorists scrambling to obtain weapons of mass destruction were not on the horizon. From a national security standpoint, the statute might as well have been enacted in 1878 to regulate the interception of telegrams. In the words of General Michael Hayden, director of NSA on September 11 and now the principal deputy director of national intelligence, the NSA program is designed to "detect and prevent," whereas "fisa was built for long-term coverage against known agents of an enemy power."

In the immediate aftermath of the September 11 attacks, Hayden, on his own initiative, expanded electronic surveillance by NSA without seeking fisa warrants. The United States had been invaded. There was fear of follow-up attacks by terrorists who might already be in the country. Hayden's initiative was within his military authority. But, if a provision of fisa that allows electronic surveillance without a warrant for up to 15 days following a declaration of war is taken literally (and I am not opining on whether it should or shouldn't be; I am not offering any legal opinions), Hayden was supposed to wait at least until September 14 to begin warrantless surveillance. That was the date on which Congress promulgated the Authorization for Use of Military Force, which the administration considers a declaration of war against Al Qaeda. Yet the need for such surveillance was at its most acute on September 11. And, if a war is raging inside the United States on the sixteenth day after an invasion begins and it is a matter of military necessity to continue warrantless interceptions of enemy communications with people in the United States, would anyone think the 15-day rule prohibitive?

We must not ignore the costs to liberty and privacy of intercepting phone calls and other electronic communications. No one wants strangers eavesdropping on his personal conversations. And wiretapping programs have been abused in the past. But, since the principal fear most people have of eavesdropping is what the government might do with the information, maybe we can have our cake and eat it, too: Permit surveillance intended to detect and prevent terrorist activity but flatly forbid the use of information gleaned by such surveillance for any purpose other than to protect national security. So, if the government discovered, in the course of surveillance, that an American was not a terrorist but was evading income tax, it could not use the discovery to prosecute him for tax evasion or sue him for back taxes. No such rule currently exists. But such a rule (if honored) would make more sense than requiring warrants for electronic surveillance.

Once you grant the legitimacy of surveillance aimed at detection rather than at gathering evidence of guilt, requiring a warrant to conduct it would be like requiring a warrant to ask people questions or to install surveillance cameras on city streets. Warrants are for situations where the police should not be allowed to do something (like search one's home) without particularized grounds for believing that there is illegal activity going on. That is too high a standard for surveillance designed to learn rather than to prove.

RICHARD A. POSNER is a federal circuit judge and the author of the forthcoming *Uncertain Shield: The U.S. Intelligence System in the Throes of Reform.*

RELATED LINKS

Character Flaw
Bush's new humility

The Insider
Bush and the GOP scandals web only

Rebel Quelled
Suddenly, Bush just wants to be liked

Spy Crimes
The president's domestic wiretapping program is illegal

Breakfast at Epiphanies
Bush officials are frequently misunderstood. Allow them to

Con Text
Bush's new strategy for defending the war? Take

clarify web only

Democratic quotes out of context web only

Bradbury, Steve

From: Bradbury, Steve
Sent: Tuesday, January 31, 2006 5:46 PM
To: 'Brett_M._Kavanaugh@who.eop.gov'; 'Raul_F._Yanes [redacted (b) (6)]'
Cc: Harriet_Miers@who.eop.gov; Brett_C._Gerry@who.eop.gov; 'William_K._Kelley@who.eop.gov'; Sampson, Kyle; Eisenberg, John; Elwood, Courtney
Subject: AG's prepared statement & responses to Sen. Specter re NSA hearing
Attachments: Prepared_Statement_1_31.doc; Specter_Response_1_31_am3.doc

Attached for staffing purposes are drafts of (1) the Attorney General's prepared (written) statement for the February 6 Senate Judiciary Committee hearing on the NSA activities and (2) responses to the written questions posed by Chairman Specter in anticipation of the hearing. We intend [redacted (b) (5)]

Raul_F._Yanes@ (b) (6)

From: Raul_F._Yanes@ (b) (6)
Sent: Wednesday, February 01, 2006 11:54 AM
To: Bradbury, Steve; Brett_M._Kavanaugh@who.eop.gov
Cc: Sampson, Kyle; Eisenberg, John; Elwood, Courtney; Harriet_Miers@who.eop.gov; Brett_C._Gerry@who.eop.gov; William_K._Kelley@who.eop.gov
Subject: RE: AG's prepared statement & responses to Sen. Specter re NSA hearing

We will be clearing this through OMB's usual process.

-----Original Message-----
From: Steve.Bradbury@usdoj.gov [mailto:Steve.Bradbury@usdoj.gov]
Sent: Tuesday, January 31, 2006 5:47 PM

duplicate

Brett_C._Gerry@who.eop.gov

From: Brett_C._Gerry@who.eop.gov
Sent: Sunday, February 05, 2006 11:10 AM
To: Sampson, Kyle
Cc: Bradbury, Steve; Harriet_Miers@who.eop.gov; Brett_M._Kavanaugh@who.eop.gov; (b)(3) 50 USC § 3024(m)(1) @dni.gov
Subject: Fw: More comments

Kyle-

Some additional wh comments below. Also, one more general comment I received: (b) (5)

Brett

-----Original Message-----
From: Brett Gerry <(b)(6) Brett Gerry (personal)>
To: Gerry, Brett C. <Brett_C._Gerry@who.eop.gov>
Sent: Sun Feb 05 10:59:55 2006
Subject: More comments

Some more WH comments on the AG's opening remarks:

1. (b) (5)

2. (b) (5)

3. (b) (5)

4. (b) (5)

5. (b) (5)

[redacted] (b) (5) [redacted]

6. [redacted] (b) (5) [redacted]

7. [redacted] (b) (5) [redacted]

8. [redacted] (b) (5) [redacted]

Bradbury, Steve

From: Bradbury, Steve
Sent: Thursday, February 23, 2006 11:31 AM
To: 'Harriet_Miers@who.eop.gov'; (b)(3) 50 USC s.3024(m)(1) @dni.gov; 'Brett_C._Gerry@who.eop.gov'; 'Brett_M._Kavanaugh@who.eop.gov'; 'Michael_Allen@nsc.eop.gov'
Cc: Sampson, Kyle; Elwood, Courtney; Moschella, William; Baker, James; Elwood, John; Eisenberg, John
Subject: Revised AG letter to SJC
Attachments: SJC Letter_2 23 06 Draft_v8.doc

Attached for WH TSP staffing is a draft letter from the AG to the Senate Judiciary Committee responding to questions posed by the Senators and clarifying certain of the AG's answers at the 2/6 hearing. Please provide any comments today. The AG would like to send this letter up to the Hill by tomorrow. Please note that this draft incorporates comments received from ODNI. Thx. Steve

(b)(3) 50 USC § 3605

From: (b)(3) 50 USC § 3605

Sent: Thursday, February 23, 2006 5:58 PM

To: Moschella, William; (b)(3) 50 USC § 3024(m)(1) @dni.gov

Cc: Scolinos, Tasia; Bradbury, Steve; Elwood, John; Elwood, Courtney; (b)(3) 50 USC § 3024(m)(1) @dni.gov; (b)(3) 50 USC § 3605; (b)(3) 50 USC § 3605; (b)(3) 50 USC § 3605; (b)(3) 50 USC § 3507, (b)(6); dsadoff@nsc.eop.gov; (b)(3) 50 USC § 3024(m)(1) dni.gov; Brett_C._Gerry@who.eop.gov; ryanes@ (b) (6) ; jjukes@ (b) (6) ; jwiegmann@nsc.eop.gov; dfiddelke@who.eop.gov; (b)(3) 50 USC § 3507, (b)(6); smithjm (b) (6) ; gary.testut (b) (6) ; Michael_Allen@nsc.eop.gov; valerie.caproni@ic.fbi.gov; Eleni.Kalisch@ic.fbi.gov; Shannen_W._Coffin@ovp.eop.gov; (b)(3) 50 USC § 3024(m)(1) @dni.gov; (b)(3) 50 USC § 3024(m)(1) dni.gov; (b)(3) 50 USC § 3024(m)(1) dni.gov; (b)(3) 50 USC § 3024(m)(1) @dni.gov; Brett_M._Kavanaugh@who.eop.gov

Subject: RE: Draft AG Letter to Judiciary

Attachments: tmp.htm

For Steve Bradbury (fyi to others)

NSA appreciates the opportunity to comment on the draft AG responses to QFRs from the Senate Judiciary hearing. We have some comments to offer that we feel are (b) (5) . We made significant progress on pulling together our comments today and will get you something early tomorrow. We are mindful that you want to send up the answers tomorrow and will work hard so you can accomplish that.

(b)(3) 50 USC § 3605
Associate General Counsel (Legislation)
(b)(3) 50 USC § 3605

-----Original Message-----
From: Benjamin Powell [mailto:(b)(3) 50 USC § 3024(m)(1) @dni.gov]
Sent: Thursday, February 23, 2006 12:08 PM
To: William Moschella
Cc: Darlene Connelly; (b)(3) 50 USC § 3605; (b)(3) 50 USC § 3605; (b)(3) 50 USC § 3605; (b)(3) 50 USC § 3605; (b)(3) 50 USC § 3507, (b)(6); dsadoff@nsc.eop.gov; 'Judith A. Emmel'; Gerry, Brett C.; ryanes@ (b) (6) ; jjukes@ (b) (6) ; jwiegmann@nsc.eop.gov; dfiddelke@who.eop.gov; (b)(3) 50 USC § 3507, (b)(6); smithjm (b) (6) ; gary.testut (b) (6) ; Steve.Bradbury@usdoj.gov; John.Elwood@usdoj.gov; Allen, Michael; Courtney.Elwood@usdoj.gov; Tasia Scolinos; Valerie Caproni; Kalisch, Eleni P.; Coffin, Shannen W.; (b)(3) 50 USC § 3024(m)(1); (b)(3) 50 USC § 3024(m)(1); (b)(3) 50 USC § 3024(m)(1); (b)(3) 50 USC § 3024(m)(1); Kavanaugh, Brett M.
Subject: Draft AG Letter to Judiciary

See attached letter. Please provide comments to Steve Bradbury at DOJ.
They would appreciate comments by today. His email is:

Steve.Bradbury@usdoj.gov

-------- Original Message --------
Subject: Revised AG letter to SJC
Date: Thu, 23 Feb 2006 11:31:45 -0500 (EST)
From: Steve.Bradbury@usdoj.gov <mailto:Steve.Bradbury@usdoj.gov>
<Steve.Bradbury@usdoj.gov>

duplicate

(b)(3) 50 USC § 3605

From: (b)(3) 50 USC § 3605
Sent: Friday, February 24, 2006 12:35 PM
To: Moschella, William; (b)(3) 50 USC § 3024(m)(1) @dni.gov
Cc: Scolinos, Tasia; Bradbury, Steve; Elwood, John; Elwood, Courtney; (b)(3) 50 USC § 3024(m)(1) @dni.gov; (b)(3) 50 USC § 3605; (b)(3) 50 USC § 3605; (b)(3) 50 USC § 3605; (b)(3) 50 USC § 3507, (b)(6); dsadoff@nsc.eop.gov; (b)(3) 50 USC § 3024(m)(1) dni.gov; Brett_C._Gerry@who.eop.gov; ryanes@ (b) (6) ; jjukes@ (b) (6) ; jwiegmann@nsc.eop.gov; dfiddelke@who.eop.gov; (b)(3) 50 USC § 3507, (b)(6); smithjm (b) (6) ; gary.testut (b) (6) ; Michael_Allen@nsc.eop.gov; valerie.caproni@ic.fbi.gov; Eleni.Kalisch@ic.fbi.gov; Shannen_W._Coffin@ovp.eop.gov; (b)(3) 50 USC § 3024(m)(1) @dni.gov; (b)(3) 50 USC § 3024(m)(1) dni.gov; (b)(3) 50 USC § 3024(m)(1) dni.gov; (b)(3) 50 USC § 3024(m)(1) @dni.gov; Brett_M._Kavanaugh@who.eop.gov; (b)(3) 50 USC § 3605
Subject: RE: Draft AG Letter to Judiciary
Attachments: tmp.htm; Draft-AG Response to Specter QFRs-24 Feb 06.doc

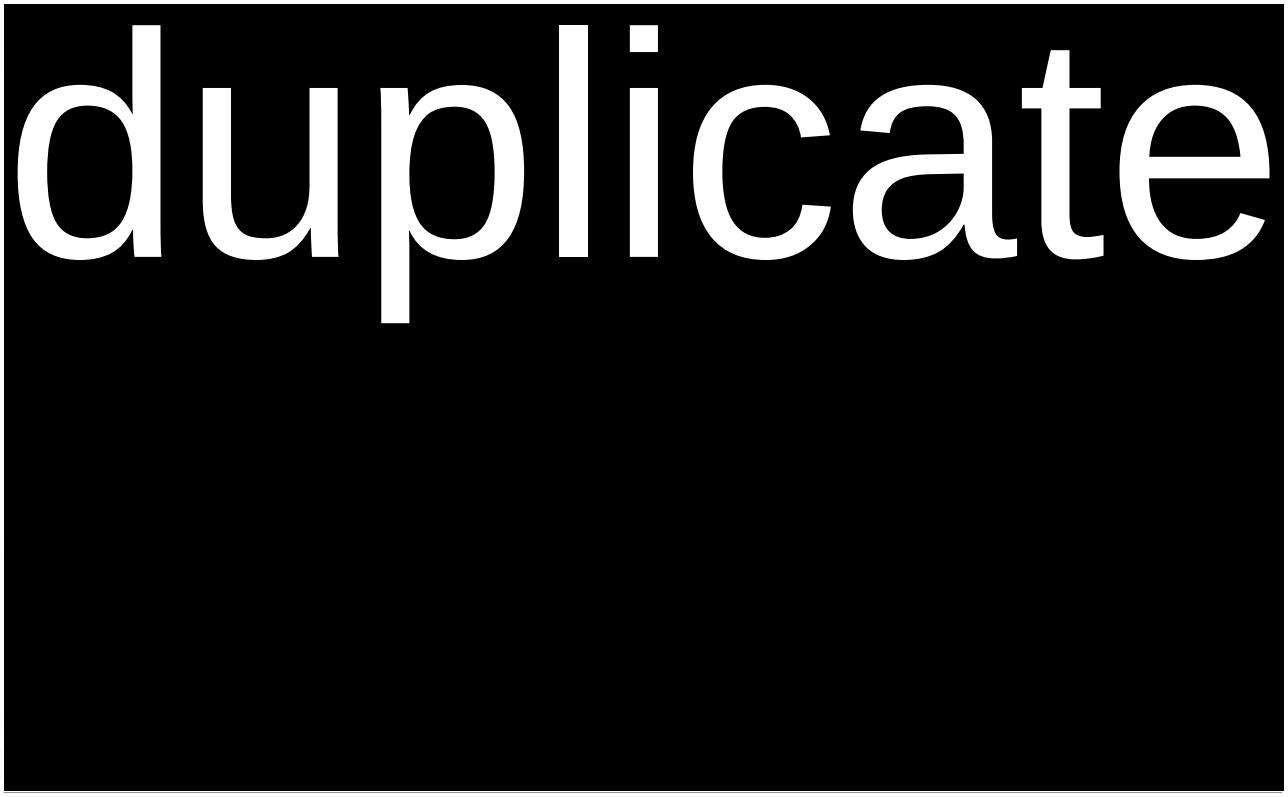
Steve and John (cc to the rest)

Here are NSA's comments on the AG's answers to Chairman Specter.

(b)(3) 50 USC § 3605

-----Original Message-----
From: Benjamin Powell [mailto:(b)(3) 50 USC § 3024(m)(1) @dni.gov]
Sent: Thursday, February 23, 2006 12:08 PM

duplicate



Steve and John (cc to the rest)

Here are NSA's comments on the AG's answers to Chairman Specter.

(b)(3) 50 USC § 3605

Bradbury, Steve

From:	Bradbury, Steve
Sent:	Wednesday, March 01, 2006 9:32 AM
To:	'(b)(3) 50 USC § 3024(m)(1) @dni.gov'; 'Michael_Allen@nsc.eop.gov'; Brett_C._Gerry@who.eop.gov; 'Harriet_Miers@who.eop.gov'; 'Brett_M._Kavanaugh@who.eop.gov'
Cc:	'(b)(3) 50 USC § 3024(m)(1) @dni.gov'; '(b)(3) 50 USC § 3024(m)(1) @dni.gov'; Sampson, Kyle; Elwood, Courtney; Scolinos, Tasia; Elwood, John; Eisenberg, John; Edney, Michael; Willen, Brian
Subject:	DOJ letters to hill
Attachments:	2.28.06.AG responses to 2.6.QFRs.pdf; 2.28.06.response to Feinstein pre-hearing questions.pdf; Responses to Sen. Feinstein's Questions (2 28 06).pdf

Attached are the letters and QFR responses on the TSP that DOJ sent to the Senate Judiciary Committee yesterday. There are numerous additional QFRs that we are working on, and we will circulate drafts of those responses shortly.

The Attorney General

Washington, D.C.

February 28, 2006

The Honorable Arlen Specter
Chairman, Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Chairman Specter:

I write to provide responses to several questions posed to me at the hearing on "Wartime Executive Power and the National Security Agency's Surveillance Authority," held Monday, February 6, 2006, before the Senate Committee on the Judiciary. I also write to clarify certain of my responses at the February 6th hearing.

Except when otherwise indicated, this letter will be confined to addressing questions relating to the specific NSA activities that have been publicly confirmed by the President. Those activities involve the interception by the NSA of the contents of communications in which one party is outside the United States where there are reasonable grounds to believe that at least one party to the communication is a member or agent of al Qaeda or an affiliated terrorist organization (hereinafter, the "Terrorist Surveillance Program").

Additional Information Requested by Senators at February 6th Hearing

Senator Leahy asked whether the President first authorized the Terrorist Surveillance Program after he signed the Authorization for Use of Military Force of September 18, 2001 ("Force Resolution") and before he signed the USA PATRIOT Act. 2/6/06 Unofficial Hearing Transcript ("Tr.") at 50. The President first authorized the Program in October 2001, before he signed the USA PATRIOT Act.

Senator Brownback asked for recommendations on improving the Foreign Intelligence Surveillance Act ("FISA"). Tr. at 180-81. The Administration believes that it is unnecessary to amend FISA to accommodate the Terrorist Surveillance Program. The Administration will, of course, work with Congress and evaluate any proposals for improving FISA.

Senator Feinstein asked whether the Government had informed the Supreme Court of the Terrorist Surveillance Program when it briefed and argued *Hamdi v. Rumsfeld*, 542 U.S. 507 (2004). Tr. at 207. The question presented in *Hamdi* was whether the military had validly detained Yaser Esam Hamdi, a presumed American citizen who was captured in Afghanistan during the combat operations in late 2001, whom the military had concluded to be an enemy combatant who should be detained in

connection with ongoing hostilities. No challenge was made concerning electronic surveillance and the Terrorist Surveillance Program was not a part of the lower court proceedings. The Government therefore did not brief the Supreme Court regarding the Terrorist Surveillance Program.

Senator Feinstein asked whether "any President ever authorized warrantless surveillance in the face of a statute passed by Congress which prohibits that surveillance." Tr. at 208. I recalled that President Franklin Roosevelt had authorized warrantless surveillance in the face of a contrary statute, but wanted to confirm this. To the extent that the question is premised on the understanding that the Terrorist Surveillance Program conflicts with any statute, we disagree with that premise. The Terrorist Surveillance Program is entirely consistent with FISA, as explained in some detail in my testimony and the Department's January 19th paper. As for the conduct of past Presidents, President Roosevelt directed Attorney General Jackson "to authorize the necessary investigating agents that they are at liberty to secure information by listening devices directed to the conversation or other communications of persons suspected of subversive activities against the Government of the United States." Memorandum from President Roosevelt (May 21, 1940), *reproduced in United States v. United States District Court,* 444 F.2d 651, 670 (6th Cir. 1971) (Appendix A). President Roosevelt authorized this activity notwithstanding the language of 47 U.S.C. § 605, a prohibition of the Communications Act of 1934, which, at the time, provided that "no person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person." President Roosevelt took this action, moreover, despite the fact that the Supreme Court had, just three years earlier, made clear that section 605 "include[s] within its sweep federal officers." *Nardone v. United States*, 302 U.S. 379, 384 (1937). It should be noted that section 605 prohibited interception followed by divulging or publishing the contents of the communication. The Department of Justice took the view that interception without "divulg[ing] or publish[ing]" was not prohibited, and it interpreted "divulge" narrowly to allow dissemination within the Executive Branch.

Senator Feingold asked, "[D]o you know of any other President who has authorized warrantless wiretaps outside of FISA since 1978 when FISA was passed?" Tr. at 217. The laws of the United States, both before and after FISA's enactment, have long permitted various forms of foreign intelligence surveillance, including the use of wiretaps, outside the procedures of FISA. If the question is limited to "electronic surveillance" as defined in FISA, however, we are unaware of any such authorizations.

Senator Feingold asked, "[A]re there other actions under the use of military force for Afghanistan resolution that without the inherent power would not be permitted because of the FISA statute? Are there any other programs like that?" Tr. at 224. I understand the Senator to be referring to the Force Resolution, which authorizes the President to "use all necessary and appropriate force against those nations, organizations, or persons" responsible for the attacks of September 11th in order to prevent further terrorist attacks on the United States, and which by its terms is not limited to action

against Afghanistan or any other particular nation. I am not in a position to provide information here concerning any other intelligence activities beyond the Terrorist Surveillance Program. Consistent with long-standing practice, the Executive Branch notifies Congress concerning the classified intelligence activities of the United States through appropriate briefing of the oversight committees and congressional leadership.

Senator Feingold noted that, on September 10, 2002, then-Associate Deputy Attorney General David S. Kris testified before the Senate Judiciary Committee. Senator Feingold quoted Mr. Kris's statement that "[w]e cannot monitor anyone today whom we could not have monitored this time last year," and he asked me to provide the names of individuals in the Department of Justice and the White House who reviewed and approved Mr. Kris's testimony. Tr. at 225-26. Mr. Kris's testimony was addressing the Government's appeal in 2002 of decisions of the Foreign Intelligence Surveillance Court to the Foreign Intelligence Surveillance Court of Review. In the course of that discussion, Mr. Kris explained the effects of the USA PATRIOT Act's amendments to FISA, and, in particular, the amendment to FISA requiring that a "significant purpose" of the surveillance be the collection of foreign intelligence information. Mr. Kris explained that that amendment "will not and cannot change who the government may monitor." Mr. Kris emphasized that under FISA as amended, the Government still needed to show that there is probable cause that the target of the surveillance is an agent of a foreign power and that the surveillance has at least a significant foreign intelligence purpose. In context, it is apparent that Mr. Kris was addressing only the effects of the USA PATRIOT Act's amendments to FISA. In any event, his statements are also accurate with respect to the President's Terrorist Surveillance Program, because the Program involves the interception of communications only when there is probable cause ("reasonable grounds to believe") that at least one party to the communication is an agent of a foreign power (al Qaeda or an affiliated terrorist organization). Please note that it is Department of Justice policy not to identify the individual officials who reviewed and approved particular testimony.

Senators Biden and Schumer asked whether the legal analysis underlying the Terrorist Surveillance Program would extend to the interception of purely domestic calls. Tr. at 80-82, 233-34. The Department believes that the Force Resolution's authorization of "all necessary and appropriate force," which the Supreme Court in *Hamdi* interpreted to include the fundamental and accepted incidents of the use of military force, clearly encompasses the narrowly focused Terrorist Surveillance Program. The Program targets only communications in which one party is outside the United States and there are reasonable grounds to believe that at least one party to the communication is a member or agent of al Qaeda or an affiliated terrorist organization. The Program is narrower than the wartime surveillances authorized by President Woodrow Wilson (*all* telephone, telegraph, and cable communications into and out of the United States) and President Franklin Roosevelt ("*all . . . telecommunications traffic* in and out of the United States"), based on their constitutional authority and general force-authorization resolutions like the Force Resolution. The Terrorist Surveillance Program fits comfortably within this historical precedent and tradition. The legal analysis set forth in the Department's January 19th paper does not address the interception of purely domestic communications.

The Department believes that the interception of the contents of domestic communications would present a different question from the interception of international communications, and the Department would need to analyze that question in light of all current circumstances before any such interception would be authorized.

Senator Schumer asked me whether the Force Resolution would support physical searches within the United States without complying with FISA procedures. Tr. at 159. The Terrorist Surveillance Program does not involve physical searches. Although FISA's physical search subchapter contains a provision analogous to section 109 of FISA, *see* 50 U.S.C. § 1827(a)(1) (prohibiting physical searches within the United States for foreign intelligence "except as authorized by statute"), physical searches conducted for foreign intelligence purposes present issues different from those discussed in the Department's January 19th paper addressing the legal basis for the Terrorist Surveillance Program. Thus, we would need to consider that issue specifically before taking a position.

Senator Schumer asked, "Have there been any abuses of the NSA surveillance program? Have there been any investigations arising from concerns about abuse of the NSA program? Has there been any disciplinary action taken against any official for abuses of the program?" Tr. at 237-38. Although no complex program like the Terrorist Surveillance Program can ever be free from inadvertent mistakes, the Program is the subject of intense oversight both within the NSA and outside that agency to ensure that any compliance issues are identified and resolved promptly on recognition. Procedures are in place, based on the guidelines I approved under Executive Order 12333, to protect the privacy of U.S. persons. NSA's Office of General Counsel has informed us that the oversight process conducted both by that office and by the NSA Inspector General has uncovered no abuses of the Terrorist Surveillance Program, and, accordingly, that no disciplinary action has been needed or taken because of abuses of the Program.

Clarification of Certain Responses

I would also like to clarify certain aspects of my responses to questions posed at the February 6th hearing.

First, as I emphasized in my opening statement, in all of my testimony at the hearing I addressed—with limited exceptions—only the legal underpinnings of the Terrorist Surveillance Program, as defined above. I did not and could not address operational aspects of the Program or any other classified intelligence activities. So, for example, when I testified in response to questions from Senator Leahy, "Sir, I have tried to outline for you and the Committee what the President has authorized, and that is all that he has authorized," Tr. at 53, I was confining my remarks to the Terrorist Surveillance Program as described by the President, the legality of which was the subject of the February 6th hearing.

Second, in response to questions from Senator Biden as to why the President's authorization of the Terrorist Surveillance Program does not provide for the interception of domestic communications within the United States of persons associated with al

Qaeda, I stated, "That analysis, quite frankly, had not been conducted." Tr. at 82. In response to similar questions from Senator Kyl and Senator Schumer, I stated, "The legal analysis as to whether or not that kind of [domestic] surveillance—we haven't done that kind of analysis because, of course, the President—that is not what the President has authorized," Tr. at 92, and "I have said that I do not believe that we have done the analysis on that." Tr. at 160. These statements may give the misimpression that the Department's legal analysis has been static over time. Since I was testifying only as to the legal basis of the activity confirmed by the President, I was referring only to the legal analysis of the Department set out in the January 19th paper, which addressed that activity and therefore, of course, does not address the interception of purely domestic communications. However, I did not mean to suggest that no analysis beyond the January 19th paper had ever been conducted by the Department. The Department believes that the interception of the contents of domestic communications presents a different question from the interception of international communications, and the Department's analysis of that question would always need to take account of all current circumstances before any such interception would be authorized.

Third, at one point in my afternoon testimony, in response to a question from Senator Feinstein, I stated, "I am not prepared at this juncture to say absolutely that if the AUMF argument does not work here, that FISA is unconstitutional as applied. I am not saying that." Tr. at 209. As set forth in the January 19th paper, the Department believes that FISA is best read to allow a statute such as the Force Resolution to authorize electronic surveillance outside FISA procedures and, in any case, that the canon of constitutional avoidance requires adopting that interpretation. It is natural to approach the question whether FISA might be unconstitutional as applied in certain circumstances with extreme caution. But if an interpretation of FISA that allows the President to conduct the NSA activities were not "fairly possible," and if FISA were read to impede the President's ability to undertake actions necessary to fulfill his constitutional obligation to protect the Nation from foreign attack in the context of a congressionally authorized armed conflict against an enemy that has already staged the most deadly foreign attack in our Nation's history, there would be serious doubt about the constitutionality of FISA as so applied. A statute may not "*impede* the President's ability to perform his constitutional duty," *Morrison v. Olson*, 487 U.S. 654, 691 (1988) (emphasis added); *see also id.* at 696-97, particularly not the President's most solemn constitutional obligation—the defense of the Nation. *See also In re Sealed Case,* 310 F.3d 717, 742 (Foreign Intel. Surv. Ct. of Rev. 2002) (explaining that "FISA could not encroach on the President's constitutional power"). I did not mean to suggest otherwise.

Fourth, in response to questions from Senator Leahy about when the Administration first determined that the Force Resolution authorized the Terrorist Surveillance Program, I stated, "From the very outset, before the program actually commenced." Tr. at 184. I also stated, "Sir, it has always been our position that the President has the authority under the authorization to use military force and under the Constitution." Tr. at 187. These statements may give the misimpression that the Department's legal analysis has been static over time. As I attempted to clarify more generally, "[i]t has always been the [Department's] position that FISA cannot be

interpreted in a way that infringes upon the President's constitutional authority, that FISA must be interpreted, can be interpreted" to avoid that result. Tr. at 184; *see also* Tr. at 164 (Attorney General: "It has always been our position that FISA can be and must be read in a way that it doesn't infringe upon the President's constitutional authority."). Although the Department's analysis has always taken account of both the Force Resolution and the Constitution, it is also true, as one would expect, that the Department's legal analysis has evolved over time.

Fifth, Senator Cornyn suggested that the Terrorist Surveillance Program is designed to address the problem that FISA requires that we already know that someone is a terrorist before we can begin coverage. Senator Cornyn asked, "[T]he problem with FISA as written is that the surveillance it authorizes is unusable to discover who is a terrorist, as distinct from eavesdropping on known terrorists. Would you agree with that?" I responded, "That would be a different way of putting it, yes, sir." Tr. at 291. I want to be clear, however, that the Terrorist Surveillance Program targets the contents of communications in which one party is outside the United States and there are reasonable grounds to believe that at least one party to the communication is a member or agent of al Qaeda or an affiliated terrorist organization. Although the President has authorized the Terrorist Surveillance Program in order to provide the early warning system we lacked on September 11th, I do not want to leave the Committee with the impression that it does so by doing away with a probable cause determination. Rather, it does so by allowing intelligence experts to respond agilely to all available intelligence and to begin coverage as quickly as possible.

Finally, in discussing the FISA process with Senator Brownback, I stated, "We have to know that a FISA Court judge is going to be absolutely convinced that this is an agent of a foreign power, that this facility is going to be a facility that is going to be used or is being used by an agent of a foreign power." Tr. at 300. The approval of a FISA application requires only probable cause to believe that the target is an agent of a foreign power and that the foreign power has used or is about to use the facility in question. 50 U.S.C. § 1805(a)(3). I meant only to convey how cautiously we approach the FISA process. It is of paramount importance that the Department maintain its strong and productive working relationship with the Foreign Intelligence Surveillance Court, one in which that court has come to know that it can rely on the representations of the attorneys that appear before it.

I hope that the Committee will find this additional information helpful.

Sincerely,

Alberto R. Gonzales

cc: The Honorable Patrick Leahy
Ranking Member

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

February 28, 2006

The Honorable Dianne Feinstein
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Senator Feinstein:

Please find attached responses to your letter, dated January 30, 2006, which posed questions to Attorney General Gonzales prior to his appearance before the Senate Committee on the Judiciary on February 6, 2006. The subject of the hearing was, "Wartime Executive Power and the National Security Agency's Surveillance Authority."

We trust you will find this information helpful. If we may be of further assistance on this, or any other matter, please do not hesitate to contact this office.

Sincerely,

William E. Moschella
Assistant Attorney General

Enclosure

cc: The Honorable Arlen Specter
Chairman, Committee on the Judiciary

The Honorable Patrick J. Leahy
Ranking Minority Member

RESPONSES TO QUESTIONS FROM SENATOR FEINSTEIN

1. I have been informed by former Majority Leader Senator Tom Daschle that the Administration asked that language be included in the "*Joint Resolution to Authorize the use of United States Armed Forces against those responsible for the recent attacks launched against the United States*" (P.L. 107-40) (hereinafter "the Authorization" or "AUMF") which would add the words "in the United States" to its text, after the words "appropriate force."

- **Who in the Administration contacted Senator Daschle with this request?**

- **Please provide copies of any communication reflecting this request, as well as any documents reflecting the legal reasoning which supported this request for additional language.**

The Congressional Research Service recently concluded that the account of Senator Daschle to which your question refers "is not reflected in the official record of the legislative debate" on the Authorization for Use of Military Force (hereinafter "Force Resolution"). *See* Richard F. Grimmet, *Authorization for Use of Military Force in Response to the 9/11 Attacks (P.L. 107-40): Legislative History* at 3 n.5 (Jan. 4, 2006). We do not recall such a discussion with former Senator Daschle and are not aware of any record reflecting such a conversation. In any event, a private discussion cannot change the plain meaning and evident intent of the Force Resolution, which clearly confirms and supplements the President's authority to take military action within the United States.

In the Force Resolution, Congress expressly recognized that the September 11th attacks "render it both necessary and appropriate that the United States exercise its rights to self-defense and to protect United States citizens both *at home* and abroad." Force Resolution pmbl. (emphasis added). Congress concluded that the attacks "continue to pose an unusual and extraordinary threat to the national security." *Id.* Congress affirmed that "the President has authority under the Constitution to take action to deter and prevent actions of international terrorism *against the United States*." *Id.* (emphasis added). Accordingly, Congress authorized the President "to use all necessary and appropriate force against those" associated with the attacks "in order to prevent future acts of international terrorism *against the United States*." *Id.* (emphasis added).

The plain language of the Force Resolution clearly encompasses action within the United States. In addition, when Congress passed the Force Resolution on September 14, 2001, the World Trade Center was still burning, combat air patrols could be heard over many American cities, and there was great concern that another attack would follow shortly. Further, the attacks of September 11th were launched on United States soil by foreign agents who had been living in this country. Given this context and the plain meaning of the Force Resolution, Congress must be understood as having ratified the President's authority to use force within the United States. A crucial responsibility of the President—charged by the Force Resolution and the Constitution to defend our Nation—

was and is to identify and disable those enemies, *especially if they are in the United States*, waiting to stage another strike.

2. Did any Administration representative communicate to any Member of Congress the view that the language of the Authorization as approved would provide legal authority for what otherwise would be a violation of the criminal prohibition of domestic electronic collection within the United States?

- **If so, who in the Administration made such communications?**
- **Are there any contemporaneous documents which reflect that view within the Administration?**

Although your question does not indicate what timeframe it covers, we understand it to ask whether, contemporaneous with the passage of the Force Resolution, Administration officials told Members of Congress that the Force Resolution would provide legal authorization for interception of the international communications of members and agents of al Qaeda and affiliated terrorist organizations. We are not aware of any specific communications between the Administration and Members of Congress during the three days between the September 11th attacks and the passage of the Force Resolution involving the particular issue of electronic surveillance—or, for that matter, any of the other fundamental incidents of the use of military force encompassed within the Force Resolution (such as the detention of U.S. citizens who are enemy combatants, which has since been upheld by the Supreme Court).

Although we are not aware of any specific discussion of what incidents of force would be authorized by a general authorization of force, the Supreme Court has explained that Congress must be understood to have authorized "fundamental and accepted" incidents of waging war. *Hamdi v. Rumsfeld*, 542 U.S. 507, 518 (2004) (plurality opinion); *see id.* at 587 (Thomas, J., dissenting). Consistent with this traditional understanding, other Presidents, including Woodrow Wilson and Franklin Roosevelt, have interpreted general force authorization resolutions to permit warrantless surveillance to intercept suspected enemy communications. *Cf. generally* Curtis A. Bradley & Jack L. Goldsmith, *Congressional Authorization and the War on Terrorism*, 118 Harv. L. Rev. 2048, 2091 (2005) (explaining that, with the Force Resolution, "Congress intended to authorize the President to take at least those actions permitted by the laws of war").

The understanding at the time of the passage of the Force Resolution was that it was important to act quickly and to invest the President with the authority to use "all necessary and appropriate force" against those associated with the September 11th attacks and to prevent further terrorist attacks on the United States. Congress could not have cataloged every possible aspect of the use of military force it intended to endorse. Rather than engage in that difficult and impractical exercise, Congress authorized the President, in general but intentionally broad and powerful terms, to use the fundamental and accepted incidents of the use of military force and to determine how best to identify and to engage the enemy in the current armed conflict. That is traditionally how Congress has acted at the outset of armed conflict: "because of the changeable and

explosive nature of contemporary international relations . . . Congress—in giving the Executive authority over matters of foreign affairs—must of necessity paint with a brush broader than that it customarily wields in domestic areas." *Zemel v. Rusk,* 381 U.S. 1, 17 (1965); *cf. Dames & Moore v. Regan*, 453 U.S. 654, 678 (1981) ("Congress cannot anticipate and legislate with regard to every possible action the President may find it necessary to take.").

3. According to Assistant Attorney General William Moschella's letter of December 22, 2005, and the subsequent "White Paper," it is the view of the Department of Justice that the Authorization "satisfies section [FISA section] 109's requirement for statutory authorization of electronic surveillance."[1]

- **Are there other statutes which, in the view of the Department, have been similarly affected by the passage of the Authorization?**
- **If so, please provide a comprehensive list of these statutes.**
- **Has the President, or any other senior Administration official, issued any order or directive based on the AUMF which modifies, supersedes or alters the application of any statute?**

Five members of the Supreme Court concluded in *Hamdi v. Rumsfeld*, 542 U.S. 507 (2004), that the Force Resolution satisfies 18 U.S.C. § 4001(a)'s prohibition on detention of U.S. citizens "except pursuant to an Act of Congress," and thereby authorizes the detention even of Americans who are enemy combatants. The Foreign Intelligence Surveillance Act of 1978 ("FISA") contains a similar provision indicating that it contemplates that electronic surveillance could be authorized in the future "by statute." Section 109 of FISA prohibits persons from "engag[ing] . . . in electronic surveillance under color of law *except as authorized by statute*." 50 U.S.C. § 1809(a)(1) (emphasis added). Just as the Force Resolution satisfies the restrictions imposed by section 4001(a), it also satisfies the statutory authorization requirement of section 109 of FISA.

We have not sought to catalog every instance in which the Force Resolution might satisfy a statutory authorization requirement contained in another statute, other than FISA and section 4001(a), the provision at issue in *Hamdi*. We have not found it necessary to determine the full effect of the Force Resolution to conclude that it authorizes the terrorist surveillance program described by the President, which involves the interception of the contents of communications where one end of the communication is outside the United States and there are reasonable grounds to believe that at least one party to the communication is a member or agent of al Qaeda or an affiliated terrorist organization (hereinafter, the "Terrorist Surveillance Program").

---

[1] **Letter, Assistant Attorney General Williams Moschella to Senator Pat Roberts, et al., December 22, 2005, at p. 3 (hereinafter "Moschella Letter").**

4. The National Security Act of 1947, as amended, provides that "[a]ppropriated funds available to an intelligence agency may be obligated or expended for an intelligence or intelligence-related activity only if . . . (1) those funds were specifically authorized by the Congress for use for such activities . . ."[2] It appears that the domestic electronic surveillance conducted within the United States by the National Security Agency was not "specifically authorized," and thus may be prohibited by the National Security Agency of 1947.

- **What legal authority would justify expending funds in support of this program without the required authorization?**

The General Counsel of the National Security Agency has assured the Department of Justice that the Terrorist Surveillance Program complies with section 504 of the National Security Act of 1947, the provision quoted in your question.

5. The Constitution provides that "[n]o money shall be drawn from the Treasury, but in consequence of appropriations made by law."[3] Title 31, Section 1341 (the Anti-Deficiency Act) provides that "[a]n officer or employee of the United States Government . . . may not – make or authorize an expenditure or obligation exceeding an amount available in an appropriation or fund for the expenditure or obligation," and Section 1351 of the same Title adds that "an officer or employee of the United States Government or of the District of Columbia government knowingly and willfully violating sections 1341(a) or 1342 of this title shall be fined not more than $5,000, imprisoned for not more than 2 years, or both." In sum, the Constitution prohibits, and the law makes criminal, the spending of funds except those funds appropriated in law.

- **Were the funds expended in support of this program appropriated?**
- **If yes, which law appropriated the funds?**
- **Please identify, by name and title, what "officer or employee" of the United States made or authorized the expenditure of the funds in support of this program?**

As stated above, the General Counsel of the National Security Agency has assured the Department of Justice that the applicable statutory standard has been satisfied.

6. Are there any other intelligence programs or activities, including, but not limited to, monitoring internet searches, emails and online purchases, which, in the view of

---

[2] **National Security Act of 1947, as amended, Section 504, codified at 50 U.S.C. 414.**

[3] **U.S. Constitution, Article I, Section 7**.

the Department of Justice, have been authorized by law, although kept secret from some members of the authorizing committee?

- **If so, please list and describe such programs.**

The National Security Act of 1947 contemplates that the Intelligence Committees of both Houses would be appropriately notified of intelligence programs and the Act specifically contemplates more limited disclosure in the case of exceptionally sensitive matters. Title 50 of the U.S. Code provides that the Director of National Intelligence and the heads of all departments, agencies, and other entities of the Government involved in intelligence activities shall keep the Intelligence Committees fully and currently informed of intelligence activities "[t]o the extent consistent with due regard for the protection from unauthorized disclosure of classified information relating to sensitive intelligence sources and methods or other exceptionally sensitive matters." 50 U.S.C. §§ 413a(a), 413b(b). It has long been the practice of both Democratic and Republican administrations to inform the Chair and Ranking Members of the Intelligence Committees about exceptionally sensitive matters. The Congressional Research Service has acknowledged that the leaders of the Intelligence Committees "over time have accepted the executive branch practice of limiting notification of intelligence activities in some cases to either the Gang of Eight, or to the chairmen and ranking members of the intelligence committees." *See* Alfred Cumming, *Statutory Procedures Under Which Congress is to be Informed of U.S. Intelligence Activities, Including Covert Actions*, Congressional Research Service Memorandum at 10 (Jan. 18, 2006). This Administration has followed this well-established practice by briefing the leadership of the Intelligence Committees about intelligence programs or activities as required by the National Security Act of 1947.

7. Are there any other expenditures which have been made or authorized which have not been specifically appropriated in law, and which have been kept secret from members of the Appropriations Committee?

- **If so, please list and describe such programs.**

As stated above, the NSA has indicated that expenditures on the Terrorist Surveillance Program comply with the National Security Act and applicable appropriations law.

8. At a White House press briefing, on December 19, 2005, you stated that that the Administration did not seek authorization in law for this NSA surveillance program because "you were advised that that was not . . . something [you] could likely get" from Congress.

- **What were your sources of this advice?**
- **As a matter of constitutional law, is it the view of the Department that the scope of the President's authority increases when he believes that the legislative branch will not pass a law he approves of?**

As the Attorney General clarified both later in the December 19th briefing that you cite and on December 21, 2005, it is not the case that the Administration declined to seek a specific authorization of the Terrorist Surveillance Program because we believed Congress would not authorize it. *See* Remarks by Homeland Security Secretary Chertoff and Attorney General Gonzales on the USA PATRIOT Act, *available at* http://www.dhs.gov/dhspublic/display?content=5285. Rather, as the Attorney General has testified, the consensus view in the discussions with Members of Congress was that it was unlikely, if not impossible, that more specific legislation could be enacted without compromising the Terrorist Surveillance Program by disclosing operational details, limitations, and capabilities to our enemies. Such disclosures would necessarily have compromised our national security.

9. The Department of Justice's position, as explained in the Moschella Letter and the subsequent White Paper, is that even if the AUMF is determined not to provide the legal authority for conduct which otherwise would be prohibited by law, the President's "inherent" powers as Commander-in-Chief provide independent authority.

- **Is this an accurate assessment of the Department's position?**

As the Department has explained, the Force Resolution does provide legal authority for the Terrorist Surveillance Program. The Force Resolution is framed in broad and powerful terms, and a majority of the Justices of the Supreme Court concluded in *Hamdi v. Rumsfeld* that the Force Resolution authorized the "fundamental and accepted" incidents of the use of military force. Moreover, when it enacted the Force Resolution, Congress was legislating in light of the fact that past Presidents (including Woodrow Wilson and Franklin Roosevelt) had interpreted similarly broad resolutions to authorize much wider warrantless interception of international communications.

Even if there were some ambiguity regarding whether FISA and the Force Resolution may be read in harmony to allow the President to authorize the Terrorist Surveillance Program, the President's inherent powers as Commander in Chief and as chief representative of the Nation in foreign affairs to undertake electronic surveillance against the declared enemy of the United States during an armed conflict would require resolving such ambiguity in favor of the President's authority. Under the canon of constitutional avoidance, courts generally interpret statutes to avoid serious constitutional questions where "fairly possible." *INS v. St. Cyr,* 533 U.S. 289, 299-300 (2001) (citations omitted); *Ashwander v. TVA,* 297 U.S. 288, 345-48 (1936) (Brandeis, J., concurring). The canon of constitutional avoidance has particular importance in the realm of national security, where the President's constitutional authority is at its highest. *See Department of the Navy v. Egan*, 484 U.S. 518, 527, 530 (1988); William N. Eskridge, Jr., *Dynamic Statutory Interpretation* 325 (1994) (describing "[s]uper-strong rule against congressional interference with the President's authority over foreign affairs and national security"). Thus, we need not confront the question whether the President's inherent powers in this area would authorize conduct otherwise prohibited by statute.

Even if the Force Resolution were determined not to provide the legal authority, it is the position of the Department of Justice, maintained by both Democratic and Republican administrations, that the President's inherent authority to authorize foreign-intelligence surveillance would permit him to authorize the Terrorist Surveillance Program. President Carter's Attorney General, Griffin Bell, testified at a hearing on FISA as follows: "[T]he current bill recognizes no inherent power of the President to conduct electronic surveillance, and I want to interpolate here to say that *this does not take away the power of the President under the Constitution*." Hearing Before the Subcomm. on Legislation of the House Permanent Select Comm. on Intelligence (Jan. 10, 1978) (emphasis added). Thus, in saying that President Carter agreed to follow the procedures of FISA, Attorney General Bell made clear that FISA could not take away the President's Article II authority. More recently, the Foreign Intelligence Surveillance Court of Review, the specialized court of appeals that Congress established to review the decisions of the Foreign Intelligence Surveillance Court, recognized that the President has inherent constitutional authority to gather foreign intelligence that cannot be intruded upon by Congress. The court explained that all courts to have addressed the issue of the President's inherent authority have "held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information." *In re Sealed Case,* 310 F.3d 717, 742 (2002). On the basis of that unbroken line of precedent, the court "[took] for granted that the President does have that authority," and concluded that, assuming that is so, "*FISA could not encroach on the President's constitutional power*." *Id.* (emphasis added).

10. Based on the Moschella Letter and the subsequent White Paper, I understand that it is the position of the Department of Justice that the National Security Agency, with respect to this program of domestic electronic surveillance, is functioning as an element of the Department of Defense generally, and as one of a part of the "Armed Forces of the United States," as referred to in the AUMF.

- **Is this an accurate understanding of the Department's position?**

As explained above, the Terrorist Surveillance Program is not a program of "domestic" electronic surveillance.

The NSA is within the Department of Defense, and the Director of the NSA reports directly to the Secretary of Defense. Although organized under the Department of Defense, the NSA is not part of the "Armed Forces of the United States," which consists of the Army, Navy, Air Force, Marine Corps, and Coast Guard. 10 U.S.C. § 101(a)(4). The President has constitutional authority to direct that resources under his control (including assets that are not part of the Armed Forces of the United States) be used for military purposes. In addition, the Department would not interpret the Force Resolution to authorize the President to use only the Armed Forces in his effort to protect the Nation.

11. Article 8 of the Constitution provides that the Congress "shall make Rules for the Government and Regulation of the land and naval forces." It appears that the

Foreign Intelligence Surveillance Act (FISA), as applied to the National Security Agency, is precisely the type of "Rule" provided for in this section.

- **Is it the position of the Department of Justice that the President's Commander-in-Chief power is superior to the Article 8 powers of Congress?**
- **Does the Department of Justice believe that if the President disagrees with a law passed by Congress as part of its responsibility to regulate the Armed Forces, the law is not binding?**

It is emphatically *not* the position of the Department of Justice that the President's authority as Commander in Chief is superior to Congress's authority set forth in Article I, Section 8 of the Constitution. As we have explained, the Terrorist Surveillance Program is fully consistent with FISA, because Congress authorized it through the Force Resolution. Nor is it the position of the Department of Justice "that if the President disagrees with a law passed by Congress as part of its responsibility to regulate the Armed Forces, the law is not binding." No one is above the law.

The inherent authority of the President to conduct warrantless foreign intelligence surveillance is well established, and *every* court of appeals to have considered the question has determined that the President has such authority, even during peacetime. On the basis of that unbroken line of precedent, the Foreign Intelligence Surveillance Court of Review "t[ook] for granted that the President does have that authority" and concluded that, assuming that is so, "FISA could not encroach on the President's constitutional power." *In re Sealed Case*, 310 F.3d 717, 742 (2002).

The scope of Congress's authority to make rules for the regulation of the land and naval forces is not entirely clear. The Supreme Court traditionally has construed this authority to provide for military discipline of members of the Armed Forces by, for example, "grant[ing] the Congress power to adopt the Uniform Code of Military Justice" for offenses committed by servicemembers, *Kinsella v. United States ex rel. Singleton*, 361 U.S. 234, 247 (1960), and by providing for the establishment of military courts to try such cases, *see Ryder v. United States*, 515 U.S. 177, 186 (1995); *Madsen v. Kinsella*, 343 U.S. 341, 347 (1952); *see also McCarty v. McCarty*, 453 U.S. 210, 232-233 (1981) (noting enactment of military retirement system pursuant to power to make rules for the regulation of land and naval forces). That reading is consistent with the Clause's authorization to regulate "Forces," rather than the *use* of force. Whatever the scope of Congress's authority, however, Congress may not "impede the President's ability to perform his constitutional duty," *Morrison v. Olson*, 487 U.S. 654, 691 (1988); *see also id.* at 696-97, particularly not the President's most solemn constitutional obligation—the defense of the Nation.

The potential conflict of Congress's authority with the President's in these circumstances would present a serious constitutional question, which, as described above, can and must be avoided by construing the Force Resolution to authorize the fundamental and accepted incidents of war, consistent with historical practice.

12. On January 24, 2006, during an interview with CNN, you said that "[a]s far as I'm concerned, we have briefed Congress . . . [t]hey're aware of the scope of the program."

- **Please explain the basis for the assertion that I was briefed on this program, or that I am "aware of the scope of the program."**

The quotation to which your question refers is not from an interview on CNN, but is a quotation reported on the CNN Website that is attributed to the Attorney General's remarks at Georgetown University on January 24, 2006. *See* http://www.cnn.com/2006/POLITICS/01/24/nsa.strategy/index.html. The prepared text of that speech accurately reflects that "[t]he *leadership of* Congress, *including the leaders of the Intelligence Committees of both Houses of Congress*, have been briefed about this program more than a dozen times since 2001." *See* http://www.usdoj.gov/ag/speeches/2006/ag_speech_0601242.html (emphasis added). Similarly, during a January 16, 2006, interview on CNN, the Attorney General accurately stated that "we have briefed *certain members of* Congress regarding the operations of these activities and have given examples of where these authorities, where the activities under this program have been extremely helpful in protecting America." *See* http://archives.cnn.com/TRANSCRIPTS/0601/16/lkl.01.html (emphasis added). The Attorney General has not asserted that every Member of Congress was briefed on the Terrorist Surveillance Program, or that you specifically have been briefed on it. However, in accordance with long-standing practice regarding exceptionally sensitive intelligence matters, the Department believes that the briefing of congressional leaders satisfies the Administration's responsibility to keep Congress apprised of the Terrorist Surveillance Program. This view is shared by the Administration and by the Chairmen of both the House and Senate Intelligence Committees. *See* Letter from the Honorable Peter Hoekstra, Chairman, House Permanent Select Committee on Intelligence, to Daniel Mulholland, Director, Congressional Research Service at 1-3 (Feb. 1, 2006); Letter from the Honorable Pat Roberts, Chairman Senate Committee on Intelligence, to the Honorable Arlen Specter and the Honorable Patrick Leahy at 16-17 (Feb. 3, 2006).

13. It appears from recent press coverage that Mr. Rove has been briefed about this program, which, as I understand it, is considered too sensitive to brief to Senators who are members of the Senate Intelligence Committee.

- **Who decided that Mr. Rove was to be briefed about the program, and what is his need-to-know?**
- **Is the program classified pursuant to Executive Order 12958, and if so, who was the classifying authority, and under what authority provided in Executive Order 12958 was the classification decision made?**
- **How many executive branch officials have been advised of the nature, scope and content of the program? Please provide a list of their names and positions.**

- **How many individuals outside the executive branch have been advised of the nature, scope and content of the program? Please provide a list of their names and positions.**

The Terrorist Surveillance Program remains classified, and we may discuss only those aspects of the Program that have been described by the President. In general, the identity of individuals who have been briefed into the Program is also classified. The Program was classified pursuant to sections 1.4(c) and (e) of Executive Order 12958, as amended by Executive Order 13292 (March 28, 2003).

14. The AUMF authorizes the President to use "all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons, in order to prevent any future acts of international terrorism against the United States by such nations, organizations or persons."

- **What do you believe are the conditions under which the President's authority to conduct the NSA program pursuant to the Authorization would expire?**

As you know, al Qaeda leaders repeatedly have announced their intention to attack the United States again. As recently as December 7, 2005, Ayman al-Zawahiri stated that al Qaeda "is spreading, growing, and becoming stronger," and that al Qaeda is "waging a great historic battle in Iraq, Afghanistan, Palestine, and even in the Crusaders' own homes." Ayman al-Zawahiri, videotape released on Al-Jazeera television network (Dec. 7, 2005). And just last month, Osama bin Laden warned that al Qaeda was preparing another attack on our homeland. After noting the deadly bombings committed in London and Madrid, he said:

> The delay in similar operations happening in America has not been because of failure to break through your security measures. The operations are under preparation and you *will see them in your homes* the minute they are through (with preparations), with God's permission.

Quoted at http://www.breitbart.com/news/2006/01/19/D8F7SMRH5.html (Jan. 19, 2006) (emphasis added). The threat from Al Qaeda continues to be real. Thus, the necessity for the President to take these actions continues today.

As a general matter, the authorization for the Terrorist Surveillance Program that is provided by the Force Resolution would expire when the "nations, organizations, or persons [the President] determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001," no longer pose a threat to the United States. The authorization that is provided by the Force Resolution also would expire if it were repealed through legislation. In addition, the Program by its own terms expires

approximately every 45 days unless it is reauthorized after a review process that includes a review of the current threat to the United States posed by al Qaeda and its affiliates.

15. The Department of Justice White Paper states that the program is used when there is a "reasonable basis" to conclude that one party is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda.

- **Can the program be used against a person who is a member of an organization affiliated with al Qaeda, but where the organization has no connection to the 9/11 attacks themselves?**
- **Can you define the terms "reasonable basis" and "affiliated?" Are there any examples, for instance, from criminal law that can describe the "reasonable basis" standard that is being used for the NSA program? What about "affiliated?"**
- **Is it comparable to the "agent of" standard in FISA?**
- **Can the program be used to prevent terrorist attacks by an organization other than al Qaeda?**

The Terrorist Surveillance Program targets communications only where one party is outside the United States and where there are reasonable grounds to believe that at least one party to the communication is a member or agent of al Qaeda or an affiliated terrorist organization. The "reasonable grounds to believe" standard is essentially a "probable cause" standard of proof. *See Maryland v. Pringle*, 540 U.S. 366, 371 (2003) ("We have stated . . . that '[t]he substance of all the definitions of probable cause is a reasonable ground for belief of guilt.'"). The critical advantage offered by the Terrorist Surveillance Program compared to FISA is *who* makes the probable cause determination and how many layers of review will occur *before* surveillance begins. Under the Terrorist Surveillance Program, professional intelligence officers, who are experts on al Qaeda and its tactics (including its use of communication systems), with appropriate and rigorous oversight, make the decisions about which international communications should be intercepted. Relying on the best available intelligence, these officers determine before intercepting any communications whether there are "reasonable grounds to believe" that at least one party to the communication is a member or agent of al Qaeda or an affiliated terrorist organization. By contrast, even the most expedited traditional FISA process would involve review by NSA intelligence officers, NSA lawyers, Justice Department lawyers, and the Attorney General before even emergency surveillance would begin. In the narrow context of defending the Nation in this congressionally authorized armed conflict with al Qaeda, we must allow these highly trained intelligence experts to use their skills and knowledge to protect us.

Answering the rest of these questions would require discussion of operational aspects of the Program.

16. In addition to open combat, the detention of enemy combatants and electronic surveillance, what else do you consider being "incident to" the use of military force? Are interrogations of captives "incident to" the use of military force?

A majority of the Justices in *Hamdi v. Rumsfeld* concluded that the Force Resolution's authorization of "all necessary and appropriate force" includes fundamental and accepted incidents of the use of military force. *See* 542 U.S. 507, 518 (2004) (plurality opinion); *id.* at 587 (Thomas, J., dissenting). As your question acknowledges, a majority of the Justices concluded that the detention of enemy combatants is a fundamental and accepted incident of the use of military force. As explained at length in our January 19th paper, signals intelligence is a fundamental and accepted incident of the use of military force. Consistent with that understanding, other Presidents, including Woodrow Wilson and Franklin Roosevelt, have interpreted general force-authorization resolutions to permit warrantless surveillance during wartime to intercept suspected enemy communications. In addition, we note that the Supreme Court has stated in a slightly different context that "[a]n important incident to the conduct of war is the adoption of measures by the military command not only to repel and defeat the enemy, but to seize and subject to disciplinary measures those enemies who in their attempt to thwart or impede our military effort have violated the law of war." *Ex Parte Quirin*, 317 U.S. 1, 29 (1942).

In light of the strictly limited nature of the Terrorist Surveillance Program, we do not think it a useful or a practical exercise to engage in speculation about the outer limits of what kinds of military activity might be authorized by the Force Resolution. It is sufficient to note that, as discussed at length in the Department's January 19th paper, the use of signals intelligence to intercept the international communications of the enemy has traditionally been recognized as one of the core incidents of the use of military force.

17. The program is reportedly defined as where one party is in the U.S. and one party in a foreign country. Regardless of how the program is actually used, does the AUMF authorize the President to use the program against calls or emails entirely within the U.S.?

We believe that the Force Resolution's authorization of "all necessary and appropriate force," which the Supreme Court in *Hamdi* interpreted to include the fundamental and accepted incidents of the use of military force, clearly encompasses the narrowly focused Terrorist Surveillance Program. The Program targets only the communications where one party is outside the United States and where there are reasonable grounds to believe that at least one party to the communication is a member or agent of al Qaeda or an affiliated terrorist organization. Indeed, the Program is much narrower than the wartime surveillances authorized by President Woodrow Wilson (*all* telephone, telegraph, and cable communications into and out of the United States) and President Franklin Roosevelt ("*all . . . telecommunications traffic* in and out of the United States"), based on their constitutional authority and general force-authorization resolutions like the Force Resolution. The narrow Terrorist Surveillance Program fits comfortably within this precedent and tradition. Interception of the contents of domestic communications presents a different legal question which is not implicated here.

18. FISA has safeguard provisions for the destruction of information that is not foreign intelligence. For instance, albeit with some specific exceptions, if no FISA order is obtained within 72 hours, material gathered without a warrant is destroyed.

- **Are there procedures in place for the destruction of information collected under the NSA program that is not foreign intelligence?**
- **If so, what are the procedures?**
- **Who determines whether the information is retained?**

Procedures are in place to protect U.S. privacy rights, including applicable procedures from Attorney General guidelines issued pursuant to Executive Order 12333, that govern acquisition, retention, and dissemination of information relating to U.S. persons.

19. The DOJ White Paper relies on broad language in the preamble that is contained in both the AUMF and the *Authorization for the Use of Military Force Against Iraq* as a source of the President's authority.

- **Does the Iraq Resolution provide similar authority to the President to engage in electronic surveillance? For instance, would it have been authorized to conduct surveillance of communications between an individual in the U.S. and someone in Iraq immediately after the invasion?**

The Authorization for Use of Military Force Against Iraq, Pub. L. 107-243 (Oct. 16, 2002), provides that the "President is authorized to use the Armed Forces of the United States as he determines to be necessary and appropriate in order to—(1) defend the national security of the United States against the continuing threat posed by Iraq; and (2) enforce all relevant United Nations Security Council resolutions regarding Iraq." *Id.* § 3(a). Under appropriate circumstances, the Iraq Resolution would authorize electronic surveillance of enemy communications. *See generally* Curtis A. Bradley & Jack L. Goldsmith, *Congressional Authorization and the War on Terrorism*, 118 Harv. L. Rev. 2047, 2093 (2005) (stating that the "generally accepted view" is "that a broad and unqualified authorization to use force empowers the President to do to the enemy what the laws of war permit").

20. In a December 17, 2005, radio address the President stated, "I authorized the National Security Agency…to intercept the international communications of people with known links to al Qaeda and related terrorist organizations."

- **What is the standard for establishing a link between a terrorist organization and a target of this program?**
- **How many such communications have been intercepted during the life of this program? How many disseminated intelligence reports have resulted from this collection?**
- **Has the NSA intercepted under this program any communications by journalists, clergy, non-governmental organizations (NGOs) or family**

members of U.S. military personnel? If so, for what purpose, and under what authority?

Before the international communications of an individual may be targeted for interception under the Terrorist Surveillance Program, there must be reasonable grounds to believe that the individual is a member or agent of al Qaeda or an affiliated terrorist organization. That standard of proof is appropriately considered as "a practical, nontechnical conception that deals with the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act." *Maryland v. Pringle*, 540 U.S. 366, 370 (2003) (internal quotation marks omitted) (describing "probable cause" standard). We cannot provide more detail without discussing operational aspects of the Program.

21. In a December 17, 2005, radio address the President stated, "The activities I authorized are reviewed approximately every 45 days…The review includes approval by our Nation's top legal officials, including the Attorney General and the Counsel to the President."

- **As White House Counsel during the first 4 years this program was implemented, were you aware of this program and of the legal arguments supporting it when this Committee considered your nomination to be Attorney General?**
- **Who is responsible for determining whether to reauthorize this program, and upon what basis is this determination made?**

As an initial matter, the Department wishes to emphasize the seriousness with which this Administration takes these periodic reviews and reauthorizations of the Terrorist Surveillance Program. The requirement that the Terrorist Surveillance Program be reviewed and reauthorized at the highest levels of Government approximately every 45 days ensures that the Program will not be continued unless the al Qaeda threat to the United States continues to justify use of the Program.

The President sought legal advice prior to authorizing the Program and was advised that it is lawful. The Program has been reviewed by the Department of Justice, by lawyers at the NSA, and by the Counsel to the President. The Attorney General was involved in advising the President about the Program in his capacity as Counsel to the President, and he has been involved in approving the legality of the Program during his time as Attorney General. Since 2001, the Program has been reviewed multiple times by different counsel. The Terrorist Surveillance Program is lawful in all respects, as explained in the Justice Department paper of January 19, 2006.

The President is responsible for reauthorizing the Program. That determination is based on reviews undertaken by the Intelligence Community and Department of Justice, a strategic assessment of the continuing importance of the Program to the national security of the United States, and assurances that safeguards continue to protect civil liberties.

22. In a Press Briefing on December 19, 2005, you said that you "believe the President has the inherent authority under the Constitution, as Commander-in-Chief, to engage in this kind of activity [domestic surveillance]." This authority is further asserted in the Department of Justice White Paper of January 19, 2006.

- **Has the President ever invoked this authority, with respect to any activity other than the NSA surveillance program?**
- **Has any other order or directive been issued by the President, or any other senior administration official, based on such authority which authorizes conduct which would otherwise be prohibited by law?**

i. Can the President suspend (in secret or otherwise) the application of Section 503 of the National Security Act of 1947 (50 U.S.C. 413(b)), which states that "no convert action may be conducted which is intended to influence United States political processes, public opinion, policies or media?"

1. If so, has such authority been exercised?

ii. Can the President suspend (in secret or otherwise) the application of the Posse Comitatus Act (18 U.S.C. 1385)?

1. If so, has such authority been exercised?

iii. Can the President suspend (in secret or otherwise) the application of 18 U.S.C. 1001, which prohibits "the making the false statements within the executive, legislative, or judicial branch of the Government of the United States."

1. If so, has such authority been exercised?

The Terrorist Surveillance Program targets for interception *international* communications of our enemy in the armed conflict with al Qaeda. As Congress expressly recognized in the Force Resolution, "the President has authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States," Force Resolution pmbl., especially in the context of the current conflict. Article II of the Constitution vests in the President all executive power of the United States, including the power to act as Commander in Chief, *see* U.S. Const. art. II, § 2, and authority over the conduct of the Nation's foreign affairs. As the Supreme Court has explained, "[t]he President is the sole organ of the nation in its external relations, and its sole representative with foreign nations." *United States v. Curtiss-Wright Export Corp.,* 299 U.S. 304, 319 (1936) (internal quotation marks and citations omitted). In this way, the Constitution grants the President inherent power to protect the Nation from foreign attack, *see, e.g.*, *The Prize Cases,* 67 U.S. (2 Black) 635, 668 (1863), and to protect national security information, *see, e.g.*, *Department of the Navy v. Egan,* 484 U.S. 518, 527 (1988).

The President has used his constitutional authority to protect the Nation. Although no statute had yet authorized the use of military force, the President scrambled military aircraft during the attacks of September 11th to protect the Nation from further attack and continued those patrols for days before the Force Resolution was passed by Congress and signed by the President.

The Terrorist Surveillance Program is not, as your question suggests, "otherwise prohibited by law." FISA expressly contemplates that in a separate statute Congress may authorize electronic surveillance outside FISA procedures. *See* 50 U.S.C. § 1809(a)(1) (FISA § 109, prohibiting any person from intentionally "engag[ing] . . . in electronic surveillance under color of law *except as authorized by statute*") (emphasis added). That is what Congress did in the Force Resolution. As *Hamdi v. Rumsfeld*, 542 U.S. 507 (2004), makes clear, a general authorization to use military force carries with it the authority to employ the fundamental and accepted incidents of the use of force. That is so even if Congress did not specifically address each of the incidents of force; thus, a majority of the Court concluded that the Force Resolution authorized the detention of enemy combatants as a fundamental incident of force, and Justice O'Connor stated that "it is of no moment that the [Force Resolution] does not use specific language of detention." *Id*. at 519 (plurality opinion). Indeed, a majority of Justices in *Hamdi* concluded that the Force Resolution satisfied a statute nearly identical to section 109 of FISA, 18 U.S.C. § 4001(a), which prohibits the detention of United States citizens "except pursuant to an Act of Congress." As explained at length in the Department's January 19th paper, signals intelligence is a fundamental and accepted incident of the use of military force. Consistent with this traditional practice, other Presidents, including Woodrow Wilson and Franklin Roosevelt, have interpreted general force-authorization resolutions to permit interception of suspected enemy communications. Thus, the President has not "authorize[d] conduct which would otherwise be prohibited by law."

It would not be appropriate for the Department to speculate about whether various other statutes, in circumstances not presented here, could yield to the President's constitutional authority. As Justice Jackson has written, the division of authority between the President and Congress should not be delineated in the abstract. *See Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 635 (1952) (Jackson, J., concurring) ("The actual art of governing under our Constitution does not and cannot conform to judicial definitions of the power of any of its branches based on isolated clauses or even single Articles torn from context."); *see also Dames & Moore v. Regan*, 453 U.S. 654, 660-61 (1981). Without a specific factual circumstance in which such a decision would be made, speculating about such possibilities in the abstract is not fruitful.

Nevertheless, we have explained that the Force Resolution provides authority for the fundamental incidents of the use of force. The Department does not believe that covert action aimed at affecting the United States political process or lying to Congress would constitute a fundamental incident of the use of force.

Finally, the Posse Comitatus Act generally prohibits using the Army or Air Force for domestic law enforcement purposes absent statutory authorization. That statute does

not address the use of military force for military purposes, including national defense, in the armed conflict with al Qaeda.

23. Had the Department of Justice adopted the interpretation of the AUMF asserted in the Moschella letter and subsequent White Paper at the time it discussed the USA-Patriot Act with members of Congress? That act substantially altered FISA, and yet, to my knowledge, there was no discussion of the legal conclusions you now assert – that the AUMF has triggered the "authorized by other statute" wording of FISA.

- **Please provide any communications, internal or external, which are contemporaneous to the negotiation of the USA-Patriot Act, which contain information regarding this question.**

As you know, on January 19th, the Department of Justice released a 42-page paper setting out a comprehensive explanation of the legal authorities supporting the Terrorist Surveillance Program. The paper reflects the substance of the Department's legal analysis of the Terrorist Surveillance Program. We have always interpreted FISA not to infringe on the President's constitutional authority to protect the Nation from foreign attacks. It is also true, as one would expect, that our legal analysis has evolved over time.

It would be inappropriate for us to reveal any confidential and privileged internal deliberations of the Executive Branch. The Department is not aware of communications with Congress in connection with the negotiation of the USA PATRIOT Act concerning the effect of the Force Resolution.

24. The USA-Patriot Act reauthorization bill is currently being considered by the Congress. Among the provisions at issue is Section 215, which governs the physical search authorization under FISA. Does the legal analysis proposed by the Department also apply to this section of FISA? If so, is the Department's position that, regardless of whether the Congress adopts the pending Conference Report, the Senate bill language, or some other formulation, the President may order the application of a different standard or procedure based on the AUMF or his Commander-in-Chief authority?

- **If so, is there any need to reauthorize those sections of the USA-Patriot Act which authorize domestic surveillance?**

FISA remains an essential and invaluable tool for foreign intelligence collection both in the armed conflict with al Qaeda and in other contexts. In contrast to surveillance conducted pursuant to the Force Resolution, FISA is not limited to al Qaeda and affiliated terrorist organizations. In addition, FISA has procedures that specifically allow the Government to use evidence in criminal prosecutions and, at the same time, protect intelligence sources and methods. In short, there is an urgent need to reauthorize the USA PATRIOT Act.

The Terrorist Surveillance Program does not involve physical searches. FISA's physical search subchapter contains a provision analogous to section 109, *see* 50 U.S.C. § 1827(a)(1) (prohibiting physical searches within the United States for foreign intelligence "except as authorized by statute"). Physical searches conducted for foreign intelligence purposes present questions different from those discussed in the January 19th paper addressing the legal basis for the Terrorist Surveillance Program. Thus, we would need to consider that issue specifically before taking a position.

25. Public statements made by you, as well as the President, imply that this program is used to identify terrorist operatives within the United States. Have any such operatives in fact been identified? If so, have these individuals been detained, and if so, where, and under what authority? Have any been killed?

- **The arrest and subsequent detention of Jose Padilla is, to my knowledge, the last public acknowledgement of the apprehension of an individual classified as an "enemy combatant" within the United States. Have there been any other people identified as an "enemy combatant" and detained with the United States, and if so, what has been done with these individuals?**

With respect, we cannot answer these questions without revealing the operational details of the Terrorist Surveillance Program, other than to point to the testimony of General Hayden and Director Mueller at the February 2d Worldwide Threat Briefing. Specifically, General Hayden stated that "the program has been successful; . . . we have learned information from this program that would not otherwise have been available" and that "[t]his information has helped detect and prevent terrorist attacks in the United States and abroad." Director Muller stated that "leads from that program have been valuable in identifying would-be terrorists in the United States, individuals who were providing material support to terrorists."

26. Senator Roberts has stated that the program is limited to: "when we know within a terrorist cell overseas that there is a plot and that plot is very close to its conclusion or that plot is very close to being waged against America – now, if a call comes in from an Al Qaeda cell and it is limited to that where we have reason to believe that they are planning an attack, to an American phone number, I don't think we're violating anybody's Fourth Amendment rights in terms of civil liberties."[4]

- **Is the program limited to such imminent threats against the United States, or where an attack is being planned? Is this an accurate description of the program?**

As the Attorney General has explained elsewhere, the Terrorist Surveillance Program is an early warning system aimed at detecting and preventing another

---

[4] Senator Pat Roberts, CNN Late Edition with Wolf Blitzer, January 29, 2006

catastrophic al Qaeda terrorist attack. It targets communications only when one party to the communication is outside of the country and professional intelligence experts have reasonable grounds to believe that at least one party to the communication is a member or agent of al Qaeda or an affiliated terrorist organization.

Beyond that, it would be inappropriate to provide a more specific description of the Program, as the operational details remain classified and further disclosure would compromise the Program's effectiveness.

27. In a speech given in Buffalo, New York by the President, in April 2004, he said: "Now, by the way, any time you hear the United States government talking about wiretap, it requires – a wiretap requires a court order. Nothing has changed, by the way. When we're talking about chasing down terrorists, we're talking about getting a court order before we do so. It's important for our fellow citizens to understand, when you think Patriot Act, constitutional guarantees are in place when it comes to doing what is necessary to protect our homeland, because we value the Constitution."[5]

- **Is this statement accurate?**

We believe that the statement is accurate when placed in context. As the text of your question itself indicates, in his Buffalo speech, the President was talking about the USA PATRIOT Act, certain provisions of which amended FISA to change the standard for obtaining electronic surveillance orders. In the paragraphs surrounding the portion you quoted, the President reiterated three times that he is discussing the PATRIOT Act. In particular, the President was speaking about the roving wiretap provision of the USA PATRIOT Act, noting that while such wiretaps previously were not available under FISA to intercept the communications of suspected terrorists, "[t]he Patriot Act changed that." When surveillance is conducted under FISA, as amended by the PATRIOT Act, generally we are—as the President said—"talking about getting a court order." The President's statement cannot be taken out of context. In a wide variety of situations, we do not (and at times cannot) get court orders. For example, there is no provision by which the Executive Branch can obtain court orders to conduct certain surveillances overseas.

28. According to press reports, the Administration at some point determined that the authorities provided in the FISA were, in their view, inadequate to support the President's Commander-in-Chief responsibilities.

- **At what point was this determination reached?**
- **Who reached this determination?**

---

[5] Information sharing, Patriot Act Vital to Homeland Security, Remarks by the President in a Conversation on the USA Patriot Act, Kleinshans Music Hall, Buffalo, New York, April 20, 2004

- **If such determination had been reached, why did the Administration conceal the view that existing law was inadequate from the Congress?**

FISA itself permits electronic surveillance authorized by statute, and, as explained above, the Force Resolution satisfies FISA and provides the authorization required for the Terrorist Surveillance Program.

The determination was made, based on the advice of intelligence experts, that we needed an early warning system, one that could help detect and prevent the next catastrophic al Qaeda attack and that might have prevented the attacks of September 11th, had it been in place. As the Department has explained elsewhere, including our paper of January 19, 2006, speed and agility are critical here and "existing law" is *not* inadequate. The Force Resolution, combined with the President's authority under the Constitution, amply supports the Terrorist Surveillance Program. Because "existing law" provides ample authority for the Terrorist Surveillance Program, the Administration did not choose to seek additional statutory authority to support the Program, in part because, as discussed above, the consensus in discussions with congressional leaders was that pursuing such legislation would likely compromise the Program.

It would be inappropriate for us to reveal the confidential and privileged internal deliberations of the Executive Branch, including who made specific recommendations.

29. Based upon press reports, it does not appear that the NSA surveillance program at issue makes use of any intelligence sources and methods which have not been briefed (in a classified setting) to the Intelligence Committees. Other than the adoption of a legal theory which allows the NSA to undertake surveillance which on its face would be prohibited by law, what about this program is secret or sensitive?

- **Is there any precedent for developing a body of secret law such as has been revealed by last month's *New York Times* article about the NSA surveillance program?**

As explained above, the Terrorist Surveillance Program is fully consistent with all applicable federal law, including FISA. Although the broad contours of the Terrorist Surveillance Program have been disclosed, details about the operation of the Terrorist Surveillance Program remain highly classified and exceptionally sensitive. Thus, we must continue to strive to protect the intelligence sources and methods of this vital program. It is important that we not damage national security through revelations of intelligence sources and methods during these proceedings or elsewhere.

The legal authorities for the Terrorist Surveillance Program do not constitute a "body of secret law," as your question suggests. The Force Resolution and its broad authorizing language are public. Nor is it a secret that five Justices of the Supreme Court concluded in *Hamdi v. Rumsfeld* that the Force Resolution authorizes the use of the "fundamental incidents" of war. The breadth of the Force Resolution also has been the subject of prominent law review articles. *See, e.g.*, Curtis A. Bradley & Jack L.

Goldsmith, *Congressional Authorization and the War on Terrorism*, 118 Harv. L. Rev. 2048 (2005); Michael Stokes Paulsen, Youngstown *Goes to War,* 19 Const. Comment. 215, 252 (2002). It has long been public knowledge that other Presidents have concluded that their inherent powers under the Constitution, together with similarly broad authorizations of force, authorized the warrantless interception of international communications during armed conflicts. In short, all of the sources relied upon in the Department's January 19th paper to demonstrate that signals intelligence is a fundamental and accepted incident of the use of military force are readily available to the public.

30. At a public hearing of the Senate/House Joint Inquiry, then-NSA Director Hayden said: "My goal today is to provide you and the American people with as much insight as possible into three questions: (a) What did NSA know prior to September 11th, (b) what have we learned in retrospect, and (c) what have we done in response? I will be as candid as prudence and the law allow in this open session. If at times I seem indirect or incomplete, *I hope that you and the public understand that I have discussed our operations fully and unreservedly in earlier closed sessions*" (emphasis added).[6]

- **Under what, if any, legal authority did General Hayden make this inaccurate statement to the Congress (and to the public)?**

Although the Department cannot speak for General Hayden in this context, it does not appear that the statement was inaccurate. As discussed above, it has long been the practice of both Democratic and Republican administrations under the National Security Act of 1947 to limit full briefings of certain exceptionally sensitive matters to key members of the Intelligence Committees.

31. Were any collection efforts undertaken pursuant to this program based on information obtained by torture?

- **Was the possibility that information obtained by torture would be rejected by the FISA court as a basis for granting a FISA warrant a reason for undertaking this program?**

As the President has repeatedly made clear, the United States does not engage in torture and does not condone or encourage any acts of torture by anyone under any circumstances. In addition, we have already explained our reasons for establishing the

---

[6] Statement for the Record by Lieutenant General Michael V. Hayden, USAF, Director, National Security Agency/Chief. Central Security Service, Before the Joint Inquiry of the Senate Select Committee on Intelligence and the house Permanent Select Committee on Intelligence, 17 October 2002, available at hhtp://intelligence.senate.gov/0210hrg/021017/hayden.pdf.

Terrorist Surveillance Program. It is an early warning system designed to detect and prevent another catastrophic terrorist attack on the United States.

32. If the President determined that a truthful answer to questions posed by the Congress to you, including the questions asked here, would hinder his ability to function as Commander-in-Chief, does the AUMF, or his inherent powers, authorize you to provide false or misleading answers to such questions?

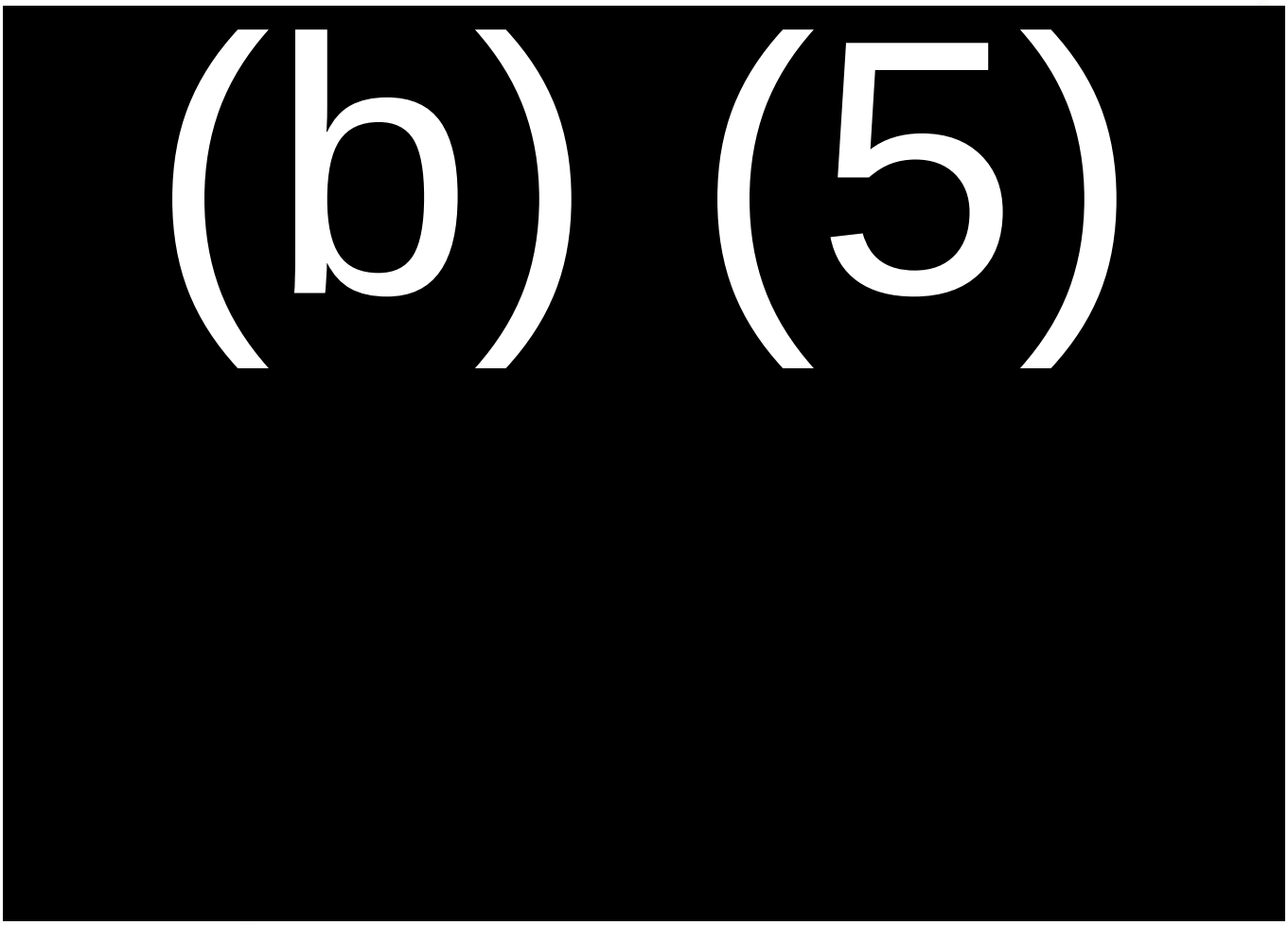
Absolutely not. Congressional oversight is a healthy and necessary part of our democracy. This Administration would not under any circumstances countenance the provision of false or misleading answers to Congress. Under our system of government, no one—particularly not the Attorney General—is permitted to commit perjury. Nor is that something that the Force Resolution authorizes. We are not aware of any theory under which committing perjury before Congress is a fundamental and accepted incident of the use of force.

In those instances where the Administration believes that answering questions about certain intelligence operations would compromise national security, we would follow long-established principles of accommodation between the Branches, by, for example, informing the chairs and vice chairs of the Intelligence Committees, and the House and Senate leaders, as appropriate.

Bradbury, Steve

From: Bradbury, Steve
Sent: Wednesday, March 01, 2006 2:43 PM
To: (b)(3) 50 USC § 3024(m)(1) @dni.gov'; (b)(3) 50 USC § 3605'; 'Harriet_Miers@who.eop.gov'; Brett_C._Gerry@who.eop.gov; 'Brett_M._Kavanaugh@who.eop.gov'; 'Shannen_W._Coffin@ovp.eop.gov'
Cc: Sampson, Kyle; Elwood, Courtney; Moschella, William; Elwood, John; Eisenberg, John; Edney, Michael; Willen, Brian
Subject: Draft DOJ responses to SJC QFRs re NSA hearing
Attachments: Joint Qs of SJC Democrats_3 1 06 v2.doc

Attached is a draft of responses to post-hearing QFRs from SJC Democrats.



-----Original Message-----
From: Miers, Harriet
Sent: Tuesday, May 02, 2006 7:50 PM
To: Perino, Dana M.; 'tasia.scolinos@usdoj.gov'; Gerry, Brett C.; Brown, Jamie E.
Cc: Mamo, Jeanie S.; 'Steve.Bradbury@usdoj.gov'; Kelley, William K.; Kavanaugh, Brett M.
Subject: RE: Boston globe

[redacted] (b) (5)

-----Original Message-----
From: Perino, Dana M.
Sent: Tuesday, May 02, 2006 7:41 PM
To: 'tasia.scolinos@usdoj.gov'; Gerry, Brett C.; Miers, Harriet; Brown, Jamie E.
Cc: Mamo, Jeanie S.
Subject: Boston globe

(b) (5)

Here are his additional questions:

How about real answers to questions such as:

- How can Bush assert that he believes the Constitution forbids Congress from giving executive branch officials the power to act independently of his direction (whistleblower provisions, empowering inspectors and researchers to do things without political interference), given a long line of precedents in which the Supreme Court has upheld such laws (Morrison, Humphrey's Executor, etc)? Same thing on flagging the affirmative action provisions - especially after the '03 Michigan Law School decision?

- In what way is Bush not using this tool as an override-proof line-item veto, given his otherwise inexplicable failure to veto a single bill over the past 5+ years unlike every other president in modern history (including Reagan/Bush41/Clinton)? If that is how it's functioning, under what constitutional theory is that justifiable?

- If that's not it, then what is the real explanation for why Bush is doing this so much more frequently than any predecessor? The talking point that previous administrations have also done this is not an answer, because it's a question of degree. He's broken all records - by far. And he's never issued a veto. Something new and important is obviously happening. What is it, and why?

Etc.

Bradbury, Steve

From: Bradbury, Steve
Sent: Friday, May 05, 2006 2:38 PM
To: 'Brett_M._Kavanaugh@who.eop.gov'
Cc: Macklin, Kristi R
Subject: FW: (b) (5) issues ...
Attachments: tmp.htm; (b) (5) Final.doc

Brett: Attached is summary of (b) (5) cases and materials. I hope this is helpful.

-----Original Message-----
From: Macklin, Kristi R
Sent: Friday, May 05, 2006 2:18 PM
To: Bradbury, Steve
Subject: FW: (b) (5) issues ...

Do you have any recommendations?

-----Original Message-----
From: Brett_M._Kavanaugh@who.eop.gov [mailto:Brett_M._Kavanaugh@who.eop.gov]
Sent: Friday, May 05, 2006 2:14 PM
To: Brett_C._Gerry@who.eop.gov
Cc: Macklin, Kristi R
Subject: (b) (5) issues ...

(b) (5)

duplicate

Macklin, Kristi R

From: Macklin, Kristi R
Sent: Friday, May 05, 2006 4:17 PM
To: Macklin, Kristi R; Brand, Rachel; Cook, Elisebeth C; Jaffer, Jamil N; Sampson, Kyle; 'Neomi_J._Rao@who.eop.gov'; 'Grant_Dixton@who.eop.gov'; 'Brett_C._Gerry@who.eop.gov'; 'Chris Bartolomucci (HBartolomucci@HHLAW.com)'; 'Brian.Benczkowski@mail.house.gov'; 'Raul_F._Yanes (b) (6) '; Richard Klingler (Richard_D._Klingler@who.eop.gov); Bradbury, Steve
Cc: 'William_K._Kelley@who.eop.gov'; 'Brett_M._Kavanaugh@who.eop.gov'; John Persinger (John_M._Persinger@who.eop.gov); 'Kristen_K._Slaughter@who.eop.gov'
Subject: RE: BK Moot - revised
Attachments: BK Moots.doc

Attached is a revised chart noting the addition of Steve Bradbury and Richard Klingler. The moot times are included on the chart. The moots will be held in Room 180 of the EEOB each day. Over the weekend, if you are driving and are not a WH passholder (and have already provided me with your information), please enter at 17th and E - you will be able to park on State Place, which will be the first driveway after entering the gate on the left. My cell phone number i (b) (6) .

BK Moots: 180 EEOB

Saturday: 11:00 – 2:00	**Sunday: 1:30 -4:30**	**Monday: 11:00 – 2:00**
Kristi (b) (5)	Kristi (b) (5)	Kristi (b) (5)
Beth (b) (5)	Beth (b) (5)	Beth (b) (5)
	Rachel (b) (5)	Rachel (b) (5)
Jamil (b) (5)		
		Kyle (b) (5)
	Neomi (b) (5)	Neomi (b) (5)
Grant (b) (5)		
Steve Bradbury (b) (5)		
	Brett (b) (5)	Brett (b) (5)
		Richard Klingler (b) (5)
		Raul (b) (5)
	Chris B. (b) (5)	
Brian (b) (5)	Brian (b) (5)	

Format: We'll plan on doing 10 minute rounds, probably with 2 rounds each. You should cover the topic you are assigned but can ask additional questions on other topic areas if time allows. You should stay out of other participants' topics, but can follow up on other Senators questions on your time. Please don't jump in on another questioner. If you see a big gap in topics, let me know.

(b) (5)

- [redacted] (b) (5)
- [redacted]
- [redacted]
- [redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

- [redacted] (b) (5)
- [redacted]
- [redacted]
- [redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

- [redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

(b) (5)

[redacted]

- [redacted]
- [redacted]
- [redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]

[redacted]

- [redacted]
- [redacted]

[redacted]

- [redacted]
- [redacted]

[redacted] (b) (5)

- [redacted]
- [redacted]
- [redacted]

Bradbury, Steve

From: Bradbury, Steve
Sent: Friday, May 05, 2006 5:08 PM
To: 'Brett_M._Kavanaugh@who.eop.gov'
Cc: Macklin, Kristi R
Subject: Presidental Signing Statements
Attachments: Presidential Signing Statements (5-5-2006).pdf

Brett: [redacted (b) (5)]. Please note that DOJ is sharing these talking points with reporters and others outside the Executive Branch. Steve

PRESIDENTIAL SIGNING STATEMENTS

Like many Presidents before him, President Bush has issued statements on signing legislation into law. Presidents have used these "signing statements" for a variety of purposes. Sometimes Presidents use signing statements to explain to the public, and more particularly to interested constituencies, what the President understands to be the likely effects of the bill.

Presidents throughout history also have issued what some have called "constitutional" signing statements, and it is this use of the signing statement that has recently been the subject of public attention. Presidents are sworn to "preserve, protect, and defend the Constitution," and thus are responsible for ensuring that the manner in which they enforce acts of Congress is consistent with America's founding document. Presidents have long used signing statements for the purpose of "informing Congress and the public that the Executive believes that a particular provision would be unconstitutional in certain of its applications," Office of Legal Counsel, *The Legal Significance of Presidential Signing Statements*, 17 Op. O.L.C. 131, 131 (1993) (*available at* http://www.usdoj.gov/olc/signing.htm); Office of Legal Counsel, *Presidential Authority to Decline to Execute Unconstitutional Statutes*, 18 Op. O.L.C. 199, 202 (1994) ("[E]very President since Eisenhower has issued signing statements in which he stated that he would refuse to execute unconstitutional provisions") (*available at* http://www.usdoj.gov/olc/nonexcut.htm), or for stating that the President will interpret or execute provisions of a law in a manner that would avoid constitutional infirmities. As Assistant Attorney General Walter Dellinger noted early during the Clinton Administration, "[s]igning statements have *frequently* expressed the President's intention to construe or administer a statute in a particular manner (*often* to save the statute from unconstitutionality)." 17 Op. O.L.C. at 132 (emphasis added).

President Bush, like many of his predecessors dating back at least to President James Monroe, has issued constitutional signing statements. The constitutional concerns identified in these statements often concern provisions of law that could be read to infringe explicit constitutional provisions (such as the Recommendations Clause, the Presentment Clauses, and the Appointments Clause) or to violate specific constitutional holdings of the Supreme Court. Common examples are provided below.

President Bush's use of "signing statements" is consistent with tradition.

- Presidents have issued constitutional signing statements since the early years of the Republic. One scholar identifies President James Monroe as the first to issue a constitutional signing statement, when he stated that he would construe a statutory provision in a manner that did not conflict with his prerogative to appoint officers. *See* Christopher Kelley, *A Comparative Look at the Constitutional Signing Statement* 5 (2003) (*available at* http://mpsa.indiana.edu/conf2003papers/1031858822). Louis Fisher of the Congressional Research Service notes that in 1830, Andrew Jackson "signed a bill and simultaneously sent to Congress a message" setting forth his interpretation "that restricted the reach of

the statute." 17 Op. O.L.C. at 138 (quoting Louis Fisher, *Constitutional Conflicts between Congress and the President* 128 (3d ed. 1991)). Assistant Attorney General Dellinger conducted a thorough study and concluded that "signing statements of this kind can be found as early as the Jackson and Tyler Administrations, and later Presidents, including Lincoln, Andrew Johnson, Theodore Roosevelt, Wilson, Franklin Roosevelt, Truman, Eisenhower, Lyndon Johnson, Nixon, Ford and Carter, also engaged in the practice." 17 Op. O.L.C. at 138.

- In recent presidencies, the use of the constitutional signing statement has become more common. While the task of counting signing statements is inexact because of difficulties in characterizing some statements, Presidents Reagan, George H.W. Bush, Clinton, and George W. Bush have issued constitutional signing statements with respect to similar numbers of laws. According to one scholar, President Reagan issued constitutional signing statements with respect to 71 laws; George H.W. Bush, 146; Clinton, 105. *See* Kelley, *supra*, at 18. By our count, President Bush has issued such statements with respect to 104 laws as of January of this year.

The practice of issuing signing statements does not, as some critics have charged, mean that a President has acted contrary to law.

- The practice is consistent with, and derives from, the President's constitutional obligations, and is an ordinary part of a respectful constitutional "dialogue" between the Branches.

- The Constitution requires the President to take an oath to "preserve, protect, and defend the Constitution," and directs him to "take care that the Laws be faithfully executed." When Congress passes legislation containing provisions that could be construed or applied in certain cases in a manner as contrary to well settled constitutional principles, the President can and should take steps to ensure that such laws are interpreted and executed in a manner consistent with the Constitution.

    - The Constitution contemplates that Presidents interpret laws in the course of implementing them. The Supreme Court specifically has stated that the President has the power to "supervise and guide [Executive officers'] construction of the statutes under which they act in order to secure that unitary and uniform execution of the laws which Article II of the Constitution evidently contemplated in vesting general executive power in the President alone," *Myers v. United States*, 272 U.S. 52, 135 (1926); *see also Bowsher v. Synar*, 478 U.S. 714, 733 (1986) ("Interpreting a law enacted by Congress to implement the legislative mandate is the very essence of 'execution' of the law.").

- Employing signing statements to advise Congress of constitutional objections is actually *more respectful* of Congress's role as an equal branch of government than the alternatives proposed by some critics.

    - Recent administrations, including the Reagan, George H.W. Bush, and Clinton Administrations, consistently have taken the position that "the Constitution provides [the President] with the authority to decline to enforce a clearly unconstitutional law." 17 Op. O.LC. at 133 (opinion of Assistant Attorney General Dellinger) (noting that understanding is "consistent with the view of the Framers" and has been endorsed by many members of the Supreme Court); 18 Op. O.L.C. at 199 (opinion of Assistant Attorney General Dellinger) (noting that "consistent and substantial executive practice" since "at least 1860 assert[s] the President's authority to decline to effectuate enactments that the President views as unconstitutional"); *Attorney General's Duty to Defend and Enforce Constitutionally Objectionable Legislation*, 4A Op. O.L.C. 55, 59 (1980) (opinion of Benjamin R. Civiletti, Attorney General to President Carter) ("the President's constitutional duty does not require him to execute unconstitutional statutes"); *see also* 2 Debates in the Several State Conventions on the Adoption of the Federal Constitution 446 (2d ed. 1836) (noting that just as judges have a duty "to pronounce [an unconstitutional law] void . . . In the same manner, the President of the United States could . . . refuse to carry into effect an act that violates the Constitution.") (statement of James Wilson, signer of Constitution from Pennsylvania). Rather than tacitly placing limitations on the enforcement of provisions (or declining to enforce them), as has been done in the past, signing statements promote a constitutional dialogue with Congress by openly stating the interpretation that the President will give certain provisions.

    - It is not the case, as some have suggested, that the President's only option when confronting a bill containing a provision that is constitutionally problematic is to veto the bill. Presidents Jefferson (*e.g.*, the Louisiana Purchase), Lincoln, Theodore Roosevelt, Wilson, Franklin Roosevelt, Truman, Eisenhower, Kennedy, Lyndon Johnson, Ford, and Carter have signed legislation rather than vetoing it despite concerns that the legislation posed constitutional concerns. *See* 17 Op. O.L.C. at 132 nn.3 & 5, 134, 138; *see INS v. Chadha*, 462 U.S. 919, 942 n.13 (1983) ("it is not uncommon for Presidents to approve legislation containing parts which are objectionable on constitutional grounds").

- Compared to vetoing a bill, giving constitutionally infirm provisions a "saving" interpretation through a signing statement gives fuller effect to the wishes of Congress by giving complete effect to the vast majority of a law's provisions. This approach is not, as some have suggested, an affront to Congress. Instead, it gives effect to the well established legal presumption that Congress did not enact an unconstitutional provision. As Assistant Attorney General Dellinger explained, this practice is "analogous to the Supreme Court's practice of construing statutes, where possible, to avoid holding them unconstitutional." A veto, by comparison, would render all of Congress's work a nullity, even if, as is often the case, the constitutional concerns involve relatively minor provisions of major legislation.

- This approach is also fully consistent with past practice. As Assistant Attorney General Dellinger explained early during the Clinton Administration: "In light of our constitutional history, we do not believe that the President is under any duty to veto legislation containing a constitutionally infirm provision." Rather, giving problematic provisions a "saving" construction in a signing statement "serve[s] legitimate and defensible purposes." 17 Op. O.L.C. at 137; *see also* 18 Op. O.L.C. at 202-203 ("the President has the authority to sign legislation containing desirable elements while refusing to execute a constitutionally defective position").

Many of President Bush's constitutional signing statements have sought to preserve three specific constitutional provisions that are sometimes overlooked in the legislative process: the Recommendations Clause; the Presentment Clauses; and the Appointments Clause. While critics claim that the President has used signing statements in "unprecedented fashion," his constitutional signing statements are completely consistent with those of his predecessors.

- **Recommendations Clause**. Presidents commonly have raised objections when Congress purports to *require* the President to submit legislative recommendations, because the Constitution vests the President with discretion to do so when he sees fit, stating that he "shall from time to time . . . recommend to [Congress's] Consideration such Measures as he shall judge necessary and expedient." U.S. Const., Art. II, § 3, cl. 1.

    - President Bush raised this objection 55 times in his 104 constitutional signing statements.
    - Bush: "To the extent that provisions of the Act, such as sections 614 and 615, purport to require or regulate submission by executive branch officials of legislative recommendations to the Congress, the executive branch shall construe such provisions in a manner consistent with the President's constitutional authority to

supervise the unitary executive branch and to submit for congressional consideration such measures as the President judges necessary and expedient." *Statement on Signing the Intelligence Authorization Act for Fiscal Year 2005* (Dec. 23, 2004).

- Clinton: "Because the Constitution preserves to the President the authority to decide whether and when the executive branch should recommend new legislation, Congress may not require the President or his subordinates to present such recommendations (section 6). I therefore direct executive branch officials to carry out these provisions in a manner that is consistent with the President's constitutional responsibilities." *Statement on Signing the Shark Finning Prohibition Act* (Dec. 26, 2000).

- **Presentment Clauses/Bicameralism/*INS v. Chadha.*** Presidents commonly raise objections when Congress purports to authorize a single House of Congress to take action on a matter in violation of the well established rule, embodied in the Supreme Court's decision in *INS v. Chadha*, 462 U.S. 919, 958 (1983), that Congress can act only by "passage by a majority of both Houses and presentment to the President." *See* U.S. Const., Art. I, § 7 (requiring that bills and resolutions pass both Houses before being presented to the President).

    - President Bush raised this objection 44 times in his 104 constitutional signing statements.
    - Bush: "The executive branch shall construe certain provisions of the Act that purport to require congressional committee approval for the execution of a law as calling solely for notification, as any other construction would be inconsistent with the constitutional principles enunciated by the Supreme Court of the United States in *INS v. Chadha*." *Statement on Signing the Departments of Labor, Health and Human Services, and Education, and Related Agencies Appropriations Act* (Dec. 30, 2005).
    - Clinton: "There are provisions in the Act that purport to condition my authority or that of certain officers to use funds appropriated by the Act on the approval of congressional committees. My Administration will interpret such provisions to require notification only, since any other interpretation would contradict the Supreme Court ruling in *INS v. Chadha*." *Statement on Signing the Consolidated Appropriations Act, FY 2001* (Dec. 21, 2000).

- **Appointments Clause.** The Appointments Clause of the Constitution, U.S. Const., Art. II, § 2, provides that the President, with the advice and consent of the Senate, shall appoint principal officers of the United States (heads of agencies, for example); and that "inferior officers" can be appointed *only* by the President, by the heads of "Departments" (agencies), or by the courts. Presidents commonly raise an objection when Congress purports to restrict the President's ability to

appoint officers, or to vest entities other than the President, agency heads, or courts with the power to appoint officers.

- President Bush raised this objection 19 times in his 104 constitutional signing statements.
- Bush: "The executive branch shall construe the described qualifications and lists of nominees under section 4305(b) as recommendations only, consistent with the provisions of the Appointments Clause of the Constitution." *Statement on Signing the Safe, Accountable, Flexible, Efficient Transportation Equity Act: A Legacy for Users* (Aug. 10, 2005).
- Clinton: "Under section 332(b)(1) of the bill, the President would be required to make such appointments from lists of candidates recommended by the National Association of Insurance Commissioners. The Appointments Clause, however, does not permit such restrictions to be imposed upon the President's power of appointment. I therefore do not interpret the restrictions of section 332(b)(1) as binding and will regard any such lists of recommended candidates as advisory only." *Statement on Signing Legislation To Reform the Financial System* (Nov. 12, 1999).

Many of President Bush's constitutional signing statements have sought to preserve the confidentiality of national security information.

- The Supreme Court has held that the Constitution gives the President authority to control the access of Executive Branch officials to classified information. The President's "authority to classify and control access to information bearing on national security and to determine whether an individual is sufficiently trustworthy to occupy a position in the Executive Branch that will give that person access to such information flows primarily from this constitutional investment of power in the President and *exists quite apart from any explicit congressional grant*." *Dep't of Navy v. Egan*, 484 U.S. 518, 527 (1988). Presidents commonly have issued signing statements when newly enacted provisions might be construed to involve the disclosure of sensitive information.

  - President Bush raised this objection 60 times in his 104 constitutional signing statements.
  - Bush: "Sections 2(5) and 2(6) of the Act purport to require the annual report of the Secretary of the Treasury to include a description of discussions between the United States and Mexican governments. In order to avoid intrusion into the President's negotiating authority and ability to maintain the confidentiality of diplomatic negotiations, the executive branch will not interpret this provision to require the disclosure of either the contents of diplomatic communications or specific plans for particular negotiations in the future." *Statement on Signing Legislation on*

Amendments to the Mexico-United States Agreement on the Border Environment Cooperation Commission and the North American Development Bank (Apr. 5, 2004).

- Clinton: "A number of other provisions of this bill raise serious constitutional concerns. Because the President is the Commander in Chief and the Chief Executive under the Constitution, the Congress may not interfere with the President's duty to protect classified and other sensitive national security information or his responsibility to control the disclosure of such information by subordinate officials of the executive branch (sections 1042, 3150, and 3164) . . . . To the extent that these provisions conflict with my constitutional responsibilities in these areas, I will construe them where possible to avoid such conflicts, and where it is impossible to do so, I will treat them as advisory. I hereby direct all executive branch officials to do likewise." *Statement on Signing the National Defense Authorization Act for Fiscal Year 2000* (Oct. 5, 1999).
- Eisenhower: "I have signed this bill on the express premise that the three amendments relating to disclosure are not intended to alter and cannot alter the recognized Constitutional duty and power of the Executive with respect to the disclosure of information, documents, and other materials. Indeed, any other construction of these amendments would raise grave Constitutional questions under the historic Separation of Powers Doctrine." Pub. Papers of Dwight D. Eisenhower 549 (1959).

President Bush also has used signing statements to safeguard the President's well-established role in the Nation's foreign affairs and the President's wartime power. These signing statements also are in keeping with the practice of his predecessors.

- While some critics have argued that President Bush has increased the use of Presidential signing statements, any such increase must be viewed in light of current events and the legislative response to those events. While President Bush has issued numerous signing statements of this sort, the significance of legislation affecting national security has increased markedly since the September 11th attacks and Congress's authorization of the use of military force against the terrorists who perpetrated those attacks. Even before the War on Terror, President Clinton issued numerous such statements. One scholar identified this objection as the most common use of the constitutional signing statements by Presidents Clinton and George H.W. Bush, because it is in this area "where presidential power is at its zenith." Kelley, *supra*, at 18.

    - Bush: "Section 107 of the Act purports to direct negotiations with foreign governments and international organizations. The executive branch shall implement section 107 in a manner consistent with the Constitution's grant to the President of the

authority to conduct the foreign affairs of the United States." *Statement on Signing the North Korean Human Rights Act of 2004* (Oct. 18, 2004).

- Bush: "The executive branch shall construe subsection 1025(d) of the Act, which purports to determine the command relationships among certain elements of the U.S. Navy forces, as advisory, as any other construction would conflict with the President's constitutional authority as Commander in Chief." *Statement on Signing the Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief Act, 2005* (May 11, 2005).
- Clinton: "Section 610 of the Commerce/Justice/State appropriations provision prohibits the use of appropriated funds for the participation of U.S. armed forces in a U.N. peacekeeping mission under foreign command unless the President's military advisers have recommended such involvement and the President has submitted such recommendations to the Congress. The 'Contributions for International Peacekeeping Activities' provision requires a report to the Congress prior to voting for a U.N. peacekeeping mission. These provisions unconstitutionally constrain my diplomatic authority and my authority as Commander in Chief, and I will apply them consistent with my constitutional responsibilities." *Statement on Signing the Omnibus Consolidated and Emergency Supplemental Appropriations Act* (Oct. 23, 1998).
- Clinton: "I also oppose language in the Act related to the Kyoto Protocol. . . . My Administration's objections to these and other language provisions have been made clear in previous statements of Administration policy. I direct the agencies to construe these provisions to be consistent with the President's constitutional prerogatives and responsibilities and where such a construction is not possible, to treat them as not interfering with those prerogatives and responsibilities." *Statement on Signing the Departments of Commerce, Justice, State, the Judiciary, and Related Agencies Appropriations Act* (Dec. 21, 2000).
- Carter: Congress "cannot mandate the establishment of consular relations at a time and place unacceptable to the President." *Statement on Signing the FY 1980-81 Department of State Appropriations Act*, *see* 2 Pub. Papers of Jimmy Carter 1434 (1979).
- Nixon: Mansfield Amendment setting a final date for the withdrawal of U.S. Forces from Indochina was "without binding force or effect." Pub. Papers of Richard Nixon 1114 (1971).
- Truman: "I do not regard this provision [involving loans to Spain] as a directive, which would be unconstitutional, but instead as an authorization, in addition to the authority already in existence under which loans to Spain may be made." *Statement on Signing*

the General Appropriations Act of 1951, Pub. Papers of Harry S. Truman 616 (1950).

- Wilson: Expressed an intention not to enforce a provision on the grounds it was unconstitutional because doing so "would amount to nothing less than the breach or violation" of some thirty-two treaties. Louis Fisher, *Constitutional Conflicts between Congress and the President* 134 (4th ed. 1997).

Harriet_Miers@who.eop.gov

From:	Harriet_Miers@who.eop.gov
Sent:	Thursday, May 11, 2006 9:04 PM
To:	Scolinos, Tasia; Bradbury, Steve; Elwood, John; Roehrkasse, Brian; Kenneth_A._Lisaius@who.eop.gov; Dana_M._Perino@who.eop.gov
Cc:	Eisenberg, John; Brett_C._Gerry@who.eop.gov; (b)(3) 50 USC § 3024(m)(1) @dni.gov; Dan_Bartlett@who.eop.gov; Brett_M._Kavanaugh@who.eop.gov; William_K._Kelley@who.eop.gov; Joel_D._Kaplan@who.eop.gov; Michael_Allen@nsc.eop.gov
Subject:	RE: Talking Points
Attachments:	(b) (5) Talkers (5-11-06).doc

One additional change... (b) (5) Additionally, Ben Powell had some interesting suggestions about (b) (5). I will ask him to send his comments around if he would like to do so.

-----Original Message-----
From: John.Elwood@usdoj.gov [mailto:John.Elwood@usdoj.gov]
Sent: Thursday, May 11, 2006 8:53 PM
To: Brian.Roehrkasse@usdoj.gov; Steve.Bradbury@usdoj.gov; Tasia.Scolinos@usdoj.gov; Lisaius, Kenneth A.; Perino, Dana M.
Cc: John.Eisenberg@usdoj.gov; Miers, Harriet; Gerry, Brett C.
Subject: RE: Talking Points

I understand that Steve has had a conversation with Harriet and that these are cleared for use. Thank you.

-----Original Message-----
From: Roehrkasse, Brian
Sent: Thursday, May 11, 2006 7:19 PM
To: Elwood, John; Bradbury, Steve; Scolinos, Tasia; 'Kenneth_A._Lisaius@who.eop.gov'; 'Dana_M._Perino@who.eop.gov'
Cc: Eisenberg, John; 'Brett_C._Gerry@who.eop.gov'
Subject: RE: Talking Points

OK - I assume these are now cleared by OLC/DOJ. Has the WH cleared?

-----Original Message-----
From: Elwood, John
Sent: Thursday, May 11, 2006 7:14 PM
To: Bradbury, Steve; Roehrkasse, Brian; Scolinos, Tasia; 'Kenneth_A._Lisaius@who.eop.gov'; 'Dana_M._Perino@who.eop.gov'
Cc: Eisenberg, John; 'Brett_C._Gerry@who.eop.gov'

Subject: RE: Talking Points

I would propose using these talking points, which are revised from Draft #4.

-----Original Message-----
From: Bradbury, Steve
Sent: Thursday, May 11, 2006 7:12 PM
To: Roehrkasse, Brian; Scolinos, Tasia; 'Kenneth_A._Lisaius@who.eop.g
ov'; 'Dana_M._Perino@who.eop.gov'
Cc: Eisenberg, John; 'Brett_C._Gerry@who.eop.gov'; Elwood, John
Subject: RE: Talking Points

Pls include John Elwood in these messages. Thx

-----Original Message-----
From: Roehrkasse, Brian
Sent: Thursday, May 11, 2006 7:10 PM
To: Scolinos, Tasia; Bradbury, Steve; 'Kenneth_A._Lisaius@who.eop.gov'; 'Dana_M._Perino@who.eop.
gov'
Cc: Eisenberg, John; 'Brett_C._Gerry@who.eop.gov'; Eisenberg, John
Subject: RE: Talking Points

Not to confuse things anymore, but assuming that DRAFT 4 is the latest and final draft, (b) (5) [redacted]

-----Original Message-----
From: Scolinos, Tasia
Sent: Thursday, May 11, 2006 7:05 PM
To: Roehrkasse, Brian; Bradbury, Steve; 'Kenneth_A._Lisaius@who.eop.g
ov'; 'Dana_M._Perino@who.eop.gov'
Cc: Eisenberg, John; 'Brett_C._Gerry@who.eop.gov'; Eisenberg, John
Subject: RE: Talking Points

Just so we are clear, the Draft #4 Legal Authority Talking Points are cleared and we are just waiting for additional Q and A's from OLC?

-----Original Message-----
From: Roehrkasse, Brian
Sent: Thursday, May 11, 2006 6:35 PM
To: Bradbury, Steve; Scolinos, Tasia; 'Kenneth_A._Lisaius@who.eop.gov'; 'Dana_M._Perino@who.eop.
gov'
Cc: Eisenberg, John; 'Brett_C._Gerry@who.eop.gov'; Eisenberg, John
Subject: RE: Talking Points

Are the legal authority points the draft 4 from the correspondence at 4:06 below or are there new points?

points?

-----Original Message-----
From: Roehrkasse, Brian
Sent: Thursday, May 11, 2006 4:06 PM
To: 'Harriet_Miers@who.eop.gov'; Dana_M._Perino@who.eop.gov; William_K._Kelley@who.eop.gov; Brett_C._Gerry@who.eop.gov
Cc: Scolinos, Tasia; Dan_Bartlett@who.eop.gov; Catherine_Martin@who.eop.gov; Michele_A._Davis@nsc.eop.gov; Tony_Snow@who.eop.gov; Bradbury, Steve; Eisenberg, John
Subject: RE: Need whc help

That is correct. We made a few minor edits to [redacted] (b) (5) [redacted] and OLC changed the sentence [redacted] (b) (5) [redacted]

-----Original Message-----
From: Bradbury, Steve
Sent: Thursday, May 11, 2006 6:33 PM
To: Scolinos, Tasia; 'Kenneth_A._Lisaius@who.eop.gov'; 'Dana_M._Perino@who.eop.gov'
Cc: Eisenberg, John; Roehrkasse, Brian; 'Brett_C._Gerry@who.eop.gov'; Eisenberg, John
Subject: RE: Talking Points

John Elwood and John Eisenberg are working on the Q&As right now and will get them back around ASAP. There are legal authority talking points, which I believe are final. The core of those talkers are incorporated into the Q&As, I believe.

-----Original Message-----
From: Scolinos, Tasia
Sent: Thursday, May 11, 2006 6:27 PM
To: 'Kenneth_A._Lisaius@who.eop.gov'; Dana_M._Perino@who.eop.gov
Cc: Eisenberg, John; Bradbury, Steve; Roehrkasse, Brian; Brett_C._Gerry@who.eop.gov
Subject: RE: Talking Points

I just want to be clear on this point because DOJ is under the impression that we are waiting for final WH clearance on the talking points.

-----Original Message-----
From: Kenneth_A._Lisaius@who.eop.gov [mailto:Kenneth_A._Lisaius@who.eop.gov]
Sent: Thursday, May 11, 2006 6:19 PM
To: Scolinos, Tasia; Dana_M._Perino@who.eop.gov
Subject: FW: Talking Points

From: Persinger, John M.
Sent: Thursday, May 11, 2006 6:18 PM
To: Lisaius, Kenneth A.

Subject: Talking Points

Bill said Justice is still finalizing the Talking Points.
They know they are urgent but Bill does not have a specific timeline.

Roehrkasse, Brian

From:	Roehrkasse, Brian
Sent:	Friday, May 12, 2006 8:43 AM
To:	Scolinos, Tasia; Bradbury, Steve; Elwood, John; Kenneth_A._Lisaius@who.eop.gov; Dana_M._Perino@who.eop.gov; Brett_C._Gerry@who.eop.gov; Eisenberg, John
Cc:	(b)(3) 50 USC § 3024(m)(1) @dni.gov; Dan_Bartlett@who.eop.gov; Brett_M._Kavanaugh@who.eop.gov; William_K._Kelley@who.eop.gov; Joel_D._Kaplan@who.eop.gov; Michael_Allen@nsc.eop.gov; Sampson, Kyle; Moschella, William; Tony_Snow@who.eop.gov; 'Harriet_Miers@who.eop.gov'; Scolinos, Tasia
Subject:	FINAL DRAFT Q&A/Talking Points
Attachments:	(b) (5) Talkers Final Draft.doc
Importance:	High

I have reformatted last night's final draft Q & A for ease of reading including combining questions 2 and 3 since they have the same answer. (b) (5) . Please let me know if these are the final Q & As.

Thanks.

William_K._Kelley@who.eop.gov

From:	William_K._Kelley@who.eop.gov
Sent:	Friday, May 12, 2006 9:14 AM
To:	Scolinos, Tasia; Bradbury, Steve; Elwood, John; Eisenberg, John; Roehrkasse, Brian; Kenneth_A._Lisaius@who.eop.gov; Dana_M._Perino@who.eop.gov; Brett_C._Gerry@who.eop.gov
Cc:	Sampson, Kyle; Moschella, William; Harriet_Miers@who.eop.gov; Michael_Allen@nsc.eop.gov; (b)(3) 50 USC § 3024(m)(1) @dni.gov; Dan_Bartlett@who.eop.gov; Brett_M._Kavanaugh@who.eop.gov; Joel_D._Kaplan@who.eop.gov; Tony_Snow@who.eop.gov
Subject:	Re: FINAL DRAFT Q&A/Talking Points

Fine by me.

-----Original Message-----
From: Brian.Roehrkasse@usdoj.gov <Brian.Roehrkasse@usdoj.gov>
To: Tasia.Scolinos@usdoj.gov <Tasia.Scolinos@usdoj.gov>; Steve.Bradbury@usdoj.gov <Steve.Bradbury@usdoj.gov>; John.Elwood@usdoj.gov <John.Elwood@usdoj.gov>; John.Eisenberg@usdoj.gov <John.Eisenberg@usdoj.gov>; Lisaius, Kenneth A. <Kenneth_A._Lisaius@who.eop.gov>; Perino, Dana M. <Dana_M._Perino@who.eop.gov>; Gerry, Brett C. <Brett_C._Gerry@who.eop.gov>
CC: Kyle.Sampson@usdoj.gov <Kyle.Sampson@usdoj.gov>; William.Moschella@usdoj.gov <William.Moschella@usdoj.gov>; Miers, Harriet <Harriet_Miers@who.eop.gov>; Tasia.Scolinos@usdoj.gov <Tasia.Scolinos@usdoj.gov>; Allen, Michael <Michael_Allen@nsc.eop.gov>; (b)(3) 50 USC § 3024(m)(1) @dni.gov <(b)(3) 50 USC § 3024(m)(1) @dni.gov>; Bartlett, Dan <Dan_Bartlett@who.eop.gov>; Kavanaugh, Brett M. <Brett_M._Kavanaugh@who.eop.gov>; Kelley, William K. <William_K._Kelley@who.eop.gov>; Kaplan, Joel <Joel_D._Kaplan@who.eop.gov>; Snow, Tony <Tony_Snow@who.eop.gov>
Sent: Fri May 12 08:42:14 2006

duplicate

Dan_Bartlett@who.eop.gov

From:	Dan_Bartlett@who.eop.gov
Sent:	Friday, May 12, 2006 9:31 AM
To:	Scolinos, Tasia; Bradbury, Steve; Elwood, John; Roehrkasse, Brian; Harriet_Miers@who.eop.gov; Kenneth_A._Lisaius@who.eop.gov; Dana_M._Perino@who.eop.gov
Cc:	Eisenberg, John; Brett_C._Gerry@who.eop.gov; (b)(3) 50 USC § 3024(m)(1) @dni.gov; Brett_M._Kavanaugh@who.eop.gov; William_K._Kelley@who.eop.gov; Joel_D._Kaplan@who.eop.gov; Michael_Allen@nsc.eop.gov
Subject:	FINAL TALKING POINTS
Attachments:	(b) (5) Talkers.Final (5-11-06).doc

Please use these.

Brett_M._Kavanaugh@who.eop.gov

From: Brett_M._Kavanaugh@who.eop.gov
Sent: Friday, May 12, 2006 4:36 PM
To: Bradbury, Steve
Subject: RE:

Steve: Belated thanks for this kind email. I am glad to be on to the next step!

-----Original Message-----
From: Steve.Bradbury@usdoj.gov [mailto:Steve.Bradbury@usdoj.gov]
Sent: Tuesday, May 09, 2006 6:00 PM
To: Kavanaugh, Brett M.
Subject:

Brett: Congratulations on successfully completing a second hearing.
You did a great job today!

Brett_M._Kavanaugh@who.eop.gov

From: Brett_M._Kavanaugh@who.eop.gov
Sent: Monday, May 29, 2006 3:11 PM
To: Bradbury, Steve
Subject: RE: The Newest Judge on the D.C. Circuit

Steve:

Thanks for the kind words. I have appreciated and learned from the work ethic, sound judgment, and intellectual integrity you have demonstrated in your work at K&E and in the government. I look forward to seeing you soon.

Brett

-----Original Message-----
From: Steve.Bradbury@usdoj.gov [mailto:Steve.Bradbury@usdoj.gov]
Sent: Friday, May 26, 2006 12:00 PM
To: Kavanaugh, Brett M.
Subject: FW: The Newest Judge on the D.C. Circuit

Congratulations to you, Brett, and to us all!!! Phenomenal news for the Republic!!!

From: Elwood, John
Sent: Friday, May 26, 2006 11:54 AM
To: OLC_Attorneys
Subject: The Newest Judge on the D.C. Circuit

http://www.senate.gov/legislative/LIS/roll_call_lists/roll_call_vote_cfm
.cfm?congress=109&session=2&vote=00159