

FEDERAL BUREAU OF INVESTIGATION
 FOI/PA
 DELETED PAGE INFORMATION SHEET
 17th Interim Release
 Civil Action# 18-cv-1833, FOIA 1404359-0

Total Withheld Page(s) =92

Bates Page Reference	Reason for Withholding (i.e., exemptions with coded rationale, duplicate, sealed by order of court, etc.)
18-cv-1833 - 7356-7357	Referral Consult
7361, 7363-7367	(b)(5)-1, (b)(7)(E)-6
7362	(b)(5)-1, (b)(6)-2, (b)(7)(C)-2, (b)(7)(E)-6
7377	Duplicate of Bates Page 7374
7447-7486	(b)(6)-4, (b)(7)(C)-4
7488-7527	Duplicate to Bates Pages 7447-7486
7587-7588	(b)(6)-2, 4, (b)(7)(C)-2, 4

XXXXXXXXXXXXXXXXXXXXXXXXXXXXX
 X Deleted Page(s) X
 X No Duplication Fee X
 X For this Page X
 XXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Friday, January 13, 2017 4:46 PM
To: [REDACTED] (DO) (FBI)
Subject: Re: OGE 450 Training
Attachments: x9y8z.pdf

b6 -1
b7C -1

Just passed my course!!! Yay for me.

Since i don't have the right acrobat, i couldn't save my fancy certificate with my name written it. But here's what i have d

From: [REDACTED] (DO) (FBI)
Sent: Friday, January 13, 2017 3:20 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: OGE 450 Training

b6 -1
b7C -1

Okay let me know if you can't get in and we will have to come up with another plan. I just tried too and can't get in but I could yesterday. I have the name of someone at the field office who you can schedule a time with and get into the building.

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

From: Richman, Daniel C. (DO) (OGA)
Sent: Friday, January 13, 2017 3:15 PM
To: [REDACTED] (DO) (FBI) [REDACTED]
Subject: Re: OGE 450 Training

b6 -1
b7C -1
b7E -3

I've been trying for a while today to get onto the OGE site, but without success. Wonder whether the agency's new high profile has led to too much traffic. At any rate, I'll keep trying, but can't promise I get thru in time to be included in your stats d _____

From: [REDACTED] (DO) (FBI)
Sent: Friday, January 13, 2017 8:51 AM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: OGE 450 Training

b6 -1
b7C -1

Please let me know when you are done with the training. I have to turn in stats today. Thanks.

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

From: [REDACTED] (DO) (FBI)
Sent: Thursday, January 12, 2017 8:08 AM
To: Richman, Daniel C. (DO) (OGA) [REDACTED] (DO) (FBI)
[REDACTED]
Subject: RE: OGE 450 Training

b6 -1
b7C -1
b7E -3

Great that there is an on line course you can take and you don't have to go into the NY office. Let me know when you are done. Thanks.

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

From: Richman, Daniel C. (DO) (OGA)

FBI 18-CV-1833-7350

Sent: Wednesday, January 11, 2017 5:08 PM

To: [REDACTED] (DO) (FBI) [REDACTED] (DO) (FBI)

b6 -1,4
b7C -1,4
b7E -3

Subject: Re: OGE 450 Training

sorry for the delay. Messy day. My cell is [REDACTED] But in the interim, [REDACTED] told me that The required SGE training can be found on OGE's website:

<https://www.oge.gov/web/oge.nsf/Education%20Resources%20for%20Ethics%20Officials/1BB7E0DEBDD562D885257F6A0077E2FE?opendocument>

so I guess I'll go there. Happy to chat if there's more to discuss and thanks again for all your help dan richman

From: [REDACTED] (DO) (FBI)

b6 -1
b7C -1

Sent: Wednesday, January 11, 2017 11:44 AM

To: [REDACTED] (DO) (FBI); Richman, Daniel C. (DO) (OGA)

Subject: RE: OGE 450 Training

Thanks, [REDACTED]

Daniel-- let me know your best number to call you.

[REDACTED]

b6 -1
b7C -1
b7E -3

[REDACTED]

Chief, Ethics and Integrity Unit (EIU)

Office of Integrity and Compliance (OIC)

Desk: [REDACTED] Mobile: [REDACTED]

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

From: [REDACTED] (DO) (FBI)

b6 -1
b7C -1
b7E -3

Sent: Wednesday, January 11, 2017 11:32 AM

To: Richman, Daniel C. (DO) (OGA) [REDACTED]

Cc: [REDACTED] (DO) (FBI) [REDACTED]

Subject: RE: OGE 450 Training

Daniel, [REDACTED] is the Unit Chief over the ethics program. He can talk to you by phone for the training. He will contact you.

Also, the actual OGE 450 is due to me by 2/15/2017. Any questions, let me know. Thanks.

[REDACTED]

Administrative Management and Administrative Unit, Resource Planning Unit/Director's Office JEH,
Room 9798 [REDACTED]

b6 -1
b7C -1
b7E -3

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

FBI 18-CV-1833-7351

From: Richman, Daniel C. (DO) (OGA)
Sent: Monday, January 09, 2017 6:05 PM

To: [REDACTED] (DO) (FBI) [REDACTED]
Subject: Re: OGE 450 Training

b6 -1
b7C -1
b7E -3

You put your finger on the problem. Over a year ago, I was set up in the NYO SCIF, where I can get high-side access, but I don't have a current POC there. But you're right to imply that I ought to take care of this now. I have a card from [REDACTED] the Assoc Chief Sec Off at NYO, who I met way back. I will reach out to him (unless you have a better idea) d _____

From: [REDACTED] (DO) (FBI) Sent: Monday, January 9, 2017 2:29 PM To: Richman, Daniel C. (DO) (OGA) Subject: RE: OGE 450 Training

Where do you sit when you into the NY office and who is your POC? Thanks.

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

From: Richman, Daniel C. (DO) (OGA)
Sent: Friday, January 06, 2017 4:43 PM
To: [REDACTED] (DO) (FBI) [REDACTED]
Subject: Re: OGE 450 Training

b6 -1
b7C -1
b7E -3

No Sasha didn't mention it. Darn. It's a particular mess because I need high-side access for the training, and, altho my FBI creds are in fine shape, my GSA card at 26 Federal has expired and it's a pain to get in. But I will see what I can do in the next few weeks.
sorry

From: [REDACTED] (DO) (FBI)
Sent: Friday, January 6, 2017 4:40 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: OGE 450 Training

b6 -1
b7C -1

Yes 2/15/2017. Do you know when you might be able to take the training? I thought that Sasha said you were going to take it when you visited her. That is why I said that. Thanks.

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

From: Richman, Daniel C. (DO) (OGA)
Sent: Friday, January 06, 2017 4:03 PM
To: [REDACTED] (DO) (FBI) [REDACTED]
Subject: Re: OGE 450 Training

b6 -1
b7C -1
b7E -3

I don't believe I've done it for 2016. Our last exchange was in Dec 2015, right?
Thanks for the reminder on the form (due 2/15/17, right) _____

From: [REDACTED] (DO) (FBI) Sent: Friday, January 6, 2017 3:52 PM To: Richman, Daniel C. (DO) (OGA) Subject: OGE 450 Training

Did you take your OGE 450 training when you were here or anytime in 2016?

Also, the actual OGE 450 form is due to me by 2/15/2016. Thanks.



Name:

Date:

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Saturday, January 14, 2017 1:35 PM
To: [REDACTED] (DO) (OGA)
Subject: Re: Director's remarks at Conference of Chief Justices meeting - Jan. 31

b6 -1
b7C -1

[REDACTED]

b5 -1

[REDACTED]
From: [REDACTED] (DO) (OGA)
Sent: Friday, January 13, 2017 4:55 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: FW: Director's remarks at Conference of Chief Justices meeting - Jan. 31

b6 -1
b7C -1

Dan,

D is speaking to an association of state court Chief Justices at the end of the month (see below). [REDACTED]

b5 -1

[REDACTED]
Any thoughts on that would be welcome, as would thoughts on the more general second category below.

Have a great weekend.

[REDACTED]

b6 -1
b7C -1
b7E -3

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

From: [REDACTED] (DO) (FBI)
Sent: Friday, January 13, 2017 3:04 PM
To: [REDACTED] (DO) (OGA) [REDACTED]
Subject: Director's remarks at Conference of Chief Justices meeting - Jan. 31

Hello [REDACTED]

FBI 18-CV-1833-7354

I hope you are well. Not quite the finish for Michigan football that we'd hoped for after such a promising start, I'm afraid... J.T. Barrett was short on that fourth down and that's all I will say about that. :-) On to next year!

[redacted] and I wanted to touch base with you re: the D's upcoming remarks to the Conference of Chief Justices meeting on 1/31 in Scottsdale, AZ. [redacted] told us she spoke briefly to him about this event; he asked for us to provide speech reminders and then he can follow up if he needs additional information. In order to prepare those, we'd like to get your thoughts as well. The event POC has indicated they want to hear about:

b6 -1
b7C -1

1) "Emerging issues in national security and law enforcement" (This is the working title they've given to the lunch session when the Director will speak. Seems like [redacted])

b5 -1

[redacted] 2) "Importance of effective interaction between law enforcement agencies and state courts" [redacted]
[redacted]

I'd be grateful for any thoughts/guidance you can send us sometime next week [redacted] wants the speech reminders for review by the 24th).

b6 -1
b7C -1

Many thanks in advance for your help --

[redacted]

[redacted]

Federal Bureau of Investigation
Office of Public Affairs
Executive Writing Unit

[redacted] office)
[redacted] cell)

b6 -1
b7C -1
b7E -3

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Wednesday, January 18, 2017 12:36 PM
To: [REDACTED] (NY) (FBI)
Subject: checking in

b6 -1
b7C -1

Hey [REDACTED] Just checking in to say hi. The main reason I've not been bothering you recently about cyber strategy and recruitment issues is that [REDACTED], who's working on the Cyber DPI and with whom I had a lovely conversation, tells me that some exec decisions have to be made before we get going. But I'm much looking forward to bother you again
best
dan richman

[redacted] (NY) (FBI)

b6 -1
b7C -1

From: [redacted] (NY) (FBI)
Sent: Wednesday, January 18, 2017 5:11 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: checking in

Hi Dan,

Great to hear from you. Thanks again for your interest -- I'm here to support and provide any feedback you find relevant. Happy to continue the conversation when appropriate.

[redacted]
b6 -1
b7C -1

From: Richman, Daniel C. (DO) (OGA)
Sent: Wednesday, January 18, 2017 12:36 PM
To: [redacted] (NY) (FBI)
Subject: checking in

b6 -1
b7C -1

Hey [redacted] Just checking in to say hi. The main reason I've not been bothering you recently about cyber strategy and recruitment issues is that [redacted] who's working on the Cyber DPI and with whom I had a lovely conversation, tells me that some exec decisions have to be made before we get going. But I'm much looking forward to bother you again
best
dan richman

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Wednesday, January 18, 2017 5:20 PM
To: Cofield, Valerie M. (DO) (FBI); Littlehale, Richard; [REDACTED] (DO) (OGA)
Subject: [REDACTED]
Attachments: [REDACTED]

b5 -1
b6 -1
b7C -1

Lovely chatting. Attached is the outline on [REDACTED] that I gave Amy Hess a while back. Feel free to use (or improve) in any way
thx
dan r

Richard Littlehale

From: Richard Littlehale
Sent: Thursday, January 19, 2017 1:49 PM
To: Richman, Daniel C. (DO) (OGA); Cofield, Valerie M. (DO) (FBI); [REDACTED]
Subject: RE: [REDACTED]

b5 -1
b6 -1
b7C -1

Same here, enjoyed it, thanks to everyone for taking the time! I look forward to keeping the dialogue going. Please let me know if there is anything I can help with on the state and local side, or with the NAS effort.

Richard W. Littlehale
Special Agent in Charge
Technical Services Unit
Criminal Investigation Division
Tennessee Bureau of Investigation



901 R.S. Gass Boulevard
Nashville, TN 37216

Desk [REDACTED]

Fax [REDACTED]

[REDACTED]

b6 -2
b7C -2

From: Richman, Daniel C. (DO) (OGA) [mailto:[REDACTED]]
Sent: Wednesday, January 18, 2017 4:20 PM
To: Cofield, Valerie M. (DO) (FBI) [REDACTED]; Richard Littlehale
[REDACTED] (DO) (OGA) [REDACTED]
Subject: [REDACTED]

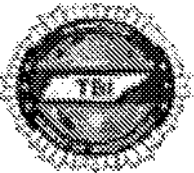
b5 -1
b6 -1,2
b7C -1,2

*** This is an EXTERNAL email. Please exercise caution. DO NOT open attachments or click links from unknown senders or unexpected email - STS-Security. ***

Lovely chatting. Attached is the outline on [REDACTED] that I gave Amy Hess a while back. Feel free to use (or improve) in any way

b5 -1

thx
dan r



Kern, Kenn

From: Kern, Kenn
Sent: Friday, January 20, 2017 3:35 PM
To: Richman, Daniel C. (DO) (OGA); Littlehale, Richard
Subject: RE: using state law to open (older) phones

Dear Dan,

Thank you very much for this writing. Is this scheduled for publication? On track for publication?

Have a nice weekend.

Sincerely,

Kenn

From: Richman, Daniel C. (DO) (OGA) [mailto:]
Sent: Thursday, January 19, 2017 6:57 PM
To: Littlehale, Richard ; Kern, Kenn
Subject: using state law to open (older) phones

b6 -2
b7C -2
b7E -3

Dear Rich and Kenn -- You both might be interested in the attached draft of a student writing on how a state court might handle the issue that came up for the San Bernardino phone in a federal/All Writs Act context. The focus is on NY Law but the analysis goes beyond that. Bottom line is that,

b6 -2
b7C -2

thx
dan richman

This email communication and any files transmitted with it contain privileged and confidential information from the New York County District Attorney's Office and are intended solely for the use of the individuals or entity to whom it has been addressed. If you are not the intended recipient, you are hereby notified that any dissemination or copying of this email is strictly prohibited. If you have received this email in error, please delete it and notify the sender by return email.

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Thursday, January 19, 2017 6:57 PM
To: Littlehale, Richard; [REDACTED]
Subject: using state law to open (older) phones
Attachments: [REDACTED] Submission Draft.docx

b6 -2
b7C -2

Dear Rich and Kenn -- You both might be interested in the attached draft of a student writing on how a state court might handle the issue that came up for the San Bernardino phone in a federal/All Writs Act context. The focus is on NY Law but the analysis goes beyond that. Bottom line is that, [REDACTED]

b6 -2
b7C -2

[REDACTED]

thx
dan richman

Richard Littlehale

From: Richard Littlehale
Sent: Friday, January 20, 2017 3:50 PM
To: Kern, Kenn; Richman, Daniel C. (DO) (OGA)
Subject: RE: using state law to open (older) phones

Where were cool note topics like this when I was in law school? Mine was on international maritime jurisdiction ...well, pirates, actually, so it was kind of cool...

Richard W. Littlehale
Special Agent in Charge
Technical Services Unit
Criminal Investigation Division
Tennessee Bureau of Investigation



901 R.S. Gass Boulevard
Nashville, TN 37216

Desk [REDACTED]

Fax [REDACTED]
[REDACTED]

b6 -2
b7C -2

From: Kern, Kenn [mailto:[REDACTED]]
Sent: Friday, January 20, 2017 2:35 PM
To: 'Richman, Daniel C. (DO) (OGA)' [REDACTED] Richard Littlehale
[REDACTED]
Subject: RE: using state law to open (older) phones

b6 -2
b7C -2
b7E -3

Dear Dan,

Thank you very much for this writing. Is this scheduled for publication? On track for publication?

Have a nice weekend.

Sincerely,

Kenn

From: Richman, Daniel C. (DO) (OGA) [mailto:[REDACTED]]
Sent: Thursday, January 19, 2017 6:57 PM
To: Littlehale, Richard [REDACTED]; Kern, Kenn [REDACTED]
Subject: using state law to open (older) phones

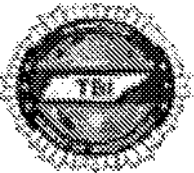
b6 -2
b7C -2
b7E -3

Dear Rich and Kenn -- You both might be interested in the attached draft of a student writing on how a state court might handle the issue that came up for the San Bernardino phone in a federal/All Writs Act context. The focus is on NY Law but the analysis goes beyond that. Bottom line is that, [REDACTED]
[REDACTED]

b6 -2
b7C -2

thx
dan richman

This email communication and any files transmitted with it contain privileged and confidential information from the New York County District Attorney's Office and are intended solely for the use of the individuals or entity to whom it has been addressed. If you are not the intended recipient, you are hereby notified that any dissemination or copying of this email is strictly prohibited. If you have received this email in error, please delete it and notify the sender by return email.



Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Saturday, January 21, 2017 3:02 PM
To: Littlehale, Richard
Subject: Re: using state law to open (older) phones

Pirate are really cool. Stop complaining. And as you can guess, this is what happens when a really strong student comes to a prof with his own quirk ideas :)

From: Richard Littlehale [redacted]
Sent: Friday, January 20, 2017 3:49 PM
To: Kern, Kenn; Richman, Daniel C. (DO) (OGA)
Subject: RE: using state law to open (older) phones

b6 -2
b7C -2

Where were cool note topics like this when I was in law school? Mine was on international maritime jurisdiction ...well, pirates, actually, so it was kind of cool...

Richard W. Littlehale
Special Agent in Charge
Technical Services Unit
Criminal Investigation Division
Tennessee Bureau of Investigation



901 R.S. Gass Boulevard
Nashville, TN 37216

Desk [redacted]
Fax [redacted]
[redacted]

b6 -2
b7C -2

From: Kern, Kenn [mailto:[redacted]]
Sent: Friday, January 20, 2017 2:35 PM
To: 'Richman, Daniel C. (DO) (OGA)' [redacted] Richard Littlehale
[redacted]
Subject: RE: using state law to open (older) phones

b6 -2
b7C -2
b7E -3

Dear Dan,

Thank you very much for this writing. Is this scheduled for publication? On track for publication?

Have a nice weekend.

Sincerely,

Kenn

From: Richman, Daniel C. (DO) (OGA) [mailto:[redacted]]
Sent: Thursday, January 19, 2017 6:57 PM

b7E -3

FBI 18-CV-1833-7375

To: Littlehale, Richard [REDACTED] Kern, Kenn [REDACTED]

Subject: using state law to open (older) phones

b6 -2
b7C -2

Dear Rich and Kenn -- You both might be interested in the attached draft of a student writing on how a state court might handle the issue that came up for the San Bernardino phone in a federal/All Writs Act context. The focus is on NY Law but the analysis goes beyond that. Bottom line is that [REDACTED]

b6 -2
b7C -2

[REDACTED]
thx
dan richman

This email communication and any files transmitted with it contain privileged and confidential information from the New York County District Attorney's Office and are intended solely for the use of the individuals or entity to whom it has been addressed. If you are not the intended recipient, you are hereby notified that any dissemination or copying of this email is strictly prohibited. If you have received this email in error, please delete it and notify the sender by return email.

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Saturday, January 21, 2017 3:03 PM
To: Kern, Kenn
Subject: Re: using state law to open (older) phones

The law rev has to decide to accept it. If not, i'll encourage the student to submit elsewhere. So no pub sched yet.

From: Kern, Kenn [REDACTED]
Sent: Friday, January 20, 2017 3:35 PM
To: Richman, Daniel C. (DO) (OGA); Littlehale, Richard
Subject: RE: using state law to open (older) phones

b6 -2
b7C -2

Dear Dan,

Thank you very much for this writing. Is this scheduled for publication? On track for publication?

Have a nice weekend.

Sincerely,

Kenn

From: Richman, Daniel C. (DO) (OGA) [mailto:[REDACTED]]
Sent: Thursday, January 19, 2017 6:57 PM
To: Littlehale, Richard [REDACTED] Kern, Kenn [REDACTED]
Subject: using state law to open (older) phones

b6 -2
b7C -2
b7E -3

Dear Rich and Kenn -- You both might be interested in the attached draft of a student writing on how a state court might handle the issue that came up for the San Bernardino phone in a federal/All Writs Act context. The focus is on NY Law but the analysis goes beyond that. Bottom line is that, [REDACTED]

b6 -2
b7C -2

[REDACTED]
thx
dan richman

This email communication and any files transmitted with it contain privileged and confidential information from the New York County District Attorney's Office and are intended solely for the use of the individuals or entity to whom it has been addressed. If you are not the intended recipient, you are hereby notified that any dissemination or copying of this email is strictly prohibited. If you have received this email in error, please delete it and notify the sender by return email.

[redacted] (DO) (OGA)

b6 -1
b7C -1

From: [redacted] (DO) (OGA)
Sent: Tuesday, January 24, 2017 9:04 AM
To: Richman, Daniel C. (DO) (OGA)
Subject: FW: Director's remarks at Conference of Chief Justices meeting - Jan. 31

Just so you know, incorporated this in my feedback to the speechwriters.

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

From: Richman, Daniel C. (DO) (OGA)
Sent: Saturday, January 14, 2017 1:35 PM
To: [redacted] (DO) (OGA) [redacted]
Subject: Re: Director's remarks at Conference of Chief Justices meeting - Jan. 31

b6 -1
b7C -1
b7E -3

b5 -1

[redacted] From: [redacted] (DO) (OGA) Sent:
Friday, January 13, 2017 4:55 PM To: Richman, Daniel C. (DO) (OGA) Subject: FW: Director's remarks at
Conference of Chief Justices meeting - Jan. 31

b6 -1
b7C -1

Dan,

D is speaking to an association of state court Chief Justices at the end of the month (see below). [redacted]

b5 -1

[redacted] Any thoughts on that would
be welcome, as would thoughts on the more general second category below.

Have a great weekend.

b6 -1
b7C -1

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

FBI 18-CV-1833-7379

From [redacted] (DO) (FBI)
Sent: Friday, January 13, 2017 3:04 PM
To: [redacted] (DO) (OGA) [redacted]
Subject: Director's remarks at Conference of Chief Justices meeting - Jan. 31

b6 -1
b7C -1
b7E -3

Hello [redacted]

I hope you are well. Not quite the finish for Michigan football that we'd hoped for after such a promising start, I'm afraid... J.T. Barrett was short on that fourth down and that's all I will say about that. :-) On to next year!

[redacted] and I wanted to touch base with you re: the D's upcoming remarks to the Conference of Chief Justices meeting on 1/31 in Scottsdale, AZ. [redacted] told us she spoke briefly to him about this event; he asked for us to provide speech reminders and then he can follow up if he needs additional information. In order to prepare those, we'd like to get your thoughts as well. The event POC has indicated they want to hear about:

b6 -1
b7C -1

1) "Emerging issues in national security and law enforcement" (This is the working title they've given to the lunch session when the Director will speak. Seems like [redacted]
[redacted] 2) "Importance of effective interaction between law enforcement agencies and state courts" [redacted]
[redacted]

b5 -1

I'd be grateful for any thoughts/guidance you can send us sometime next week [redacted] wants the speech reminders for review by the 24th).

b6 -1
b7C -1

Many thanks in advance for your help --

[redacted]

[redacted]
Federal Bureau of Investigation
Office of Public Affairs
Executive Writing Unit
[redacted] office)
[redacted] cell)

b6 -1
b7C -1
b7E -3

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Tuesday, January 24, 2017 12:08 PM
To: [REDACTED] (DO) (OGA)
Subject: Re: Director's remarks at Conference of Chief Justices meeting - Jan. 31

b6 -1
b7C -1

lovely
thx

From: [REDACTED] (DO) (OGA)
Sent: Tuesday, January 24, 2017 9:04 AM
To: Richman, Daniel C. (DO) (OGA)
Subject: FW: Director's remarks at Conference of Chief Justices meeting - Jan. 31

b6 -1
b7C -1

Just so you know, incorporated this in my feedback to the speechwriters.

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

From: Richman, Daniel C. (DO) (OGA)
Sent: Saturday, January 14, 2017 1:35 PM
To: [REDACTED] (DO) (OGA) [REDACTED]
Subject: Re: Director's remarks at Conference of Chief Justices meeting - Jan. 31

b6 -1
b7C -1
b7E -3

b5 -1

[REDACTED] **From:** [REDACTED] (DO) (OGA) **Sent:**
Friday, January 13, 2017 4:55 PM **To:** Richman, Daniel C. (DO) (OGA) **Subject:** FW: Director's remarks at
Conference of Chief Justices meeting - Jan. 31

b6 -1
b7C -1

Dan,

D is speaking to an association of state court Chief Justices at the end of the month (see below). [REDACTED]
[REDACTED]

b5 -1

[redacted] Any thoughts on that would be welcome, as would thoughts on the more general second category below.

b5 -1

Have a great weekend.

[redacted]

b6 -1
b7C -1

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

From: [redacted] (DO) (FBI)

Sent: Friday, January 13, 2017 3:04 PM

To: [redacted] (DO) (OGA) [redacted]

Subject: Director's remarks at Conference of Chief Justices meeting - Jan. 31

b6 -1
b7C -1
b7E -3

Hello [redacted]

I hope you are well. Not quite the finish for Michigan football that we'd hoped for after such a promising start, I'm afraid... J.T. Barrett was short on that fourth down and that's all I will say about that. :-) On to next year!

[redacted] and I wanted to touch base with you re: the D's upcoming remarks to the Conference of Chief Justices meeting on 1/31 in Scottsdale, AZ. [redacted] told us she spoke briefly to him about this event; he asked for us to provide speech reminders and then he can follow up if he needs additional information. In order to prepare those, we'd like to get your thoughts as well. The event POC has indicated they want to hear about:

b6 -1
b7C -1

1) "Emerging issues in national security and law enforcement" (This is the working title they've given to the lunch session when the Director will speak. Seems like [redacted]
[redacted] 2) "Importance of effective interaction between law enforcement agencies and state courts" [redacted]
[redacted]

b5 -1

I'd be grateful for any thoughts/guidance you can send us sometime next week. [redacted] wants the speech reminders for review by the 24th).

b6 -1
b7C -1

Many thanks in advance for your help --

[redacted]

[redacted]
Federal Bureau of Investigation
Office of Public Affairs
Executive Writing Unit
[redacted] (office)
[redacted] (cell)

b6 -1
b7C -1
b7E -3

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Tuesday, January 24, 2017 2:41 PM
To: [REDACTED] (DO) (OGA)
Subject: Re: 14-2985 United States of America v. In the matter of a Warrant to "Petition Order FILED"

b6 -1
b7C -1

thanks for the heads up. Time for the S Ct to actually do something

From: [REDACTED] (DO) (OGA)
Sent: Tuesday, January 24, 2017 12:39 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: FW: 14-2985 United States of America v. In the matter of a Warrant to "Petition Order FILED"

b6 -1
b7C -1

2nd Cir. Denies petition for rehearing en banc (by a divided vote).

[redacted] (OGC) (FBI)

b6 -1
b7C -1

From: [redacted] (OGC) (FBI)
Sent: Tuesday, January 24, 2017 3:52 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: OGE-450

Good afternoon Mr. Richman,

I apologize for bothering you about this, but SESU is asking if you filed your financial disclosure form (OGE-450) for FY16. They need to notify OIC. If you could confirm the status of your OGE-450, I would greatly appreciate it.

Thank you very much,

[redacted]
Management and Program Analyst
Office of the General Counsel
Federal Bureau of Investigation
Office: [redacted]
Cell: [redacted]

b6 -1
b7C -1
b7E -3

Confidentiality Statement:

This message is transmitted to you by the Office of the General Counsel of the Federal Bureau of Investigation. The message, along with any attachments, may be confidential and legally privileged. If you are not the intended recipient of this message, please destroy it promptly without further retention or dissemination (unless otherwise required by law). Please notify the sender of the error by a separate e-mail or by calling [redacted]

b7E -3

[REDACTED] (DO) (OGA)

b6 -1
b7C -1

From: [REDACTED] (DO) (OGA)
Sent: Tuesday, January 24, 2017 12:40 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: FW: 14-2985 United States of America v. In the matter of a Warrant to "Petition Order FILED"
Attachments: order denying rehearing.pdf; Droney.pdf; Raggi.pdf; Jacobs.pdf; Carney.pdf; Cabranes.pdf

2nd Cir. Denies petition for rehearing en banc (by a divided vote).

JOSÉ A. CABRANES, *Circuit Judge*, joined by DENNIS JACOBS, REENA RAGGI, and CHRISTOPHER F. DRONEY, *Circuit Judges*, dissenting from the order denying rehearing *en banc*:

An evenly-divided *en banc* court has declined to rehear a case that presents multiple questions of exceptional importance to public safety and national security.¹ I respectfully dissent.

The panel majority quashed a warrant issued under section 2703 of the Stored Communications Act (“SCA”)² by a judicial officer of the United States upon a showing of probable cause. It erroneously concluded that the government’s use of an SCA warrant to require a United States-based service “provider” (Microsoft) to disclose the contents of a customer’s emails stored on servers located in Ireland was an extraterritorial application of the SCA.³ The

¹ We have had occasion to observe that the decision to deny rehearing *en banc* “does not necessarily mean that a case either lacks significance or was correctly decided. Indeed, the contrary may be true. An oft-cited justification for voting *against* rehearing, perhaps counterintuitively, is that the case is ‘too important to *en banc*.’” *United States v. Taylor*, 752 F.3d 254, 256 (2d Cir. 2014) (quoting James L. Oakes, *Personal Reflections on Learned Hand and the Second Circuit*, 47 STAN. L. REV. 387, 392 (1995)) (emphasis in original). Accordingly, a reader should not give “any extra weight to a panel opinion in light of such a decision, inasmuch as the order denying rehearing may only reflect, for some judges, a general aversion to *en banc* rehearsings or faith in the Supreme Court to remedy any major legal errors.” *Id.* at 257.

² See 18 U.S.C. §§ 2701–12.

³ See Majority Op. at 42.

panel majority ignored the fact that Microsoft lawfully had possession of the emails; that Microsoft had access to the emails in the United States; and that Microsoft's disclosure of the emails to the government would take place in the United States. In its unprecedented ruling, the panel majority has indisputably, and severely, restricted "an essential investigative tool used thousands of times a year [in] important criminal investigations around the country."⁴ To top this off, the panel majority's decision does not serve any serious, legitimate, or substantial privacy interest.⁵

I.

The negative consequences of the panel majority's opinion are far reaching. It has substantially burdened the government's legitimate law enforcement efforts; created a roadmap for the facilitation of criminal activity;

⁴ Petition for Rehearing and Rehearing En Banc ("En Banc Petition") 2–3. In just the second half of 2015, Google alone "received 3,716 warrants seeking data from a total of 9,412 accounts." *Id.* at 18.

⁵ In his concurring opinion, Judge Lynch observes that despite Microsoft's suggestion that "this case involves a government threat to individual privacy . . . uphold[ing] the warrant here would not undermine basic values of privacy as defined in the Fourth Amendment and in the libertarian traditions of this country." Concurring Op. at 1. As he explains, "the government complied with the most restrictive privacy-protecting requirements of the [SCA]. Those requirements are consistent with the highest levels of protection ordinarily required by the Fourth Amendment for the issuance of search warrants." *Id.* at 2.

and impeded programs to protect the national security of the United States and its allies.⁶

First, as Judge Lynch's concurring opinion explains, the panel majority's holding affords "absolute" protection from disclosure to electronic communications stored abroad, regardless of whether they are controlled by a domestic service provider and are accessible from within the United States.⁷ As a result, the government can "never obtain a warrant" that would require a service provider to turn over emails stored in servers located outside the United States, regardless of how "certain [the government] may be that [emails] contain

⁶ Judge Carney's opinion concurring in the order denying rehearing *en banc* does not dispute the fact that the panel majority's decision has put the safety and security of Americans at risk. Instead, in a footnote, the concurring opinion notes two sections of the SCA that it believes lessen the severity of these consequences. *Ante* at 1 n.2 (Carney, J., concurring in the order denying reh'g *en banc*). The first section, 2702(b)(8), permits "[a] provider . . . [to] divulge the contents of a communication . . . to a government entity, *if the provider, in good faith, believes that*" there are exigent circumstances. *Id.* (quoting 18 U.S.C. § 2702(b)(8)) (emphasis added). The second section, 2703(e), "gives a provider immunity from civil liability for a voluntary production of content made 'in accordance with . . . [a] statutory authorization . . .'" *Id.* at 2 n.2 (quoting 18 U.S.C. § 2703(e)). In asking us to entrust our national security to the good faith of internet service providers, I can only assume that the concurring opinion has some unstated reason for believing that Microsoft is just an atypically unpatriotic service provider and that other, more virtuous, service providers would never put their business interests ahead of public safety and national security.

⁷ Concurring Op. at 4.

evidence of criminal activity, and even if that criminal activity is a terrorist plot.”⁸

Second, the panel majority’s opinion has created a roadmap for even an unsophisticated person to use email to facilitate criminal activity while avoiding detection by law enforcement. The Microsoft customer targeted by the government’s warrant in this case indicated to Microsoft when he signed up for its service that he resided in Ireland—a representation Microsoft took at face value.⁹ Because Microsoft has a policy of “stor[ing] a customer’s email information . . . at datacenters located near the physical location identified by the user as its own,” Microsoft automatically stored his emails on its servers in Ireland—now safely beyond the reach of an SCA warrant.¹⁰ Based on the panel majority’s holding, a criminal who resides in the United States can now check the proverbial “box” informing Microsoft that he resides in another country when signing up for service—perhaps a country without a Mutual Legal Assistance

⁸ *Id.* at 4–5.

⁹ Majority Op. at 8–9.

¹⁰ *Id.*

Treaty (“MLAT”) with the United States¹¹—and thereby avoid having his emails disclosed to the government pursuant to an SCA warrant.

Third, the panel majority’s decision has already led major service providers to reduce significantly their cooperation with law enforcement. The panel majority held that the physical location of a server containing a customer’s emails determines whether an SCA warrant seeking the disclosure of those emails is an extraterritorial application of the SCA. However, electronic data storage is more complex and haphazard than the panel majority’s holding assumes. Many service providers regularly “store different pieces of information for a single customer account in various datacenters at the same time, and routinely move data around based on their own internal business practices.”¹² Still other providers are unable to determine “where particular data is stored or whether it is stored outside the United States.”¹³ Consequently, in an effort to

¹¹ The United States has entered into MLATs with several countries, allowing parties to the treaty to request assistance with ongoing criminal investigations, including issuance and execution of search warrants. *See id.* at 41. However, many countries do not have MLATs with the United States, *e.g.*, Indonesia and Pakistan, and law enforcement cooperation with those countries is limited. *See* Gov’t Br. 48–53 (describing the inefficiencies of the MLAT process as well as its ineffectiveness in certain circumstances).

¹² *En Banc* Petition 18–19.

¹³ *Id.*

apply the panel majority's confected holding to the technological realities of electronic data storage, major service providers are adopting restrictive disclosure policies that radically undermine the effectiveness of an SCA warrant.¹⁴

For example, Google will now disclose "only those portions of customer accounts stored in the United States at the moment the warrant is served."¹⁵ Google's policy is particularly troubling because "the only [Google] employees who can access the entirety of a customer's account, including those portions momentarily stored overseas, are located in the United States."¹⁶ As a result, law enforcement might never be able obtain data stored in Google servers abroad, even with the help of an MLAT.

Yahoo! has advised law enforcement that it "will not even preserve data located outside the United States in response to a [s]ection 2703 request."¹⁷ This policy, as the government points out in its En Banc Petition, creates "a risk that

¹⁴ See *Id.* 17–19; see also Orin Kerr, *The Surprising Implications of the Microsoft/Ireland Warrant Case*, WASH. POST: THE VOLOKH CONSPIRACY (Nov. 29, 2016), <https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/11/29/the-surprising-implications-of-the-microsoftireland-warrant-case>.

¹⁵ En Banc Petition 19.

¹⁶ *Id.*

¹⁷ *Id.*

data will be moved or deleted before the United States can seek assistance from a foreign jurisdiction, much less actually serve a warrant and secure the data.”¹⁸

II.

The baleful consequences of the panel’s decision are compelled neither by the text of the statute nor by our precedent. The panel majority arrived at its damaging holding because it adopted a flawed reading of the SCA.

The second step of the two-step framework for analyzing extraterritoriality issues set forth in *Morrison v. National Australia Bank Ltd.*, 561 U.S. 247 (2010), and *RJR Nabisco, Inc. v. European Community*, 136 S. Ct. 2090 (2016), was the determinative issue in this case.¹⁹ At step two, a court must “determine whether

¹⁸ *Id.*

¹⁹ The first step of the extraterritorial analysis is “to determine whether the relevant statutory provision contemplates extraterritorial application.” Majority Op. at 22 (citing *Morrison*, 561 U.S. at 262–65). Because the government conceded at oral argument that the SCA lacks extraterritorial application, *id.*, there is no need to pursue the point. To the extent the panel majority did so in a lengthy discussion of the SCA’s use of the word “warrant” in section 2703, *see id.* at 25–31, which then informs its step-two “focus” analysis, it is appropriate to note concern with the reasoning.

The panel majority conflates SCA disclosure warrants with traditional search warrants. While the latter authorize government action as to *places*, the former authorize government action on *persons*. The fact that warrants generally do not authorize government searches of places outside the United States—a limitation grounded in respect for sovereignty, not privacy, *see, e.g., The Apollon*, 22 U.S. (9 Wheat.) 362, 371 (1824) (Story, J.); Restatement (Third) of Foreign Relations Law § 432(2); *see also In re Terrorist Bombings of U.S. Embassies in E. Africa*, 552 F.3d 157, 167–72 (2d Cir. 2008)—does not support a conclusion that warrants are impermissibly applied extraterritorially

the case involves a domestic application of the statute,” which “we do . . . by looking to the statute’s ‘focus’” and by identifying where “the conduct relevant to the statute’s focus occurred.”²⁰ Here, the panel majority explained that the “focus” of the SCA is user privacy,²¹ and in a single sentence, identified the location of the conduct relevant to that focus: “[I]t is our view that the invasion of the customer’s privacy takes place under the SCA where the customer’s protected content is accessed—here, where it is seized by Microsoft, acting as an

when they compel persons within the United States to disclose property lawfully in their possession anywhere in the world. *Cf. Linde v. Arab Bank, PLC*, 706 F.3d 92, 109 (2d Cir. 2013) (Carney, J.) (observing that the Supreme Court has held that “the operation of foreign law ‘do[es] not deprive an American court of the power to order a party subject to its jurisdiction to produce evidence even though the act of production may violate that [law].” (quoting *Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Court*, 482 U.S. 522, 544 n. 29 (1987)). In that sense, a disclosure warrant is more akin to a subpoena, *see, e.g., Marc Rich & Co. A.G. v. United States*, 707 F.2d 663, 668–70 (2d Cir. 1983) (holding that persons in the United States can be required to retrieve subpoenaed material from abroad), *but* with the important added protection of a probable cause showing to a neutral magistrate. Thus, the panel majority is simply wrong in concluding that “a warrant protects *privacy* in a distinctly territorial way.” Majority Op. at 26 (emphasis added). Warrants protect privacy through the Fourth Amendment requirement that they issue only upon probable cause. *See* Concurring Op. at 1–3.

By failing to distinguish between search warrants as to places and disclosure warrants directed to persons, and between sovereignty and privacy, the panel majority construes “warrant” as used in the SCA to yield the perverse result of affording greater privacy protection to foreign nationals and Americans who say they reside abroad than to resident United States citizens with respect to electronic communications in the lawful possession of a United States service provider.

²⁰ *RJR Nabisco*, 136 S. Ct. at 2101.

²¹ *See* Majority Op. at 32–39.

agent of the government.”²² Because the emails at issue were stored on a server in Ireland, the panel majority concluded that the warrant seeking the disclosure of those emails was an extraterritorial application of the SCA.²³ Not so.

Even if the “focus” of the SCA is user privacy, a plain reading of the statute makes clear that the conduct relevant to the SCA’s “focus,” and which the SCA seeks to regulate, is a provider’s *disclosure* or *non-disclosure* of emails to third parties, not a provider’s *access* to a customer’s data. Here, Microsoft’s disclosure

²² *Id.* at 39. Judge Carney’s opinion concurring in the order denying rehearing *en banc* reiterates the panel majority’s conclusion—that, “the locus of the SCA’s privacy protections [is] at the place of data storage”—but again provides little or no explanation for how or why the statutory language permits such a reading. *Ante* at 4 (Carney, J., concurring in the order denying reh’g *en banc*). It offers only the sphinx-like explanation that “§ 2701, by proscribing unauthorized access to storage facilities, not only limits disclosure but also ‘shelters the communications’ integrity.” *Id.* at 5 (quoting Majority Op. at 35). Conversely, and as the concurring opinion itself notes, those of us dissenting from the denial of *en banc* review “offer[] a detailed recitation of the available statutory support for [the] conclusion” that the conduct relevant to the SCA’s focus occurs at the place of disclosure. *Id.* at 6.

²³ Judge Carney’s *en banc* concurrence asserts that the panel majority’s “reading of the SCA did no more than adhere to the dictates of *Morrison* in construing the SCA.” *Ante* at 3 (Carney, J., concurring in the order denying reh’g *en banc*). I disagree. Instead of locating support for its legal conclusion in the text or structure of the SCA, the concurring opinion, like the panel majority’s opinion, fixates on its unsubstantiated belief that the warrant at issue here raises “concerns of sovereignty and international comity.” *Id.* at 4. They both then conclude, based primarily on that misconception, that the warrant at issue must be an extraterritorial application of the SCA. *Morrison*, however, does not permit a court to conclude that a particular application of a statute is extraterritorial simply because it believes that the application threatens international comity. Rather, step two of the *Morrison* framework directs courts to examine the statutory language. *See Morrison*, 561 U.S. at 266–67.

of emails to the government would take place at its headquarters in the United States. Therefore, had the panel majority correctly identified the conduct relevant to the SCA's "privacy focus," it would have concluded that the warrant at issue was a domestic application of the SCA.²⁴

A brief examination of the text and structure of the SCA leads inexorably to the conclusion that the conduct relevant to the SCA's "privacy focus" is its regulation of *disclosures* by providers to third-parties. As the panel majority

²⁴ According to the *en banc* concurrence, the panel majority considered and rejected my suggested holding partly because that holding "ignores situations in which the effects outside the United States are less readily dismissed." *Ante* at 8 (Carney, J., concurring in the order denying reh'g *en banc*). As far as I understand it, the concurring opinion asserts the belief that the facts of this case are too sympathetic to my interpretation of the law and that only under alternative, entirely fictional, circumstances would the true menace of my position be revealed. It then devises a hypothetical warrant that purports to show how my suggested holding permits the authorization of warrants with too limited a nexus to the United States: an SCA warrant requiring a "United States . . . branch office of an Irish service provider" to disclose electronic information stored in Ireland but accessible in the United States that belonged to an account "opened and established in Ireland by an Irish citizen," the disclosure of which would breach Irish law. *Id.*

This hypothetical is too clever by half. In attempting to construct the most shocking warrant conceivable, the concurring opinion omits two critical facts, both of which are required under my understanding of the law. First, a judicial officer of the United States would have to issue the warrant upon a finding of probable cause to believe that the information being sought was related to criminal activity occurring within the United States. Second, the provider would have to disclose the targeted information to the government inside the United States. Thus, if all of the conditions necessary for a valid SCA warrant are satisfied, there is no basis for concluding that even Judge Carney's imagined warrant, not to mention the warrant at issue, is an extraterritorial application of the SCA.

observes, “the first three sections of the SCA contain its major provisions.”²⁵ The first of those sections, section 2701, addresses “[u]nlawful access to stored communications.”²⁶ Section 2701 is the *only* major provision of the SCA to specifically limit *access* to customer communications. Although the panel majority fails to explain adequately why the “invasion of the customer’s privacy takes place . . . where the customer’s protected content is *accessed*,”²⁷ section 2701 is the only plausible textual basis for the panel majority’s bizarre holding.

However, while section 2701 prohibits “[u]nlawful access” (most obviously hacking), it recognizes that providers have standing authority to *access* a customer’s electronic communications.²⁸ In fact, section 2701(c) expressly exempts from its restrictions on *access* “conduct authorized . . . by the person or entity providing a wire or electronic communications service,” *i.e.*, the provider.²⁹ It is unreasonable, therefore, for the panel majority to conclude that a provider’s

²⁵ *Id.* at 35; see 18 U.S.C. §§ 2701–03

²⁶ 18 U.S.C. § 2701.

²⁷ Majority Op. at 39 (emphasis added).

²⁸ 18 U.S.C. § 2701

²⁹ *Id.* § 2701(c)(1) (emphasis added).

lawful access to a customer's emails is the conduct relevant to the SCA's "privacy focus."³⁰

On the other hand, section 2702 expressly prohibits, with some exceptions, a provider from "*disclos[ing]*" a customer's communications.³¹ For example, section 2702(a) sets forth three "[p]rohibitions" that must be followed by service providers like Microsoft.³² Each prohibition states that the provider "shall not knowingly *divulge*" certain information, such as the contents of a communication, unless an exception in subsection (b) or (c) applies.³³ In turn, section 2703 specifically empowers the government to "require the *disclosure* by a provider . . . of the contents of a[n] . . . electronic communication . . . pursuant to a warrant."³⁴

Considering sections 2701, 2702, and 2703 together, it is clear that the SCA protects user privacy by prohibiting unlawful access of customer communications (such as hacking), and by regulating a provider's *disclosure* of

³⁰ The panel majority characterizes a service provider that "access[es]" a user's email pursuant to an SCA warrant as "an agent of the government." Majority Op. at 29, 39. But, the legal authorities cited by the panel for the proposition that a private party who assists the government in conducting a search and seizure "becomes an agent of the government," *id.* at 29, do not involve circumstances, such as those here, where the private party already had possession of the relevant property.

³¹ *Id.* §§ 2702–03 (emphasis added).

³² *See id.* § 2702(a)(1)–(3).

³³ *Id.* (emphasis added).

³⁴ *Id.* § 2703(a) (emphasis added).

customer communications to third parties. Inasmuch as section 2701's limitations on *access* specifically do not apply to providers, it is only when a provider *divulges* the content of a user's communication to a third party that the provider puts a user's privacy at risk. It is not a mere coincidence that the SCA recognizes a provider's standing authority to *access* a user's communications and, at the same time, prohibits a provider from *disclosing* those communications to third-parties except as authorized by sections 2702 and 2703. Accordingly, the panel majority's focus on *access* (instead of on *disclosure*) is entirely misplaced.³⁵

Put another way, Microsoft did not need a warrant to take possession of the emails stored in Ireland. Nor did it need a warrant to move the emails from Ireland to the United States. It already had possession of, and lawful *access* to, the targeted emails from its office in Redmond, Washington. Only Microsoft's

³⁵ Neither the panel majority's opinion nor the *en banc* concurrence explains why "privacy" is better served by looking to a provider's *access* rather than its *disclosure*. They just assume the point. *See ante* at 13 (Carney, J., concurring in the order denying reh'g *en banc*) ("The better approach . . . is one that looks to the step taken before disclosure—access—in determining privacy's territorial locus."); Majority Op. at 39. Both the panel majority's opinion and the *en banc* concurrence also fail to explain why the physical location of the datacenter is the legal point of *access*, rather than the location from where the service provider electronically gains *access* to the targeted data, which, in this case, is the United States. Evidently, it is so (again) because the panel majority and the concurrence say it is so. *See ante* at 4 (Carney, J., concurring in the order denying reh'g *en banc*) ("[T]he locus of the SCA's privacy protections [is] at the place of data storage."); Majority Op. at 39. Naked assertions, however, do not the law make.

disclosure of the emails to the government would have been unlawful under the SCA absent a warrant.³⁶

In sum, the government obtained a warrant based on a showing of probable cause before a judicial officer of the United States. That warrant required Microsoft's office in Redmond, Washington, to disclose certain emails that happened to be electronically stored in its servers abroad, but to which Microsoft had immediate access in the United States. Because the location of a provider's *disclosure* determines whether the SCA is applied domestically or extraterritorially, the enforcement of the warrant here involved a domestic application of the SCA. The panel should have affirmed the District Court's denial of Microsoft's motion to quash.

For the foregoing reasons, I dissent from the order denying rehearing *en banc*. I trust that the panel's misreading of this important statute can be rectified

³⁶ To the extent the panel majority concludes that the SCA does not apply extraterritorially to compel a provider's disclosures pursuant to section 2703, its place-of-access reasoning raises concerns about the extraterritorial reach of protections from unlawful access and disclosures afforded by sections 2701 and 2702. Such a concern might be avoided if the statute is construed to reach, at least, the conduct of persons within the jurisdiction of the United States. This further concern only reinforces the need for *en banc* review.

as soon as possible by a higher judicial authority or by the Congress of the United States.³⁷

³⁷ Ultimately, Judge Carney's concurring opinion suggests that rehearing *en banc* is unnecessary because the panel majority's holding was compelled by an anachronistic statute and an inflexible framework for analyzing questions of extraterritoriality. *Ante* at 13–14 (Carney, *J.*, concurring in the order denying reh'g *en banc*). It also notes that some Members of Congress have introduced a bill purporting to resolve all of our concerns with the statute. *Id.* at 2 n.3. I submit that rehearing *en banc* is necessary precisely because the panel majority misread the SCA and misapplied the extraterritoriality framework set forth in *Morrison*. Where a decision of our court has unnecessarily created serious, on-going problems for those charged with enforcing the law and ensuring our national security, and where a legislative remedy is entirely speculative, we should not shirk our duty to interpret an extant statute in accordance with its terms.

SUSAN L. CARNEY, *Circuit Judge*, concurring in the order denying rehearing *en banc*:

The original panel majority opinion, *see Microsoft Corp. v. United States*, 829 F.3d 197 (2d Cir. 2016), fully explains why quashing the government's warrant is called for by Supreme Court precedent on extraterritoriality and the text of the Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701 *et seq.* Because the panel opinions did not include a dissent, however, I write again, briefly, to respond with respect to several points raised during our Court's consideration of whether to grant the government's petition for *en banc* review and reflected in the dissents from denial of rehearing.¹

The theme running through the government's petition and the dissents is the concern that, by virtue of the result the panel reached, U.S. law enforcement will less easily be able to access electronic data that a magistrate judge in the United States has determined is probably connected to criminal activity.² My

¹ Judges Lynch and Bolden, who comprised the rest of the panel that heard this appeal, are not eligible to participate in deciding whether to rehear this case *en banc* because they are, respectively, a judge who entered senior status not long before the *en banc* poll was requested and a district judge sitting by designation. *See* 28 U.S.C. § 46(c) (limiting *en banc* voting to "the circuit judges of the circuit who are in regular active service").

² In this regard, it bears noting that an SCA section not at issue in this case, 18 U.S.C. § 2702(b)(8), authorizes "[a] provider . . . [to] divulge the contents of a communication . . . to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person

panel colleagues and I readily acknowledge the gravity of this concern. But the SCA governs this case, and so we have applied it, looking to the statute's text and following the extraterritoriality analysis of *Morrison v. National Australia Bank Ltd.*, 561 U.S. 247 (2010). We recognize at the same time that in many ways the SCA has been left behind by technology. It is overdue for a congressional revision that would continue to protect privacy but would more effectively balance concerns of international comity with law enforcement needs and service provider obligations in the global context in which this case arose.³

Before going further, it is worth pointing out what is *not* at issue in this appeal. First, it is common ground that Congress did not intend for the SCA's warrant procedures to apply extraterritorially. *See* Gov't Pet. for Reh'g 11. Second, although the panel majority determined that the SCA's focus lies on protecting user privacy, this determination was made under the second part of

requires disclosure without delay of communications relating to the emergency," bypassing the warrant procedures of § 2703. Another section gives a provider immunity from civil liability for a voluntary production of content made "in accordance with . . . [a] statutory authorization . . . under this chapter." 18 U.S.C. § 2703(c). The panel expressed no opinion on the use of these subsections, nor has it been suggested that the exigent circumstances of a "danger of death or serious physical injury" are presented here.

³ This is a fact well appreciated by the Members of Congress who have introduced a bill proposing related amendments. *See* International Communications Privacy Act, S. 2986, H.R. 5323, 114th Cong. (2016).

the extraterritoriality analysis set forth as a canon of construction in *Morrison* and recently developed further in *RJR Nabisco, Inc. v. European Community*, 136 S. Ct. 2090 (2016). *See RJR Nabisco*, 136 S. Ct. at 2101 (“If the statute is not extraterritorial, then at the second step we determine whether the case involves a domestic application of the statute, and we do this by looking to the statute’s ‘focus.’”). Our “focus” analysis did not turn on privacy protections independently derived from the Fourth Amendment. Nor did we express or imply a view about how Congress *may* permissibly legislate to enable the government to reach data stored abroad and under the control of U.S. companies; our reading of the SCA did no more than adhere to the dictates of *Morrison* in construing the SCA. Finally, since the instrument was issued by a neutral magistrate judge upon a showing of probable cause, no one disputes that the Microsoft warrant has satisfied the most stringent privacy protections our legal system affords.

Accordingly, the dispositive question in the case, as we see it, might be framed as whether Microsoft’s execution of the warrant to retrieve a private customer’s electronic data, stored on its servers in Ireland, would constitute an extraterritorial application of the SCA in light of the statute’s “focus,”

determined in accordance with *Morrison* and *RJR Nabisco*. Again, this is a question of statutory construction. And, unsurprising in light of the need for an extraterritoriality analysis, it requires consideration of the concerns of sovereignty and international comity.

The panel majority concluded that “the relevant provisions of the SCA focus on protecting the privacy of the content of a user’s stored electronic communications.” *Microsoft*, 829 F.3d at 217. The concurring opinion noted the difficulty in determining a statute’s “focus” under *Morrison*, but agreed that in the absence of any evidence that Congress intended the SCA to reach electronic data stored abroad by a service provider (and relating potentially to a foreign citizen), the effect of the government’s demand here impermissibly fell beyond U.S. borders and therefore the Microsoft warrant should be quashed. *Id.* at 230-31 (Lynch, J., concurring).

Guided by our determination of the statute’s focus and looking at the text of the SCA itself, the panel majority read the statute to treat the locus of the SCA’s privacy protections as at the place of data storage. As further detailed in the majority opinion, this conclusion comports with the SCA’s reliance on the fact and form of content storage as predicates to its various provisions, as well as

its use of the term of art “warrant” and its requirement of compliance with Federal Rule of Criminal Procedure 41, “Search and Seizure” — features usually associated with physical access. *See, e.g.*, 18 U.S.C. § 2701(a) (prohibiting access to “facilit[ies]” where electronic communications are stored); *id.* § 2702(a)(1)-(2) (prohibiting disclosure of communications “while in electronic storage” or “which [are] carried or maintained” by an electronic communication service); *id.* § 2703(a) (imposing warrant procedures on electronic communications that are “in electronic storage in an electronic communications system for one hundred and eighty days or less”). We noted that the statute uses “[t]he circumstances in which the communications have been stored . . . as a proxy for the intensity of the user’s privacy interests, dictating the stringency of the procedural protection they receive.” *Microsoft*, 829 F.3d at 217. We also noted that § 2701, by proscribing unauthorized access to storage facilities, not only limits disclosure but also “shelters the communications’ integrity.” *Id.* at 218. Because the electronic communications to be accessed and disclosed pursuant to the Microsoft warrant are stored in a Dublin datacenter, we reasoned, the execution of the warrant would have its effect when the service provider accessed the data in Ireland, an extraterritorial application of the SCA.⁴

⁴ This approach, in which we considered several numbered sections of the SCA, is not

Characterizing the statute's focus differently, as resting on "disclosure," and offering a detailed recitation of the available statutory support for that conclusion,⁵ the dissents argue primarily that the SCA's effect occurs at the place

inconsistent with *RJR Nabisco*. Rather than requiring a provision-by-provision analysis in every instance, as the government and some of the dissents suggest in the context of their "focus" analysis, *see post* at 2 (Droney, J., dissenting from the denial of reh'g *en banc*), *RJR Nabisco* involved looking at the expressed congressional intent with regard to the separately-enacted RICO predicate statutes, one by one, in the context of an overarching structure—that is, RICO. The panel majority here saw the SCA's relevant provisions, essentially enacted of a piece, as reflecting a single congressional expression with respect to extraterritorial application—a statutory circumstance quite different from the one addressed in *RJR Nabisco*.

⁵ In support of their position my dissenting colleagues contend, as does the government, that an SCA warrant functions more like a subpoena than a traditional warrant and should be treated accordingly as reaching all documents under the control of the instrument's recipient. *See post* at 7 n.19 (Cabrane, J., dissenting from the denial of reh'g *en banc*); *id.* at 1 (Jacobs, J., dissenting from the denial of reh'g *en banc*). The SCA does not address a potential extraterritorial application of the instrument issued under § 2703—indeed it is unlikely, in view of the historical context, that Congress could have anticipated such an application, much less weighed domestic law enforcement interests against countervailing concerns with international comity. In light of the importance of these interests, it seems a stretch to conclude that we should read Congress's deliberate choice of the term "warrant" to reflect a concurrent intention to incorporate into the statute, without explicit mention, a body of case law addressing not warrants, but grand jury subpoenas. *Cf. id.* at 7 n.19 (Cabrane, J., dissenting from the denial of reh'g *en banc*) (citing *Marc Rich & Co. v. United States*, 707 F.2d 663 (2d Cir. 1983)). Even the territorial reach of subpoenas is not an easy determination, in light of the many interests that courts must balance when addressing discovery that has foreign aspects. *See, e.g.*, Restatement (Third) of the Foreign Relations Law of the United States § 442(1)(c) (listing several factors courts "should take into account" when deciding whether to order production of information located abroad). Some of my dissenting colleagues also emphasize that the customer data at issue here is already in Microsoft's possession. *See post* at 9-11 (Raggi, J., dissenting from the denial of reh'g *en banc*). The SCA constrains a service provider's use of that "possession," recognizing the provider's role as an

of disclosure, on U.S. soil.⁶ Thus, so long as (1) the warrant is served in the United States on a provider doing business in the United States, and (2) the provider can access the user's content electronically from the United States, extraterritoriality need not even be considered.⁷ Since the warrant recipient here

intermediary between the customer who created the content and third parties. Thus, it distinguishes in its level of privacy protections between customers' substantive content and the administrative data that a provider maintains for its own purposes with respect to those customers. *See* 18 U.S.C. § 2703(c) (distinguishing between "contents of communications" and information such as a customer's name, address, and service details).

⁶ As explored further below, although the SCA is broadly focused on privacy, it does address disclosure, most particularly in § 2702, as an exception to its general rule of maintaining the confidentiality of customer content. *See post* at 10-13 (Cabrane, J., dissenting from the denial of reh'g *en banc*). The panel majority read the SCA to focus foremost on protecting user privacy by controlling access to stored communications—controls that apply even to service providers (if, for example, an employee exceeded his or her authorization with respect to stored data). To the extent that the majority opinion "raises concerns about the extraterritorial reach of *protections* from unlawful access and disclosures afforded by sections 2701 and 2702," *id.* at 14 n.36 (Cabrane, J., dissenting from the denial of reh'g *en banc*) (emphasis added), one might take some comfort from the privacy laws of other countries that would apply to servers on their territory (and the significant incentives for service providers to guard against unauthorized intrusion). More importantly, however, the dissents' concerns about the reach outside the United States of the protections established by the statute provide yet another reason for congressional overhaul of the SCA.

⁷ Taken to its logical conclusion, the dissents' focus on the place of disclosure to the exclusion of other factors would mean that, so long as the requested data is to be disclosed to the government within the United States, the SCA has only domestic application. But because, presumably, data demanded by the United States government under the SCA can *always* be expected to be disclosed to the government in the United States absent special circumstances, no application of the SCA's data disclosure procedures would be extraterritorial. At a time when U.S. companies, to their great

is Microsoft, a U.S. corporation (though the reasoning would apply equally well to a foreign provider who is sufficiently present in the United States), and the data is accessible and producible by Microsoft to the U.S. government in the United States, no more is needed to enforce the warrant. The inquiry stops there.

The panel majority rejected this position, and a few reflections illustrate why we were correct to do so. First: The position of the government and the dissenters necessarily ignores situations in which the effects outside the United States are less readily dismissed, whichever label is chosen to describe the “focus” of the statute. For example, under the dissents’ reasoning (as we understand it), the SCA warrant is valid when (1) it is served in the United States on a branch office of an Irish service provider, (2) it seeks content stored in Ireland but accessible at the U.S. branch, (3) the account holding that content was opened and established in Ireland by an Irish citizen, (4) the disclosure demanded by the warrant would breach Irish law, and (5) U.S. law enforcement could request the content through the MLAT process.⁸ This hardly seems like a

credit, provide electronic communications services to customers resident around the globe, this observation suggests the demerits of the analysis.

⁸ As noted in the panel majority opinion, MLATs are Mutual Legal Assistance Treaties “between the United States and other countries, which allow signatory states to request one another’s assistance with ongoing criminal investigations, including issuance and

“domestic application” of the SCA. Rather, we find it difficult to imagine that the Congress enacting the SCA envisioned such an application, much less that it would not constitute the type of extraterritorial application with which *Morrison* was concerned. Indeed, calling such an application “domestic” runs roughshod over the concerns that undergird the Supreme Court’s strong presumption against extraterritoriality, and suggests the flaw in an approach to the SCA that considers only disclosure. *See Morrison*, 561 U.S. at 269 (citing “probability of incompatibility with applicable laws of other countries” as signaling absence of congressional attention to extraterritorial application); *EEOC v. Arabian Am. Oil Corp.*, 499 U.S. 244, 248 (1991) (observing that presumption against extraterritoriality “serves to protect against unintended clashes between our laws and those of other nations”).

execution of search warrants.” *Microsoft*, 829 F.3d at 221. The United States has entered into approximately 56 MLATs with foreign countries, including all member states of the European Union, and holds related Mutual Legal Assistance Agreements with others. *See id.* n.29; U.S. Dep’t of State, *Treaties & Agreements*, <https://www.state.gov/j/inl/rls/nrcrpt/2012/vol2/184110.htm>. As the dissenters fairly point out, however, the United States lacks an MLAT relationship with many countries, and the MLAT process can be cumbersome. *See post* at 5 n.11 (Cabrane, J., dissenting from the denial of reh’g *en banc*). In this case, the Republic of Ireland filed a brief *amicus curiae*, acknowledging its MLAT with the United States and representing its willingness “to consider, as expeditiously as possible, a request under the treaty.” Br. *Amicus Curiae* Ireland 4, *Microsoft Corp. v. United States*, No. 14-2985 (2d Cir. December 2014).

Second: My dissenting colleagues take issue with the idea that “privacy” can have a territorial locus at all when it comes to electronic data, given the ease with which the data can be subdivided or moved across borders and our now familiar notion of data existing in the ephemeral “cloud.” But, mundane as it may seem, even data subject to lightning recall has been stored somewhere, and the undisputed record here showed that the “somewhere” in this case is a datacenter firmly located on Irish soil.⁹ *See Microsoft*, 829 F.3d at 220 n.28. (Fragmentation, an issue raised by the government in its petition and by the dissents here, was not present in the facts before the panel, and only further emphasizes the need for a modernized statute.) When Congress passed the “*Stored Communications Act*” in 1986, the statute it enacted protected data by limiting access to the “facility” where the data is stored or through which electronic services are provided. 18 U.S.C. § 2701(a). It did not address the

⁹ Microsoft represents in the record that it stores data in different locations around the world not at whim, but for competitive commercial reasons: so that the data can be more quickly recalled for users based on proximity to their reported geographic locations. *See Microsoft*, 829 F.3d at 202. The record contains no basis for speculating that it has stored data in locations engineered to avoid an obligation to produce the data in response to law enforcement needs or to enable criminal activity to go undetected. Nor, although a customer could certainly do so, does the record suggest that the customer whose account is at issue falsely designated Ireland as its location to escape the reach of U.S. law enforcement. That customer could as well be a citizen of Ireland as of any other nation.

citizenship of the account holder, the nationality of the service provider, or any of the concerns that can be cited, legitimately, as relevant today to defining a sound policy concerning the privacy and disclosure of protected user content in a global setting. Nor have we been pointed to evidence suggesting that sovereigns have relinquished any claim to control over data physically stored within their boundaries. (Ireland certainly did not do so here in its submission *amicus curiae*.) Although the realities of electronic storage have widely outstripped what Congress envisioned in 1986, we are not so far from the context of the SCA that we can no longer apply it faithfully.

To connect these two points: Some of my dissenting colleagues, *see post* at 5 (Jacobs, *J.*, dissenting from the denial of reh'g *en banc*), like the panel, have noted potential concerns with reciprocity—that if the United States can direct a service provider with operations in the United States to access data of a foreign citizen stored in a foreign country, a foreign sovereign might claim authority to do the same and access data of a U.S. citizen stored in the United States, so long as the data would be disclosed abroad. If this concern holds any intuitive force, it does so only because the location of data storage *does* still have import, and therefore reaching across physical borders to access electronic data gives us pause when

we are on the receiving end of the intrusion. It is for just this sort of reason that the government has entered into MLATs with other sovereigns: to address mutual needs for law enforcement while respecting sovereign borders. And it is for just this sort of reason that the government has in other circumstances taken a position, somewhat in tension with the one it takes here, that courts should be particularly solicitous of sovereignty concerns when authorizing data to be collected in the United States but drawn from within the boundaries of a foreign nation. *See, e.g.,* Br. United States *Amicus Curiae* Opp'n Pet. Writ Cert. 8-21, *Arab Bank, PLC v. Linde*, No. 12-1485 (May 2014) (contending, in civil discovery context, that lower courts erred in "failing to accord sufficient weight to the foreign jurisdictions' interests in enforcing their bank secrecy laws").

Third, and finally: The exercise of selecting a "focus" and then determining its territorial locus highlights some of the difficulties inherent in applying the *Morrison* extraterritoriality analysis. Where the panel majority and the dissents diverge most sharply and meaningfully is on the better view of the legal consequences of the focus inquiry: *where*—for purposes of assessing extraterritoriality according to the Supreme Court's precedents—to locate the affected interest. Once we concluded that the statute focuses on protecting

privacy, the panel majority had to assess further where privacy might be considered to be physically based—an elusive inquiry, at best. As noted, the dissents emphasize disclosure, and reason from that premise that the place of disclosure establishes whether the proposed application of the statute is domestic. But we saw the overarching goal of the SCA as protecting privacy and allowing only certain exceptions, of which limited disclosure in response to a warrant is one. Considerations of privacy and disclosure cannot be divorced; they are two sides of the same coin. By looking past privacy and directly to disclosure, however, the dissents would move the “focus” of the statute to its exceptions, and away from its goal. The better approach, which in our estimation is more in keeping with the *Morrison* analysis and the SCA’s emphasis on data storage, is one that looks to the step taken before disclosure—access—in determining privacy’s territorial locus.

With a less anachronistic statute or with a more flexible armature for interpreting questions of a statute’s extraterritoriality, we might well reach a result that better reconciles the interests of law enforcement, privacy, and international comity. In an analytic regime, for example, that invited a review of the totality of the relevant circumstances when assessing a statute’s potential

extraterritorial impact, we might be entitled to consider the residency or citizenship of the client whose data is sought, the nationality and operations of the service provider, the storage practices and conditions on disclosure adopted by the provider, and other related factors. And we can expect that a statute designed afresh to address today's data realities would take an approach different from the SCA's, and would be cognizant of the mobility of data and the varying privacy regimes of concerned sovereigns, as well as the potentially conflicting obligations placed on global service providers like Microsoft. As noted above, there is no suggestion that Congress could not extend the SCA's warrant procedures to cover the situation presented here, if it so chose.

These were not the statutory context and precedent available to the panel, however, nor would they be available to our Court sitting *en banc*. Under the circumstances presented to us, the Microsoft warrant was properly quashed.

CHRISTOPHER F. DRONEY, *Circuit Judge*, joined by DENNIS JACOBS, JOSÉ A. CABRANES, and REENA RAGGI, *Circuit Judges*, dissenting from the denial of rehearing *en banc*:

The majority opinion undertook the daunting task of attempting to apply a statute enacted decades ago to present technology. For example, who knew in 1986 that electronic mail — “email” — would become such a primary means of communication that its commercial providers would have millions of servers across the world to store and manage those communications? Or that the recipient of the warrant here — Microsoft — would itself manage over one million server computers, located in over forty countries, used by over one billion customers? Such developments in electronic communications could not have been anticipated at the time of the statute’s adoption. Indeed, the task of applying statutes and rules from many years ago to unanticipated advances in technology has been undertaken in other contexts with much difficulty. *See, e.g., United States v. Ganius*, 824 F.3d 199, 219–21 (2d Cir. 2016) (*en banc*). Thus, although I agree that reconsideration *en banc* should have occurred, I do so while recognizing the majority’s efforts to solve the vexing issues presented here.

I dissent, though, from the denial of *en banc* in this case for three reasons. First, the privacy interests that are the focus of many aspects of the Stored Communications Act (“SCA”) are protected in this context by its warrant requirement. Second, the activity that is the focus of the disclosure aspects of the SCA would necessarily occur in the United States where Microsoft is headquartered and where it would comply with the § 2703 warrant, not in the foreign country where it has chosen to store the electronic communications of its customers; also, the provisions of the statute concerning the mechanics of disclosure of these communications are unrelated to its privacy provisions. Third, the prudent course of action is to allow the warrants to proceed, and if Congress wishes to change the statute, it may do so while important criminal investigations continue.

When determining whether a statute applies extraterritorially, a court must read the statute provision by provision, not as a whole. *RJR Nabisco, Inc. v. European Community*, 136 S. Ct. 2090, 2103 (2016) (analyzing provisions individually to determine the focus of each). The court is then tasked with “determin[ing] whether the case involves a domestic application of the statute, and [does] this by looking to the statute’s ‘focus.’” *Id.* at 2101.

As the majority opinion notes, the SCA was broadly focused on the privacy concerns of electronic communications and the parties to those communications. *See* Maj. Op. at 33-36. But Congress addressed those concerns through the warrant requirement in the SCA. *See* 18 U.S.C. § 2703. That requirement provides protection for individual privacy interests by requiring the Government to make an adequate showing of probable cause of evidence of a crime or property used to commit a crime to a judge—a well-established standard of Fourth Amendment protection. *See id.*; Fed. R. Crim. P. 41(c); U.S. Const. amend. IV (“[N]o warrants shall issue, but upon probable cause.”); *Camara v. Mun. Court of City & Cnty. of S.F.*, 387 U.S. 523, 528 (1967) (explaining that purpose of Fourth Amendment’s probable cause requirement “is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials”).

Furthermore, the provisions of the SCA concerning the means of disclosure following obtaining the warrant are quite separate from the privacy components of the SCA. Section 2703 includes a number of specific disclosure provisions, which state it is the *provider* of the electronic communication service that is the source of the records sought by the Government either pursuant to the

warrant or the other means provided by that section to properly obtain the electronic communications. *See id.* § 2703 (a) (“A governmental entity may require the disclosure *by a provider* of electronic communication service of the contents of a wire or electronic communication . . .”) (emphasis added); § 2703 (b)(1) (“A governmental entity may require *a provider* of remote computing service to disclose the contents of any wire or electronic communication . . .”) (emphasis added); § 2703 (c)(1) & (2) (both describing disclosure by providers); § 2703 (g) (same).

Thus, the only permissible reading of § 2703 is that it is the location of the provider of the electronic communication service that is relevant to determining whether the SCA is being applied extraterritorially under *RJR Nabisco*. Microsoft is headquartered in the United States, and there is no question that it would make the disclosure mandated by the § 2703 warrant in this country.

It makes no difference that Microsoft has chosen to store some electronic communications in other countries. That decision is based on its own business considerations, not privacy concerns for its customers. Microsoft has possession and immediate access to those emails regardless of where it chose to store them. Thus, the second prong of the *RJR Nabisco* test is satisfied here: the disclosure of

the electronic communications occurs in the United States, when Microsoft honors the warrant by disclosing those communications.

It is also important to note that the interests of foreign internet electronic communication service providers, whose headquarters are abroad and whose customers choose to subscribe to those services with the knowledge that the provider is located outside the United States, are not at stake here. If the emails sought by the Government in this case were maintained by a foreign-based internet service provider, the situation would be quite different. Here, however, the majority's concerns regarding "the interests of comity that . . . ordinarily govern the conduct of cross-boundary criminal investigations," *Maj. Op.* at 42, are overstated when the warrant is served on a U.S.-based electronic communication service provider for stored emails of a customer who *chose* to have a U.S.-based electronic communication service provider furnish his email service.

There is a real and practical component to the denial of *en banc* review of this case. This is a case that turns on statutory interpretation under *RJR Nabisco* rather than responding to a direct challenge to the constitutionality of the SCA or its disclosure provisions. The denial of *en banc* review hobbles both this specific

Government investigation as well as many others, important not only to the United States but also foreign nations. The Government's interest in continuing critical investigations into criminal activity is manifest. If Congress wishes to revisit the privacy and disclosure aspects of § 2703, it is free to do so when it chooses to do so. Until that time, this Court should allow the warrants to compel disclosure pursuant to § 2703 as it exists, and allow the Government to do its job in investigating serious criminal activity.

For these reasons, I respectfully dissent from the denial of *en banc* review.

DENNIS JACOBS, *Circuit Judge*, joined by JOSÉ A. CABRANES, REENA RAGGI, and CHRISTOPHER F. DRONEY, *Circuit Judges*, dissenting from the denial of rehearing in banc:

The United States has ordered Microsoft to provide copies of certain emails pursuant to the Stored Communications Act. A magistrate judge found probable cause to believe those emails contain evidence of a crime. (The instrument functions as a subpoena though the Act calls it a warrant.) A panel of this Court directed the district court to quash the warrant as an unlawful extraterritorial application of the Act. Now, in a vote split four–four, we decline to rehear the case in banc. I respectfully dissent from the denial.

I subscribe to the dissents of Judge Cabranes, Judge Raggi, and Judge Droney, which set out in detail the doctrinal basis for the right result in this appeal. I write separately to describe an approach that is perhaps more reductionist.

I

As all seem to agree, and as the government concedes, the Act lacks extraterritorial reach. However, no extraterritorial reach is needed to require delivery in the United States of the information sought, which is easily accessible

in the United States at a computer terminal. The majority nevertheless undertakes to determine whether this case presents a forbidden extraterritorial application by first “look[ing] to the ‘territorial events or relationships’ that are the ‘focus’ of the relevant statutory provision.” Majority Op., 829 F.3d at 216 (quoting *Mastafa v. Chevron Corp.*, 770 F.3d 170, 183 (2d Cir. 2014)). Oddly, the majority then holds that the relevant “territorial” “focus” is user privacy. But privacy, which is a value or a state of mind, lacks location, let alone nationality.¹ Territorially, it is nowhere. Important as privacy is, it is in any event protected by the requirement of probable cause; so a statutory focus on privacy gets us no closer to knowing whether the warrant in question is enforceable.

Extraterritoriality need not be fussed over when the information sought is already within the grasp of a domestic entity served with a warrant. The warrant in this case can reach what it seeks because the warrant was served on Microsoft, and Microsoft has access to the information sought. It need only touch some keys in Redmond, Washington. If I can access my emails from my

¹ As Judge Lynch wrote in his panel concurrence, privacy “is an abstract concept with no obvious territorial locus,” and the majority’s conclusion therefore “does not really help us to distinguish domestic applications of the statute from extraterritorial ones.” Concurring Op., 829 F.3d at 230 n.7.

phone, then in an important sense my emails are in my pocket, notwithstanding where my provider keeps its servers.

The majority opinion relies on an implicit analogy to paper documents: “items” and “material” and “content” that are “located” and “stored” and that the government seeks to “collect” and “import.” But electronic data are not stored on disks in the way that books are stored on shelves or files in cabinets. Electronic “documents” are literally intangible: when we say they are stored on a disk, we mean they are encoded on it as a pattern. At stake in this case is not whether Microsoft can be compelled to import and deliver a disk (or anything else), but whether Microsoft can be compelled to deliver information that is encoded on a disk in a server and that Microsoft can read.

The panel’s approach is unmanageable, and increasingly antiquated. As explained in an article Judge Lynch cites in his concurrence (829 F.3d at 229): “[T]he very idea of online data being located in a particular physical ‘place’ is becoming rapidly outdated,” because electronic “files [can] be fragmented and the underlying data located in many places around the world” such that the files “only exist in recognizable form when they are assembled remotely.” Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. Pa. L. Rev. 373, 408

(2014). The underlying data can be fragmented or recombined, copied or transferred, for convenience or maintenance or economy – or (not incidentally) to evade the police. And all that can be done at the direction of the user or without the user's knowledge, and without a care for national boundaries, tariffs or postage. Nothing moves but information.

To enforce the warrant, there is no practical alternative to relying upon access, and no need to seek an alternative. We can conclude that warrants can reach what their recipients can deliver: if the recipient can access a thing here, then it can be delivered here; and if statutory and constitutional standards are met, it should not matter where the ones-and-zeroes are "stored."

Localizing the data in Ireland is not marginally more useful than thinking of Santa Claus as a denizen of the North Pole. Problems arise if one over-thinks the problem, reifying the notional: Where in the world is a Bitcoin? Where in my DVR are the images and voices? Where are the snows of yesteryear?

II

The majority has found no indication that Congress considered in 1986 whether a warrant issued under the Act would reach data stored on servers outside the United States; and Judge Lynch's concurrence, having recognized the

flaws in the majority opinion, calls on Congress to modernize the statute. I too would like to see Congress act, chiefly to consider certain ramifications, such as whether the United States might be vulnerable to reciprocal claims of access through local offices of American companies abroad. But we are not in a position to punt when it comes to construing a statute that either does or does not allow execution of a warrant in a case that is before us now. Holding, as the panel did, that the statute does not allow enforcement of this warrant is an interpretation of the statute, not a deferential bow to Congress. So though it would best if Congress could form a consensus on the issue, that preference is not a principle of statutory construction.

Nor can it matter how we would order legislative priorities (this would seem to be a bit down the list), or how much we would welcome bipartisan consideration of a bill that has not been enacted. Legislative proposals are myriad, and they fall as leaves. Come what may, we are left for now with the law as it is. The panel misconstrues it, and I would rehear the case in banc.

14-2985

Microsoft Corp. v. United States

**United States Court of Appeals
FOR THE SECOND CIRCUIT**

At a stated term of the United States Court of Appeals for the Second Circuit, held at the Thurgood Marshall United States Courthouse, 40 Foley Square, in the City of New York, on the 24th day of January, two thousand seventeen.

PRESENT: ROBERT A. KATZMANN,
Chief Judge,
DENNIS JACOBS,
JOSÉ A. CABRANES,
ROSEMARY S. POOLER,
REENA RAGGI,
PETER W. HALL,
DEBRA ANN LIVINGSTON,
DENNY CHIN,
RAYMOND J. LOHIER, JR.,
SUSAN L. CARNEY,
CHRISTOPHER F. DRONEY,
Circuit Judges.

-----x

In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and
Maintained by Microsoft Corporation

-----x

MICROSOFT CORPORATION,

Appellant,

v.

14-2985

UNITED STATES OF AMERICA,

Appellee.

-----x

E. Joshua Rosenkranz, Orrick, Herrington & Sutcliffe LLP (Robert M. Loeb and Brian P. Goldman, Orrick, Herrington & Sutcliffe LLP, New York, NY; Guy Petrillo, Petrillo Klein & Boxer LLP, New York, NY; James M. Garland and Alexander A. Berengaut, Covington & Burling LLP, Washington, DC; Bradford L. Smith, David M. Howard, John Frank, Jonathan Palmer, and Nathaniel Jones, Microsoft Corp., Redmond, WA; *on the brief*), *for Microsoft Corporation.*

Justin Anderson, Assistant United States Attorney (Serrin Turner, Assistant United States Attorney, *on the brief*), *for* Preet Bharara, United States Attorney for the Southern District of New York, New York, NY.

Brett J. Williamson, David K. Lukmire, Nate Asher, O'Melveny & Myers LLP, New York, NY; Faiza Patel, Michael Price, Brennan Center for Justice, New York, NY; Hanni Fakhoury, Electronic Frontier Foundation, San Francisco, CA; Alex Abdo, American Civil Liberties Union Foundation, New York, NY; *for Amici Curiae* Brennan Center for Justice at NYU School of Law, American Civil Liberties Union, The Constitution Project, and Electronic Frontier Foundation, *in support of Appellant.*

Kenneth M. Dreifach, Marc J. Zwillinger, Zwillgen PLLC, New York, NY and Washington, DC, *for Amicus Curiae Apple, Inc., in support of Appellant.*

Andrew J. Pincus, Paul W. Hughes, Mayer Brown LLP, Washington, DC, *for Amici Curiae BSA | The Software Alliance, Center for Democracy and Technology, Chamber of Commerce of the United States, The National Association of Manufacturers, and ACT | The App Association, in support of Appellant.*

Steven A. Engel, Dechert LLP, New York, NY, *for Amicus Curiae Anthony J. Colangelo, in support of Appellant.*

Alan C. Raul, Kwaku A. Akowuah, Sidley Austin LLP, Washington, DC, *for Amici Curiae AT&T Corp., Rackspace US, Inc., Computer & Communications Industry Association, i2 Coalition, and Application Developers Alliance, in support of Appellant.*

Peter D. Stergios, Charles D. Ray, McCarter & English, LLP, New York, NY and Hartford, CT, *for Amicus Curiae Ireland.*

Peter Karanjia, Eric J. Feder, Davis Wright Tremaine LLP, New York, NY, *for Amici Curiae Amazon.com, Inc., and Accenture PLC, in support of Appellant.*

Michael Vatis, Jeffrey A. Novack, Steptoe & Johnson LLP, New York, NY; Randal S. Milch, Verizon Communications Inc., New York, NY; Kristofor T.

Henning, Hewlett-Packard Co., Wayne, PA; Amy Weaver, Daniel Reed, Salesforce.com, Inc., San Francisco, CA; Orin Snyder, Thomas G. Hungar, Alexander H. Southwell, Gibson, Dunn & Crutcher LLP, New York, NY; Mark Chandler, Cisco Systems, Inc., San Jose, CA; Aaron Johnson, eBay Inc., San Jose, CA, *for Amici Curiae* Verizon Communications, Inc., Cisco Systems, Inc., Hewlett-Packard Co., eBay Inc., Salesforce.com, Inc., and Infor, *in support of Appellant*.

Laura R. Handman, Alison Schary, Davis Wright Tremaine LLP, Washington, DC, *for Amici Curiae* Media Organizations, *in support of Appellant*.

Philip Warrick, Klarquist Sparkman, LLP, Portland, OR, *for Amici Curiae* Computer and Data Science Experts, *in support of Appellant*.

Owen C. Pell, Ian S. Forrester, Q.C., Paige C. Spencer, White & Case, New York, NY, *for Amicus Curiae* Jan Philipp Albrecht, Member of the European Parliament, *in support of Appellant*.

Owen C. Pell, Ian S. Forrester, Q.C., Paige C. Spencer, White & Case, New York, NY; Edward McGarr, Simon McGarr, Dervila McGirr, McGarr Solicitors, Dublin, Ireland, *for Amicus Curiae* Digital Rights Ireland Limited, National Council for Civil Liberties, and The Open Rights Group, *in support of Appellant*.

ORDER

Following disposition of this appeal, an active judge of the Court requested a poll on whether to rehear the case *en banc*.^{*} A poll having been conducted and there being no majority favoring *en banc* review, rehearing *en banc* is hereby **DENIED**.

Susan L. Carney, *Circuit Judge*, concurs by opinion in the denial of rehearing *en banc*.

Dennis Jacobs, *Circuit Judge*, joined by José A. Cabranes, Reena Raggi, and Christopher F. Droney, *Circuit Judges*, dissents by opinion from the denial of rehearing *en banc*.

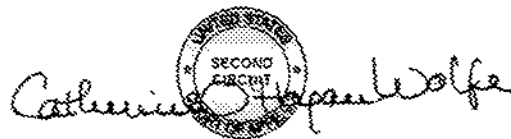
José A. Cabranes, *Circuit Judge*, joined by Dennis Jacobs, Reena Raggi, and Christopher F. Droney, *Circuit Judges*, dissents by opinion from the denial of rehearing *en banc*.

Reena Raggi, *Circuit Judge*, joined by Dennis Jacobs, José A. Cabranes, and Christopher F. Droney, *Circuit Judges*, dissents by opinion from the denial of rehearing *en banc*.

Christopher F. Droney, *Circuit Judge*, joined by Dennis Jacobs, José A. Cabranes, and Reena Raggi, *Circuit Judges*, dissents by opinion from the denial of rehearing *en banc*.

FOR THE COURT:

CATHERINE O'HAGAN WOLFE, CLERK

The image shows a handwritten signature, "Catherine O'Hagan Wolfe", written in cursive over a circular official seal. The seal contains the text "UNITED STATES" at the top, "SECOND CIRCUIT" in the center, and "NEW YORK" at the bottom.

^{*} The following active judges were recused from participating in the poll: Rosemary S. Pooler, Debra Ann Livingston, and Raymond J. Lohier, Jr.

REENA RAGGI, *Circuit Judge*, joined by DENNIS JACOBS, JOSÉ A. CABRANES, and CHRISTOPHER F. DRONEY, *Circuit Judges*, dissenting from the order denying rehearing *en banc*:

In this case, a panel of the court quashes a compelled-disclosure warrant issued under the Stored Communications Act (“SCA”) by a neutral magistrate and supported by probable cause to think that the information demanded is evidence of a crime. *See* 18 U.S.C. § 2703(a). The ground for decision is the presumption against extraterritoriality, *see Morrison v. Nat’l Australia Bank Ltd.*, 561 U.S. 247, 255 (2010), which the panel construes to allow United States corporation Microsoft to refuse to disclose subscriber communications in its possession and responsive to the warrant because Microsoft, for its own business reasons and unbeknownst to its subscriber, has chosen to store the communications in Ireland. The panel does not simply set a *higher* bar for the government to secure such electronic communications. Rather, it erects an “*absolute*” bar so that “the government can never obtain a warrant that would require Microsoft,” or any other U.S.-based service provider, to turn over electronic communications stored abroad, “however certain it may be that they contain evidence of criminal activity, and even if that criminal activity is a

terrorist plot.” *Microsoft Corp. v. United States* (“*Microsoft*”), 829 F.3d 197, 224 (2d Cir. 2016) (Lynch, J., concurring in the judgment) (emphasis in original).¹ This ruling merits *en banc* review. To the extent an equally divided court today denies such review, I respectfully dissent.

1. Matter of Exceptional Importance

The panel’s ruling, the reasoning informing it, and its disturbing consequences raise questions “of exceptional importance to public safety and national security.” Cabranes, J., Op. Dissenting from Denial of Reh’g En Banc (“Cabranes, J., Op.”), *ante* at 1. The panel nevertheless urges us to forego *en banc* review because the SCA is outdated and overdue for congressional revision. See *Microsoft*, 829 F.3d at 201; Carney, J., Op. Concurring in Denial of Reh’g En Banc (“Carney, J., Op.”), *ante* at 2 & n.3. I am not persuaded.

This is not a case where some legal principle (*e.g.*, standing, mootness) allowed the panel to avoid applying the SCA, thereby affording Congress time to enact new legislation. This is a case where the panel reached the merits and

¹ On the panel’s reasoning, if on September 10, 2001, the government had been able to show probable cause to believe that Mohamed Atta, Abdul Aziz al Omari, etc., were communicating electronically about an imminent, devastating attack on the United States, and that Microsoft possessed those emails, no federal court could have issued a § 2703(a) warrant compelling Microsoft to disclose those emails if it had stored them overseas, even though its employees would not have had to leave their desks in Redmond, Washington, to retrieve them.

construed the SCA to foreclose altogether § 2703(a) warrants requiring United States service providers to disclose electronic communications stored overseas. This construction now controls the SCA's application in this circuit. In its Petition for Rehearing, the government details the immediate and serious adverse consequences of such a ruling. *See* Gov't Pet. for Reh'g at 18–19; *see also* Cabranes, J., Op., *ante* at 2–7. These consequences cannot be attributed to deficiencies in the SCA. Rather, they derive from the panel's conclusion—mistaken in my view—that the SCA is impermissibly being applied extraterritorially when a § 2703(a) warrant requires a United States service provider to disclose electronic communications that it has elected to store abroad. It is simply unprecedented to conclude that the presumption against extraterritoriality bars United States courts with personal jurisdiction over a United States person from ordering that person to produce property in his possession (wherever located) when the government has made a probable cause showing that the property is evidence of a crime. This alone warrants *en banc* review.

2. The Panel's Discussion of "Warrant"

Several aspects of the panel's extraterritoriality analysis require particular review. The first is the panel's lengthy discussion of why Congress's "use of the term of art 'warrant'" in the SCA manifests an intent for the statute to operate only domestically. *Microsoft*, 829 F.3d at 212. At the outset, I note that there was no need for the panel to locate *domestic* intent in the SCA; it is presumed in the absence of a showing of express *extraterritorial* intent, which the government concedes is absent here. *See Morrison v. Nat'l Australia Bank Ltd.*, 561 U.S. at 255. The panel majority's "warrant" discussion, however, is not simply unnecessary. It is also flawed in ways that lay an unsound foundation for the panel's ensuing identification of statutory "focus."

Notably, the panel majority concludes that Congress's use of the term "warrant" in § 2703 signals its intent to invoke all of the "traditional, domestic connotations" that pertain to traditional search warrants. *Microsoft*, 829 F.3d at 213. But, as Judge Lynch observes, a § 2703(a) warrant is not a traditional warrant. *Id.* at 226 (Lynch, J., concurring in the judgment). It does not authorize federal agents to *search* any premises or to *seize* any person or materials. Rather, it authorizes a federal agent to require a service provider to disclose materials in

its possession. The difference is significant to identifying where a warrant is being executed. Because a search warrant is executed with respect to a *place*—the place to be searched—the presumption against extraterritoriality expects that place to be within United States territory. By contrast, because a § 2703(a) warrant is executed with respect to a *person*—the person ordered to divulge materials in his possession—the presumption against extraterritoriality expects that person to be within United States territory and subject to the court’s jurisdiction. If the person is so present, execution of the warrant as to him is a domestic application of United States law without regard to from where the person must retrieve the materials ordered disclosed. Indeed, if that were not so, subpoenas requiring persons in this country to produce materials that they must retrieve from abroad could not be enforced, a position contrary to well established law. *See, e.g., Marc Rich & Co., A.G. v. United States*, 707 F.2d 663, 668–70 (2d Cir. 1983); *United States v. Bank of Nova Scotia (In re Grand Jury Proceedings)*, 740 F.2d 817, 826–29 (11th Cir. 1984).

Thus, I respectfully submit that the panel majority’s extraterritoriality analysis starts with the mistaken equation of § 2703(a) warrants with traditional

search warrants. This, in turn, leads to the mistaken conclusion that “a warrant protects privacy in a distinctly territorial way.” *Microsoft*, 829 F.3d at 212.

As to the latter point, the reason United States search warrants do not apply extraterritorially has to do with *sovereignty*, not *privacy*. Since before the republic, the law of nations has recognized that one sovereign cannot unilaterally enforce its criminal laws within the territory of another.² But a defendant’s expectations of privacy do not preclude evidence so obtained from being used in a United States prosecution. See *In re Terrorist Bombings of U.S. Embassies in E. Africa*, 552 F.3d 157, 176–77 (2d Cir. 2008). Thus, it is respect for sovereign independence that has prompted us to observe that “search warrants intended to have extraterritorial effect . . . would have dubious legal significance, if any, in a foreign nation.” *Id.* at 171. But this observation, quoted by the panel majority, does not support its ensuing conclusion that, “[a]ccordingly, a warrant protects

² See Restatement (Third) of Foreign Relations Law § 432(2) (“A state’s law enforcement officers may exercise their functions in the territory of another state only with the consent of the other state, given by duly authorized officials of that state.”); 1 *Oppenheim’s International Law* § 119 (Robert Jennings & Arthur Watts, eds., 9th ed. 1992) (“It is . . . a breach of international law for a state without permission to send its agents into the territory of another state to apprehend persons accused of having committed a crime.”); *The Apollon*, 22 U.S. (9 Wheat.) 362, 371 (1824) (Story, J.) (holding that “[i]t would be monstrous to suppose that our revenue officers were authorized to enter into foreign ports and territories, for the purpose of seizing vessels which had offended against our laws” because such conduct would be “a clear violation of the laws of nations”); *The Nereide*, 13 U.S. (9 Cranch) 388, 423 (1815) (Marshall, C.J.) (“[T]he Court is bound by the law of nations which is a part of the law of the land.”).

privacy in a distinctly territorial way.” *Microsoft*, 829 F.3d at 212 (emphasis added).

As Judge Lynch explains, how warrants protect *privacy* is through the Fourth Amendment requirement that they issue only “upon probable cause.” U.S. Const. amend. IV; *see Microsoft*, 829 F.3d at 223 (Lynch, J., concurring in the judgment). Indeed, to the extent the SCA’s legislative history shows Congress’s intent to extend privacy protections, specifically, protections “analogous to those provided by the Fourth Amendment,” to certain electronic communications, *Microsoft*, 829 F.3d at 206 (quoting Gov’t Br. at 29), one might better understand Congress to have used the term “warrant” in § 2703(a) to ensure that certain disclosures would be compelled only upon a showing of probable cause. Thus, when a § 2703(a) warrant supported by probable cause is executed on a person within the jurisdiction of the United States, the SCA is being applied domestically without regard to the location of the materials that the person must divulge.

As Judge Cabranes observes, by failing to recognize these distinctions (a) between search warrants directed to particular locations and § 2703(a) warrants directed to particular persons, and (b) between the values of sovereignty and

privacy, the panel majority construes “warrant” as used in § 2703 to yield a perverse result: affording *greater* privacy protection to foreign citizens and Americans who claim to reside abroad than to resident U.S. citizens. *See* Cabranes, J., Op., *ante* at 7–8 n.19. This troubling result and the reasons leading to it warrant *en banc* review.

3. The Focus of the Statute

Where, as here, the government does not argue that Congress intended for § 2703(a) to apply extraterritorially, the determinative question asks whether the domestic contacts associated with that statutory provision are sufficient to avoid triggering the presumption against extraterritoriality. To answer that question, a court looks to “the territorial events or relationships” that are the “focus” of the relevant statutory provision. *Mastafa v. Chevron Corp.*, 770 F.3d 170, 184 (2d Cir. 2014) (alterations omitted); *Morrison v. Nat’l Australia Bank Ltd.*, 561 U.S. at 266–68. The panel majority identifies “privacy” as the focus of § 2703(a)’s warrant requirement. *Microsoft*, 829 F.3d at 217. It then reasons that because the § 2703(a) warrant here sought disclosure of the electronic communications of a Microsoft customer, and because Microsoft stored those communications in Dublin, “[t]he content to be *seized* is stored in Dublin.” *Id.* at 220 (emphasis added). This in

turn leads it to conclude that “the invasion of the customer’s privacy takes place under the SCA where the customer’s protected content is accessed—here, where it is *seized by Microsoft, acting as an agent of the government.*” *Id.* (emphasis added). Accordingly, it concludes that the § 2703(a) warrant is being executed in Ireland in violation of the presumption against extraterritoriality.

This reasoning raises several concerns.

First, I cannot agree that a person who is compelled by a § 2703(a) warrant to disclose to the government materials already in that person’s possession is “seiz[ing]” anything as an agent of the government. *See id.* The cases cited by the panel majority identify such agency where property is *not* already in an actor’s possession. In such circumstances, but for authorizing law or warrant, the actor could not lawfully take possession of—*i.e.*, seize—third-party materials. That is not the case here. Microsoft did not need any warrant from the United States to take possession of the subscriber communications it had stored in Ireland. Nor did it need such a warrant to transfer those communications from Ireland to the United States. Indeed, it did not need the approval of Irish authorities or even of its subscriber to take such action. Thus, it is simply wrong to characterize Microsoft’s actions in retrieving customer electronic data in

Ireland as “Microsoft’s *execution* of the warrant,” much less as a *seizure* by Microsoft. Carney, J., Op., *ante* at 3 (emphasis added); *see Microsoft*, 829 F.3d at 220. The § 2703(a) warrant here at issue was executed by *federal authorities*, who were thereby authorized to compel Microsoft to *disclose* communications already lawfully in its possession. Such disclosure by Microsoft would otherwise have been prohibited by 18 U.S.C. § 2702(a). But the only territorial event that needs to be warranted under the SCA is disclosure. No warrant was needed for Microsoft lawfully to access material on its Dublin servers from the United States. Nor is a different conclusion supported by the panel majority’s observation that our court “has never upheld the use of a subpoena to compel a recipient to produce an item under its control and located overseas when the recipient is merely a caretaker for another individual or entity and that individual, not the subpoena recipient, has a protectable privacy interest in the item.” *Microsoft*, 829 F.3d at 215. The question whether the caretaker’s actions respecting materials in his possession constitute a “search” or “seizure” undertaken as an agent of the government does not turn on whether the item is located here or overseas. Indeed, as Judge Lynch states, we have upheld the use of a subpoena to compel a caretaker to produce client materials in its domestic

possession. *See id.* at 228 n.5 (Lynch, J., concurring in the judgment) (citing *In re Horowitz*, 482 F.2d 72 (2d Cir. 1973)). Such a conclusion would not have been possible if the caretaker's actions respecting materials in his possession equated to a "search" or "seizure" undertaken as an agent of the government.

Thus, we need to convene *en banc* to clarify that a service provider who complies with a § 2703(a) warrant compelling disclosure of communications in his lawful possession does not thereby conduct a search or seizure as the agent of the government.

Second, I also cannot agree with the panel that *privacy* is the focus of § 2703 and that subscriber privacy would be invaded *in Ireland* were Microsoft to access its subscriber files there. To the extent § 2702(a) generally prohibits a service provider from knowingly disclosing subscribers' electronic communications to third parties, that provision might be understood to focus on enhancing subscriber privacy. But § 2703 identifies circumstances when the government nevertheless "may require" service providers to disclose their subscribers' communications. This gives some force to the government's argument that the focus of § 2703 is compelled *disclosure*, not enhanced *privacy*. *See* Gov't Pet. for Reh'g at 11–12 (noting that focus inquiry is "provision-specific" and citing *RJR*

Nabisco, Inc. v. European Cmty., 136 S. Ct. 2090, 2101–11 (2016)). *But see Microsoft*, 829 F.3d at 218–19 (rejecting disclosure focus argument).

Even assuming that the enhanced privacy and compelled disclosure provisions of the SCA are two sides of the same coin, I think the panel errs in concluding that the privacy afforded by the SCA would be invaded by Microsoft's access of its own files in Dublin rather than by its subsequent disclosure of subscriber communications in the United States.

As already stated, Microsoft is entitled to access and to move subscriber communications at will, even without consulting its subscriber. Such actions by Microsoft disclose nothing to the government about the existence or content of such communications. The only privacy interest afforded by § 2702(a), however, is against such disclosure. The statute provides no privacy right against Microsoft's own handling of communications short of such disclosure. Thus, contrary to the panel, I think that, even if privacy is the focus of §§ 2702 and 2703, the territorial event that is the focus of that privacy interest is the service provider's disclosure of the subscriber communications to a third party—whether in violation of § 2702(a) or as authorized by warrant under § 2703(a). It

is where that disclosure occurs that determines whether these statutory provisions are being applied domestically or extraterritorially.

Here, there is no question that the challenged § 2703(a) warrant issued, was served on Microsoft in, and required disclosure in the United States. Thus, even if “privacy” is the statute’s “focus,” the challenged warrant here applies the statute domestically, not extraterritorially. We should say so *en banc*.

4. Concluding Observations

Two final points. As Judge Cabranes observes, and Judge Carney seems to agree, the same reasoning that leads the panel to conclude that § 2703(a) warrants cannot reach communications that Microsoft has stored in Ireland might also preclude affording § 2702(a) privacy protections to such materials. See Cabranes, J., Op., *ante* at 14 n.36; Carney, J., Op., *ante* at 7 n.6. But if § 2702(a) protections do not apply here, does the government even need a § 2703(a) warrant? Could it simply proceed by subpoena? See *Marc Rich & Co., A.G. v. United States*, 707 F.2d at 668–70; *United States v. Bank of Nova Scotia (In re Grand Jury Proceedings)*, 740 F.2d at 826–29. I think the government does need a § 2703(a) warrant because I understand both § 2702(a) protections and § 2703(a) warrants to exercise government authority domestically on persons subject to

United States jurisdiction. To the extent, however, that the panel's extraterritoriality reasoning might allow a United States service provider such as Microsoft to flout not only § 2703(a) warrants but also § 2702(a) protections simply by moving materials abroad, the need for *en banc* review is only heightened.

My second point is not unrelated. The panel concludes that, because the Congress that enacted the SCA could not have foreseen the technological context in which this case arises, the focus of the statute cannot be domestic disclosure of data that a service provider in the United States accesses from abroad. Therefore, the warrant should be quashed. It seems to me this allows the first prong of analysis—did Congress intend extraterritoriality?—to be determinative of the second—is the statute being applied extraterritorially in the case at hand? In fact, the two steps of analysis are distinct. *See Morrison v. Nat'l Australia Bank Ltd.*, 561 U.S. at 266. Whatever Congress may have foreseen about advances in electronic communications, I think, for the reasons already stated, that the SCA is being applied domestically here. The privacy protection afforded by § 2702(a) is against unauthorized *disclosure* to third parties. But a § 2703(a) warrant here specifically authorizes federal agents to compel disclosure in the United States.

Further, the party from whom such disclosure is being compelled is a United States service provider subject to the personal jurisdiction of United States courts.

In short, this is not the case hypothesized by the panel where the government might use a § 2703(a) warrant to demand communications *stored abroad* from a *foreign service provider* relating to a *foreign subscriber*. See, e.g., *Microsoft*, 829 F.3d at 231–32 (Lynch, J., concurring in the judgment); Carney, J., Op., *ante* at 8–9.

When such a case comes before us, we can certainly consider whether a court with personal jurisdiction over the foreign service provider can issue a § 2703(a) warrant compelling it to disclose in the United States communications stored abroad. But, in this case, where the warrant is directed to a United States provider over whom there is personal jurisdiction for production in the United States of specified communications on a federal magistrate’s identification of probable cause, I simply do not think we have an extraterritorial application of U.S. law.

For the foregoing reasons, this court *en banc* should enforce, not quash, the challenged § 2703(a) warrant.

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Tuesday, January 24, 2017 2:44 PM
To: [REDACTED] (DO) (FBI)
Subject: Re: OGE 450
Attachments: DR OGE 2017 .pdf; 20170124144129335.pdf

b6 -1
b7C -1

Hi again -- With apologies for my lateness, I'm attaching my OGE 450 form here as well as a separate file with my signature.
Please let me know if this is ok
thx
dan richman

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Tuesday, January 24, 2017 6:11 PM
To: [REDACTED] (OGC) (FBI)
Subject: Re: OGE-450
Attachments: DR OGE 2017 .pdf; 20170124144129335.pdf

b6 -1
b7C -1

Sorry for being slow. I send the forms to [REDACTED] this afternoon. I'm attaching them here too

From: [REDACTED] (OGC) (FBI)
Sent: Tuesday, January 24, 2017 3:52 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: OGE-450

b6 -1
b7C -1

Good afternoon Mr. Richman,

I apologize for bothering you about this, but SESU is asking if you filed your financial disclosure form (OGE-450) for FY16. They need to notify OIC. If you could confirm the status of your OGE-450, I would greatly appreciate it.

Thank you very much,

[REDACTED]
Management and Program Analyst
Office of the General Counsel
Federal Bureau of Investigation
Office: [REDACTED]
Cell: [REDACTED]

b6 -1
b7C -1
b7E -3

Confidentiality Statement:

This message is transmitted to you by the Office of the General Counsel of the Federal Bureau of Investigation. The message, along with any attachments, may be confidential and legally privileged. If you are not the intended recipient of this message, please destroy it promptly without further retention or dissemination (unless otherwise required by law). Please notify the sender of the error by a separate e-mail or by calling [REDACTED]

b7E -3

[REDACTED] (DO) (FBI)

b6 -1
b7C -1

From: [REDACTED] (DO) (FBI)
Sent: Wednesday, January 25, 2017 8:11 AM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: OGE 450

This is great. Thanks. Who do you work for/with now? I will get them to sign your form for me.

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

From: Richman, Daniel C. (DO) (OGA)
Sent: Tuesday, January 24, 2017 2:44 PM
To: [REDACTED] (DO) (FBI) [REDACTED]
Subject: Re: OGE 450

b6 -1
b7C -1
b7E -3

Hi again -- With apologies for my lateness, I'm attaching my OGE 450 form here as well as a separate file with my signature.
Please let me know if this is ok
thx
dan richman

[redacted] (OGC) (FBI)

b6 -1
b7C -1

From: [redacted] (OGC) (FBI)
Sent: Wednesday, January 25, 2017 10:00 AM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: OGE-450

Good morning,

Please do not apologize! Thank you so much.

Best,

[redacted]
Management and Program Analyst
Office of the General Counsel
Federal Bureau of Investigation
Office: [redacted]
Cell: [redacted]

b6 -1
b7C -1
b7E -3

Confidentiality Statement:

This message is transmitted to you by the Office of the General Counsel of the Federal Bureau of Investigation. The message, along with any attachments, may be confidential and legally privileged. If you are not the intended recipient of this message, please destroy it promptly without further retention or dissemination (unless otherwise required by law). Please notify the sender of the error by a separate e-mail or by calling [redacted]

b7E -3

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

From: Richman, Daniel C. (DO) (OGA)
Sent: Tuesday, January 24, 2017 6:11 PM
To: [redacted] (OGC) (FBI) [redacted]
Subject: Re: OGE-450

b6 -1
b7C -1
b7E -3

Sorry for being slow. I send the forms to [redacted] this afternoon. I'm attaching them here too

From: [redacted] (OGC) (FBI)
Sent: Tuesday, January 24, 2017 3:52 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: OGE-450

b6 -1
b7C -1

Good afternoon Mr. Richman,

I apologize for bothering you about this, but SESU is asking if you filed your financial disclosure form (OGE-450) for FY16. They need to notify OIC. If you could confirm the status of your OGE-450, I would

FBI 18-CV-1833-7529

greatly appreciate it.

Thank you very much,

[REDACTED]

Management and Program Analyst

Office of the General Counsel

Federal Bureau of Investigation

Office: [REDACTED]

Cell: [REDACTED]

b6 -1
b7C -1
b7E -3

Confidentiality Statement:

This message is transmitted to you by the Office of the General Counsel of the Federal Bureau of Investigation. The message, along with any attachments, may be confidential and legally privileged. If you are not the intended recipient of this message, please destroy it promptly without further retention or dissemination (unless otherwise required by law). Please notify the sender of the error by a separate e-mail or by calling [REDACTED]

b7E -3

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)

Sent: Wednesday, January 25, 2017 6:53 PM

To: [REDACTED] (DO) (OGA); Cofield, Valerie M. (DO) (FBI)

Subject: GD policy environment

b6 -1
b7C -1

hi - please let me know when Sen Session's GD greeting card to Silicon Valley sparks responses from that world beyond how the internet will break

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Wednesday, January 25, 2017 10:28 AM
To: [REDACTED] (DO) (FBI)
Subject: Re: OGE 450

b6 -1
b7C -1

With help from the D, I've forced [REDACTED] to be my supervisor :) _____

From: [REDACTED] (DO) (FBI)
Sent: Wednesday, January 25, 2017 8:11 AM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: OGE 450

b6 -1
b7C -1

This is great. Thanks. Who do you work for/with now? I will get them to sign your form for me.

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

From: Richman, Daniel C. (DO) (OGA)
Sent: Tuesday, January 24, 2017 2:44 PM
To: [REDACTED] (DO) (FBI) [REDACTED]
Subject: Re: OGE 450

b6 -1
b7C -1
b7E -3

Hi again -- With apologies for my lateness, I'm attaching my OGE 450 form here as well as a separate file with my signature.

Please let me know if this is ok

thx

dan richman

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Thursday, January 26, 2017 4:29 PM
To: [REDACTED] (OGC) (FBI); [REDACTED] (DO) (FBI)
Subject: OGE 450 Addendum

b6 -1
b7C -1

Dear [REDACTED], Having just send you my OGE 450, I wanted to flag an arrangement that I didn't put in but maybe should have. At the end of last year (2016), a former AUSA friend asked me to consult for him on some motion papers in a federal criminal prosecution in the SDNY. I think the Bu may have had an investigative role, as its a corruption prosecution. I did no work on the case last year, so initially thought that disclosure comes in the next form. (I also took comfort in the guidance I got from OGC on [REDACTED])

b5 -1,2
b6 -1,4
b7C -1,4

I just want to make sure that was the right analysis. I'll be doing no fact work and do not intend to have my name on the motion papers. My only work will be help frame arguments some issues of federal criminal law.

should I do anything more on this?

thx

dan richman

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Thursday, January 26, 2017 4:31 PM
To: [REDACTED] (DO) (OGA)
Subject: Fw: OGE 450 Addendum

b6 -1
b7C -1

just keeping my boss apprised of my ethics inquiries

From: Richman, Daniel C. (DO) (OGA)
Sent: Thursday, January 26, 2017 4:29 PM
To: [REDACTED] (OGC) (FBI); [REDACTED] (DO) (FBI)
Subject: OGE 450 Addendum

b6 -1
b7C -1

Dear [REDACTED] Having just send you my OGE 450, I wanted to flag an arrangement that I didn't put in but maybe should have. At the end of last year (2016), a former AUSA friend asked me to consult for him on some motion papers in a federal criminal prosecution in the SDNY. I think the Bu may have had an investigative role, as its a corruption prosecution. I did no work on the case last year, so initially thought that disclosure comes in the next form. (I also took comfort in the guidance I got from OGC on [REDACTED])

b5 -1,2
b6 -1,4
b7C -1,4

I just want to make sure that was the right analysis. I'll be doing no fact work and do not intend to have my name on the motion papers. My only work will be help frame arguments some issues of federal criminal law.

should I do anything more on this?
thx
dan richman

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Thursday, January 26, 2017 4:22 PM
To: Cofield, Valerie M. (DO) (FBI); Littlehale, Richard; [REDACTED]
Subject: pew report on encryption attitudes
Attachments: Americans-and-Cyber-Security-final (1).pdf

b6 -2
b7C -2

Dear Val, Rich and Kenn -- in case you missed it, attached is the Pew report on attitudes re cyber. PP.
27-28 is on encryption
dan r

FOR RELEASE JANUARY 26, 2017

Americans and Cybersecurity

Many Americans do not trust modern institutions to protect their personal data – even as they frequently neglect cybersecurity best practices in their own personal lives

BY Kenneth Olmstead and Aaron Smith

FOR MEDIA OR OTHER INQUIRIES:

Lee Rainie, Director, Internet, Science and Technology Research

Aaron Smith, Associate Director, Research

Dana Page, Senior Communications Manager

202.419.4372

www.pewresearch.org

RECOMMENDED CITATION: Pew Research Center, January, 2017, "Americans and Cybersecurity"

About Pew Research Center

Pew Research Center is a nonpartisan fact tank that informs the public about the issues, attitudes and trends shaping America and the world. It does not take policy positions. The Center conducts public opinion polling, demographic research, content analysis and other data-driven social science research. It studies U.S. politics and policy; journalism and media; internet, science and technology; religion and public life; Hispanic trends; global attitudes and trends; and U.S. social and demographic trends. All of the Center's reports are available at www.pewresearch.org. Pew Research Center is a subsidiary of The Pew Charitable Trusts, its primary funder.

© Pew Research Center 2017

Americans and Cybersecurity

Many Americans do not trust modern institutions to protect their personal data – even as they frequently neglect cybersecurity best practices in their own personal lives

Cyberattacks and data breaches are facts of life for government agencies, businesses and individuals alike in today's digitized and networked world. Just a few of the most high-profile breaches in 2016 alone include the hacking and subsequent ~~release of emails~~ from members of the Democratic National Committee; the release of testing records of ~~dozens of athletes~~ conducted by the World Anti-Doping Agency; and the ~~announcement by Yahoo~~ that hackers had accessed the private information associated with roughly 1 billion email accounts. Finally, in late 2016 and early 2017 U.S. intelligence agencies (the FBI, CIA and Department of Homeland Security) both issued statements and ~~testified before Congress~~ that the Russian government was involved in the hack of the DNC with the aim of influencing the 2016 presidential election.

Previous Pew Research Center studies of the digital privacy environment have found that many Americans fear they have ~~lost control~~ of their personal information and ~~worry~~ whether government agencies and major corporations can protect the customer data they collect. As part of this ~~ongoing series of studies~~ on the state of online privacy and security, the Center conducted a national survey of 1,040 adults in the spring of 2016 to examine their cybersecurity habits and attitudes. This survey finds that a majority of Americans have directly experienced some form of data theft or fraud, that a sizeable share of the public thinks that their personal data have become less secure in recent years, and that many lack confidence in various institutions to keep their personal data safe from misuse. In addition, many Americans are failing to follow digital security best practices in their own personal lives, and a substantial majority expects that major cyberattacks will be a fact of life in the future. Among the key findings:

A majority of Americans (64%) have personally experienced a major data breach, and relatively large shares of the public lack trust in key institutions – especially the federal government and social media sites – to protect their personal information

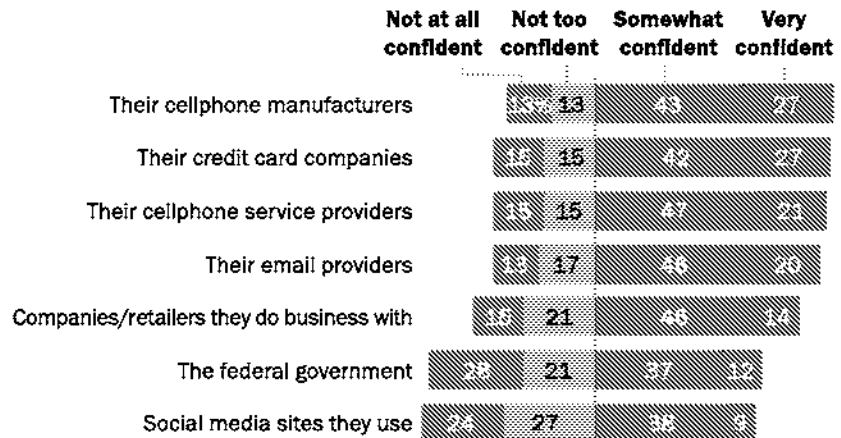
Data security is a personal issue for many Americans: The survey finds that a majority of the public has noticed or been notified of a major data breach impacting their sensitive accounts or personal data. The survey examined several different types of data theft and found that 64% of U.S. adults have been impacted by at least one of them:

- 41% of Americans have encountered fraudulent charges on their credit cards.

- 35% have received notices that some type of sensitive information (like an account number) had been compromised.
- 16% say that someone has taken over their email accounts, and 13% say someone has taken over one of their social media accounts.
- 15% have received notices that their Social Security number had been compromised.
- 14% say that someone has attempted to take out loans or lines of credit in their name.
- 6% say that someone has impersonated them in order to file fraudulent tax returns.

Roughly half of Americans do not trust the federal government or social media sites to protect their data

% of U.S. adults/tech users (see note below) who are in the ability of the following institutions to protect their data



Notes: Data on cellphone manufacturers and service providers based on cellphone owners; data on email providers based on internet users; data on social media sites based on social media users. Data for credit card companies reworded to exclude "ones not apply" responses. Otherwise, refusals and "does not apply" responses not included in this chart. Source: Survey conducted March 30-May 5, 2015.

"Americans and Cybersecurity"

PEW RESEARCH CENTER

And beyond these specific experiences, roughly half of Americans (49%) feel that their personal information is less secure than it was five years ago. Around one-in-five (18%) feel that their information has gotten more secure in recent years, while 31% feel that their information is about as safe as it was five years ago. Americans age 50 and older are especially likely to feel that their personal information has become less safe in recent years: 58% of Americans in this age group express this opinion, compared with 41% of those ages 18 to 49.

In addition, many Americans lack faith in various public and private institutions to protect their personal information from bad actors. They express some level of concern about a variety of entities, ranging from telecommunications firms to credit card companies. But their fears are especially pronounced for two institutions in particular: the federal government and social media platforms. Some 28% of Americans are *not confident at all* that the federal government can keep their personal information safe and secure from unauthorized users, while 24% of social media users lack any confidence in these sites to protect their data. By contrast, just 12% of Americans

(and 9% of social media users) have a very high level of confidence that these entities can keep their personal information safe and secure.

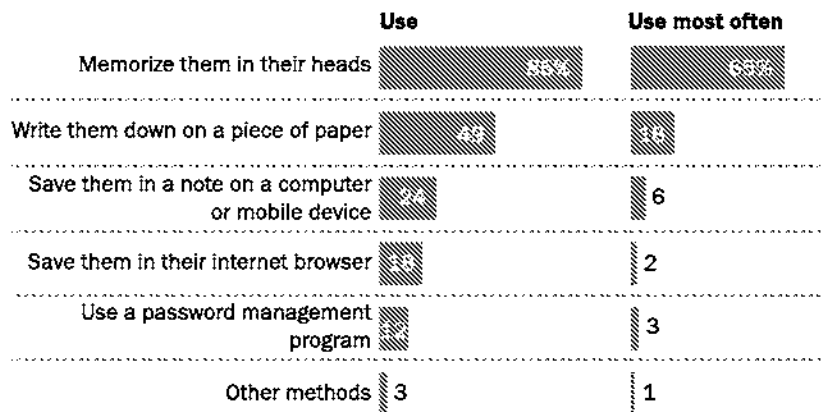
Many Americans fail to follow cybersecurity best practices in their own digital lives

At the same time that they express skepticism about whether the businesses and institutions they interact with can adequately protect their personal information, a substantial share of the public admits that they do not always incorporate cybersecurity best practices into their own digital lives.

This lack of adherence to best practices begins with the ways that Americans keep track of the passwords to their online accounts. Cybersecurity experts generally recommend password management software as the safest and most secure way to track and maintain online passwords.

Most Americans keep track of their online passwords by either memorizing them or writing them down

% internet users who keep track of their online passwords in the following ways



Notes: Results for "use most often" category include those who use only one technique to manage their passwords.

Source: Survey conducted March 30-May 3, 2016.

"Americans and Cybersecurity"

PEW RESEARCH CENTER

Still, just 12% of internet users say that they ever use password management software themselves – and only 3% say that this is the password technique they rely on most. Instead, roughly two-thirds (65%) of internet users say that memorization is the main or only way they keep track of their online passwords – and another 18% rely primarily on writing their passwords down on a piece of paper. In other words, fully 84% of online adults rely primarily on memorization or pen and paper as their main (or only) approach to password management.

A substantial share of Americans are taking steps or following password protection strategies that experts recommend against:

- 41% of online adults have shared the password to one of their online accounts with a friend or family member.
- 39% say that they use the same (or very similar) passwords for many of their online accounts.
- 25% admit that they often use passwords that are less secure than they'd like, because simpler passwords are easier to remember than more complex ones.

The survey also finds that Americans are not always vigilant in the context of mobile security. For instance, 28% of smartphone owners report that they do not use a screen lock or other security features in order to access their phone, while around one-in-ten report that they never install updates to their smartphone's apps or operating system. Meanwhile, 54% of online adults report that they utilize potentially insecure public Wi-Fi networks – with around one-in-five of these users reporting that they use these networks to perform sensitive activities such as e-commerce or online banking.

To be sure, the story of cybersecurity is far from universally negative. For instance, roughly half of online adults (52%) report that they use two-step authentication on at least some of their online accounts. And majorities indicate that they do in fact take recommended steps such as utilizing different passwords from site to site or placing a security feature on their smartphones. But overall, the way that users treat and manage their online passwords and their overall digital security can be described as mixed at best.

Cybersecurity resources

Cybersecurity experts recommend a number of “best practices” and resources for consumers to minimize their exposure to security breaches.

General information on cybersecurity:

[National Cyber Security Alliance
StaySafeOnline.org](https://www.nationalcybersecurityalliance.org/stay-safe-online.org)

[Consumer information on online security
from the Federal Trade Commission](https://www.ftc.gov/consumer/online-security)

[Top-10 safe computing tips from
Information Systems and Technology at
MIT](https://www.mit.edu/~15/6.034/secure-computing/10-top-10-safe-computing-tips)

Password management:

[7 password experts on how to lock down
your online security](https://www.passwordexperts.org/how-to-lock-down-your-online-security)

[PC Magazine: The best password
managers of 2017](https://www.eweek.com/2017/01/10/best-password-managers-2017/)

Using public Wi-Fi:

[How to stay safe on public Wi-Fi](https://www.cisco.com/steve/aaronchase/2016/06/01/how-to-stay-safe-on-public-wi-fi)

If your account has been hacked:

[FBI Internet Crime Complaint Center](https://www.fbi.gov/interior/crime-complaint-center)

Cybersecurity is not a top-of-mind worry for most Americans

Despite their concerns and experiences, most Americans do not express profound worries about cybersecurity in their personal lives or in their expectations for various public institutions.

In the context of their personal lives, fully 69% of online adults say they do not worry about how secure their online passwords are – more than double the share (30%) that admits to having worries about their personal password security. And Americans who have personally experienced a major data breach are generally no more likely than average to take additional means to secure their passwords (such as using password management software).

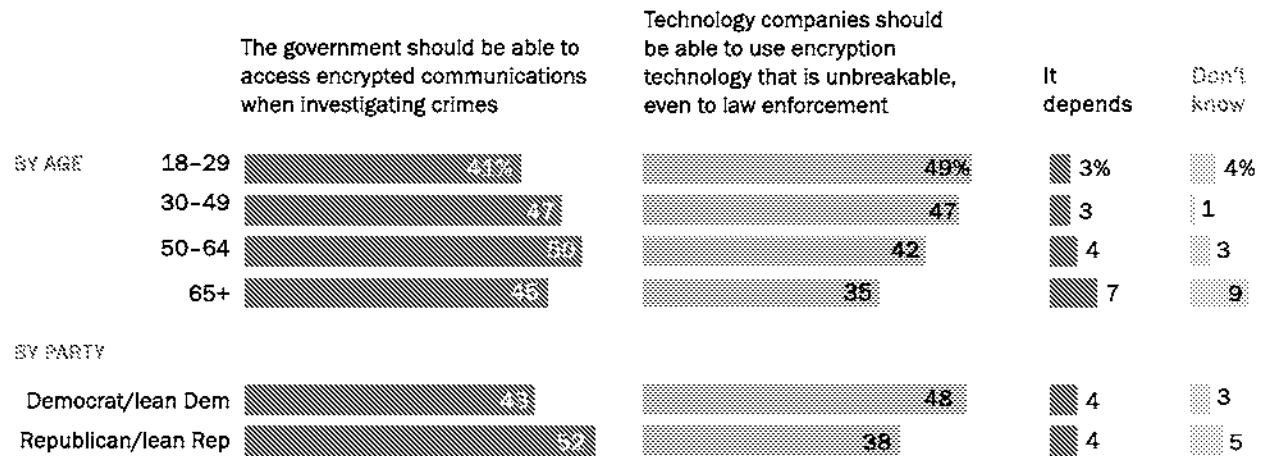
More broadly, a substantial majority of Americans anticipate major cyberattacks in the next five years on our nation's public infrastructure (70% expect that this will happen) or banking and financial systems (66%). Yet a majority of Americans feel that the U.S. government is at least somewhat prepared to handle cyberattacks on our public infrastructure (62%) or government agencies (69%), while 61% have some confidence that U.S. businesses are prepared to handle attacks on their own systems. However, it is worth noting that this survey was fielded prior to the revelations of some more recent, high-profile data breaches, including the hacking of the DNC email system and the breach of email accounts of Yahoo customers.

Americans continue to be highly divided on the issue of encryption

Americans remain divided on the issue of encryption: 46% believe that the government should be able to access encrypted communications when investigating crimes, while 44% believe that technology companies should be able to use encryption tools that are unbreakable even to law enforcement. Democrats and younger adults tend to express greater support for strong encryption, while Republicans tend to express greater support for encryption protocols that can be accessed by law enforcement in the context of criminal investigations.

Younger Americans express elevated support for unbreakable encryption standards

% of U.S. adults who agree with each statement



Source: Survey conducted March 5Q-May 3 2016.
 "Americans and Cybersecurity"

PEW RESEARCH CENTER

1. Americans' experiences with data security

Virtually any digital action that internet users may take – from using credit cards to logging into social media sites – creates data that is stored by companies, governments or other organizations. And when those data are stored, they present opportunities for theft or misuse. This chapter examines the basic contours of the cybersecurity environment for individuals, including: the types of online accounts Americans have, their experiences with various types of data theft, and their overall concerns about the safety and security of their digital information.

The survey illustrates the wide-reaching exposure that many Americans have to the world of cybersecurity. Nearly two-thirds of all Americans (64%) have at least one online account that holds their health, financial or other sensitive personal information. And a similar share (64%) have experienced or been notified of a significant data breach pertaining to their personal data or accounts. More broadly, roughly half the public feels their data have gotten less secure in recent years. Any many Americans express a lack of confidence in various institutions – most notably, the federal government and social media platforms – to safeguard and protect their personal information.

64% of Americans have an online account involving health, financial or other sensitive data

All sorts of online services – from email or social media sites to news or e-commerce platforms – require users to create an account in order to take advantage of them. But some of these services compel users to submit highly personal or sensitive information, such as details of users' financial records or medical history. And these highly sensitive records can be especially damaging if others gain access to them and exploit them. The survey asked about four general categories of these "high value" accounts and found that:

- 55% of Americans report having an online account with banks or other financial service providers.
- 36% have an online account with household utility providers.
- 32% have an online account with their healthcare providers.
- 39% have some other kind of online account that involves bill payments or transactions.

All told, 64% of Americans maintain at least one of the online accounts listed above. College graduates and those with higher household incomes are especially likely to report having all four types of online accounts. For example, half or more of Americans with annual household incomes of \$50,000 or more indicate having an online account with banks or financial institutions (73%), utility providers (55%), healthcare providers (50%) or some other type of institution with which they make online transactions (54%). Meanwhile, 42% of Americans in households earning less

than \$50,000 per year have an online account with banks or financial institutions and only around one-quarter have an account with utility providers (22%), healthcare providers (18%) or other types of service providers (27%).

Similarly, around three-quarters of college graduates (77%) have an online account with financial institutions, while half or more have online accounts with healthcare providers (53%), utility providers (52%) or some other types of service providers (58%).

Nearly two-thirds of Americans have experienced some form of data theft

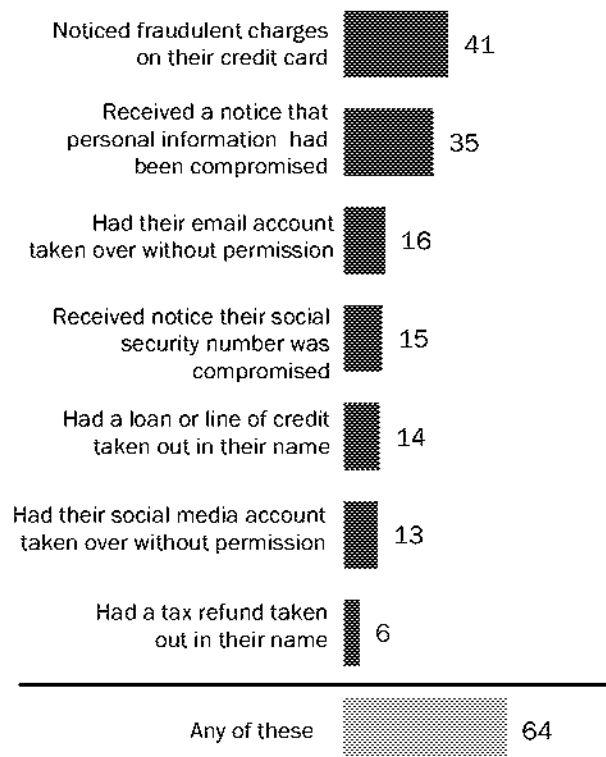
The broader debate over cybersecurity and the safety of Americans' personal data is taking place in an environment where a significant share of the public has personally experienced some type of data theft.

The survey asked about seven different types of identity or data theft that Americans might be exposed to and found that several are particularly widespread. Some 41% of Americans have learned they were the victims of a data breach by seeing fraudulent charges on their credit or debit cards. Around one-third (35%) of Americans have received notices that some sort of sensitive personal information – like an account number – had been compromised, and 15% have received notices that their social security number, specifically, had potentially fallen into the wrong hands.

In other cases, the public experiences data breaches in the context of their major online accounts: 16% of Americans have had someone take over their email accounts without their permission, while 13% say that someone has hacked or taken over one of their social media accounts.

Many Americans have experienced some form of data theft

% of U.S. adults who have ever ...



Sources: Survey conducted March 30-May 3, 2016, "Americans and Cybersecurity"

PEW RESEARCH CENTER

In addition to these breaches, a notable share of Americans have experienced even more severe forms of data theft. Some 14% of Americans report that someone has attempted to open lines of credit or take out loans using their name, while 6% have had someone impersonate them to try and claim tax refunds. All told, nearly two-thirds of Americans (64%) report that they have experienced at least one of these seven types of data theft.

Americans in their early 30s through mid-60s are especially likely to have encountered many of these forms of data theft. Nearly half (48%) of Americans ages 30 to 64 have noticed fraudulent charges on their credit cards, while around one-in-five (19%) have received notices that their social security number was compromised. Overall, nearly three-quarters of Americans in this age range (72%) have experienced at least one of the seven types of breaches (compared with 55% of those ages 18 to 29 and 50% of those 65 and older). Along with Americans in this age range, college graduates (78% of whom have experienced at least one of these breaches) and those with household incomes of \$75,000 or more per year (77%) are also relatively likely to have encountered these various types of data theft.

Many Americans lack trust in key institutions – especially the federal government and social media sites – to protect their personal information

When asked whether they have confidence in various companies and institutions to keep their personal records safe from unauthorized users, Americans' views are decidedly mixed. Some institutions – such as telecommunications firms and credit card companies – inspire relatively broad confidence. In total, around seven-in-ten cellphone owners are very (27%) or somewhat (43%) confident that the companies that manufactured their cellphones can keep their personal information safe; a similar share is very (21%) or somewhat (47%) confident that the companies that provide their cellphone services will protect their information.

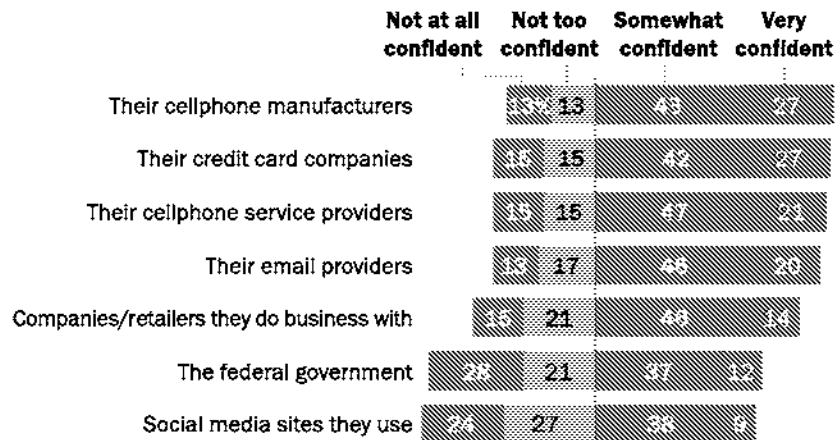
Similarly, around two-thirds of online adults are either very (20%) or somewhat (46%) confident that their email providers will keep their information safe and secure. And roughly six-in-ten Americans are very (23%) or somewhat (36%) confident that their credit card companies can protect their personal information. Other companies and retailers are viewed slightly less confidently: 14% of Americans are very confident (and 46% are somewhat confident) that these entities will keep customers' information safe.

But even as a majority of Americans express at least some confidence in each these institutions, in each instance a notable minority expresses *no confidence at all* in the ability of these entities to protect their personal data.

And some institutions – in particular, the federal government and social media platforms – are viewed with skepticism by a substantial share of the public when it comes to protecting users' personal records. Fully 28% of Americans are *not at all confident* that the federal government can protect their personal information (just 12% are very confident). And 24% of social media users are not at all confident in the ability of these sites to keep their personal information safe – nearly three times the share of social media users (9%) who have a great deal of confidence in these companies.

Roughly half of Americans do not trust the federal government or social media sites to protect their data

% of U.S. adults/tech users (see note below) who are in the ability of the following institutions to protect their data



Note. Data on cellphone manufacturers and service providers based on cellphone owners; data on email providers based on internet users; data on social media sites based on social media users. Data for credit card companies recalculated to exclude "does not apply" responses. Otherwise, refusals and "does not apply" responses not included in this chart. Source: Survey conducted March 30-May 3, 2015. "Americans and Cybersecurity"

PEW RESEARCH CENTER

Overall, there is relatively little variation in Americans' attitudes towards these entities based on their demographic characteristics. However, users who have directly experienced certain types of data theft in their own lives tend to have lower levels of confidence in the institutions that were involved in these experiences – particularly when it comes to digital institutions, such as email and social media. Some 22% of Americans who have had their email accounts accessed without their permission are not at all confident in the ability of their email providers to keep their personal information secure – that is double the share (11%) among those who have not directly experienced an email breach themselves. And 40% of those who have experienced a breach of their social media accounts are not at all confident that these platforms can protect their personal information – again double the share (20%) among those who have not had their social media accounts accessed in this way.

On the other hand, Americans' attitudes towards their credit card companies are less strongly correlated with their past experiences with data theft. Among those who have ever noticed fraudulent charges on their credit cards, 13% say they are not at all confident in the ability of these companies to protect their personal information – identical to the share among those who have not experienced this (13%). In fact, one-in-five Americans who have experienced fraudulent charges on their credit cards (22%) indicate that they are *very confident* in the ability of credit card companies to protect their personal information.

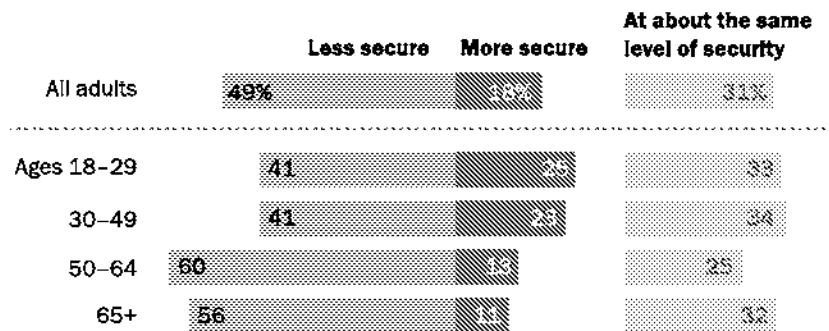
But in the end, relatively few Americans express either blanket confidence or universal concern about the institutions they entrust with their personal information. Just 13% of Americans¹ indicate that they are at least somewhat confident in *all* of these seven institutions, while just 4% indicate that they lack confidence in all of them. The vast majority of Americans fall somewhere in between – they trust some institutions but are skeptical of others.

Roughly half of Americans think their personal data are less secure compared with five years ago

At a broader level, roughly half (49%) of all Americans feel their personal information is less secure than it was five years ago. Around one-third of the public (31%) feels that their data are equally secure now compared with five years ago, while around one-in-five (18%) feel that their data are actually more secure today.

Americans 50 and older express greater concern over personal data security

% of U.S. adults who think their data are compared with five years ago



Source: Survey conducted March 30-May 3, 2016.
"Americans and Cybersecurity"

PEW RESEARCH CENTER

Americans ages 50 and older are especially likely to express concerns that their personal information has become less

protected in recent years: 58% of these older Americans feel that their data are less secure than five years ago, while just 12% feel their data are more secure. Americans under the age of 50 tend to express less concern about this issue by comparison: 24% feel that their data are more secure

¹ These figures are based on respondents who answered questions about all seven institutions.

than five years ago. But even so, a plurality of 18- to 49-year-olds (41%) feel their data are less secure now than in recent years.

Outside of age, Americans' attitudes toward this issue do not vary substantially by gender, racial background, household income or educational attainment. However, those who have themselves experienced some sort of data theft or breach express broader concerns about the overall security of their personal information. Roughly half (52%) of Americans who have experienced at least one of the seven types of data theft measured in this survey feel their data are less secure than five years ago, compared with 40% of those who have not experienced any of these forms of data theft.

In addition to these broader concerns about the security of their personal information, Americans express their worries about digital data theft in more concrete ways. Specifically, 69% of online adults report that they have chosen to not open an online account because they were worried about how their personal information would be handled by the site in question. This behavior is largely consistent across a range of demographic groups, although users who have experienced personal data theft themselves are somewhat more wary about signing up for digital platforms. Fully 73% of those who have experienced at least one form of data theft say they have refrained from opening an online account due to their concerns about how their information would be treated, compared with 61% of those who have not experienced any type of data theft.

2. Password management and mobile security

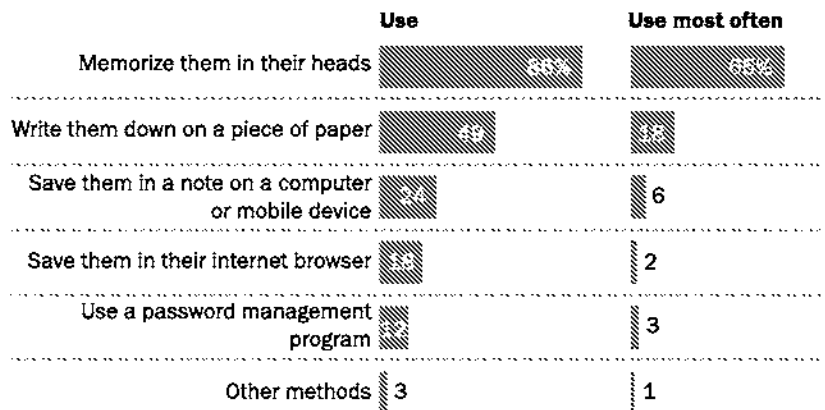
Individuals play a critical role in their own digital security. The weak link in many personal data breaches can be traced back to an overly simple password, an out-of-date smartphone app with missing security patches or the use of an unfamiliar Wi-Fi network. Cybersecurity experts generally recommend a number of steps for users to take in order to reduce their exposure to data theft, such as using a different, complex password for each account; not sharing passwords with others; using some sort of security feature on their smartphones; and always updating their smartphones' apps and operating system to ensure that they have the latest security updates. Although many Americans are utilizing at least some of these steps, this survey finds that less-than-optimum cybersecurity habits are widespread.

Most Americans use memorization or pen and paper as their primary method of keeping track of their online passwords

For average users, creating and storing passwords to their various online accounts is their primary interaction with the world of cybersecurity. Passwords are the first line of defense against unauthorized access to user data, and people's password habits – such as how they manage their passwords, or whether they use passwords that are simple or complex – directly impact their overall security. Many security professionals recommend password management software as the best way to create and store complex passwords. But this survey finds that the vast majority of Americans keep track of their passwords using much more traditional methods – specifically, by memorizing them or by writing them down on a piece of paper.

Most Americans keep track of their online passwords by either memorizing them or writing them down

% internet users who keep track of their online passwords in the following ways



Note: Reasons for "use most often" category include those who use only one technique to manage their passwords.

*Source: Survey conducted March 30-May 3, 2016.
"Americans and Cybersecurity"*

PEW RESEARCH CENTER

When asked about different ways they might keep track of their online passwords, fully 86% of internet users report that they keep track of them in their heads. Indeed, 65% report that memorization is the method they rely on the most (or is the only method they use) to keep track of their passwords. Around half of online adults (49%) say they keep the passwords to at least some of their online accounts written down on a piece of paper – with 18% saying that this is the method they rely on most heavily. In total, just over eight-in-ten online adults (84%) say that they primarily keep track of their passwords by either memorizing them or writing them down.

Other approaches to password management are far less common. Roughly one-quarter (24%) of online adults keep track of their passwords in a digital note or document on one of their devices (6% say this is the approach they rely on most), while 18% say that they save them using the built-in password saving feature available in most modern browsers (with 2% saying they rely on this technique the most). Most experts agree that saving passwords in browsers is OK if the passwords are unique to each site, however they also agree that password management software outside the browser is preferable. Meanwhile, just 12% of online adults say that they ever use password management software to keep track of their passwords – and only 3% rely on this technique as their primary method for storing passwords.

There are relatively few demographic differences when it comes to how internet users keep track of their passwords. Within every major demographic group, a majority says that memorization is the password management technique they rely on the most – and the differences that do exist on this subject tend to be relatively modest. For instance, those under the age of 50 are more likely than those ages 50 and older to primarily memorize their online passwords (72% vs. 55%), while older users are more likely to say they primarily write their passwords down on a piece of paper (27% vs. 13%). But otherwise, users of all ages manage their online passwords using largely similar approaches.

In addition, the approach to managing password that is most recommended by security professionals – password management software – is used relatively rarely across a wide range of demographic groups. College graduates tend to rely more heavily on these programs than most, but even among this “high usage” group, only 17% use these programs at all – and just 7% indicate that they use them as the sole or primary method for managing their passwords.

Interestingly, users’ personal experiences with data theft are not highly correlated with the steps they take to manage and track their online passwords. Among those who have experienced some type of personal data theft or breach, nearly two-thirds (63%) say that they primarily keep track of their passwords in their head. And although 15% of these users indicate that they use password

management software for some of their passwords, just 4% say this is the technique they rely on the most.

52% of online adults have used two-factor authentication on their online accounts – but a substantial minority use similar passwords across many sites or share passwords with others

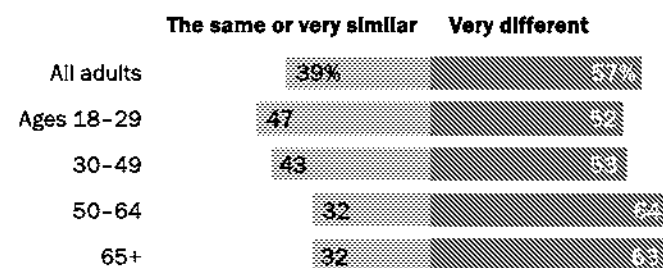
Beyond using password management software, cybersecurity experts recommend a number of other “best practices” to users. These include not using the same passwords across multiple accounts, as well as refraining from sharing passwords with others. When asked about their own behaviors in this regard, a majority of online adults (57%) report that they vary their passwords across their online accounts. However, a substantial minority (39%) indicate that most of their passwords are the same or very similar to one another. In addition, a sizeable minority of online adults (41%) have shared the password to one of their online accounts with friends or family members.

Those under the age of 50 are especially likely to indicate that their online passwords are very similar to one another:

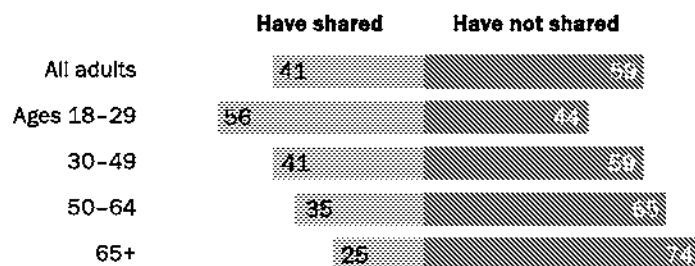
45% of internet users ages 18 to 49 say this, compared with 32% of those ages 50 and older. And

Most online adults say they vary their passwords across sites

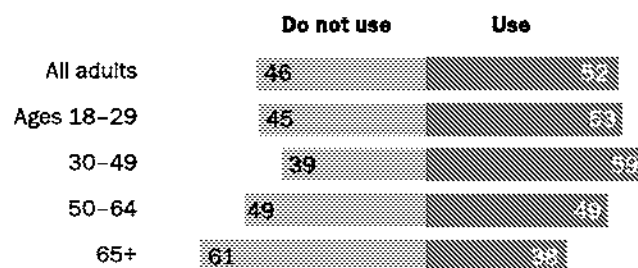
% of internet users who say the passwords they use on their accounts are ...



% of internet users who say they passwords with friends or family



% of internet users who say they two-factor authentication



Source: Survey conducted March 30-April 3 2016.
“Attitudes and Cybersecurity”

PEW RESEARCH CENTER

younger adults are especially likely to share their passwords with others: 56% of 18- to 29-year-old internet users have done so.

Many sites rely on individuals to choose strong passwords as the first line of defense for their online accounts, but there are other technologies that aim to improve – or in some cases replace – the password itself. The first of these techniques is known as “multifactor” or “two-factor” authentication. The “factors” are typically something the user *knows* (such as a password) plus something the user *possesses* (like a code sent to their smartphone). Nearly half of internet users (52%) say that they use this type of multifactor authentication on at least one of their online accounts.

The second of these techniques involves using one’s credentials from another site – often a social media platform such as Facebook – to log in to a third party site. Some 39% of social media users say they have logged into another website using the credentials from their social media accounts. Among social media users ages 18 to 29, more than half (56%) have done so.

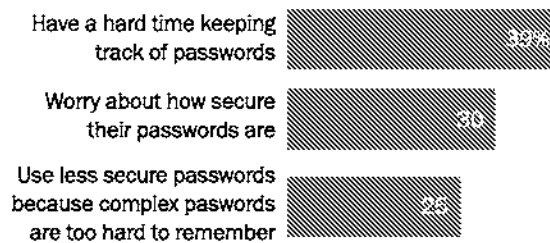
A substantial minority of online Americans find password management to be a challenge and source of worry

For a relatively substantial minority of online Americans, password management can be a stressful and uncertain process. The survey asked several questions about people's attitudes and concerns about passwords and found that 30% of online adults worry about the overall security of their online passwords, while 25% sometimes use passwords that are less secure than they'd like because remembering more complex passwords is too difficult. For the most part, these behaviors are relatively consistent across different demographic groups.

In addition, 39% of internet users report that they simply find it challenging to keep up with all of the passwords to their various online accounts. This is relatively common among those in their early 30s through mid-60s: 44% of online adults ages 30 to 64 say they have a hard time keeping track of their passwords, compared with 33% of those ages 18 to 29 and 30% of those 65 and older.

A substantial minority of online adults express password concerns

% of internet users who say they ever ...



*Source: Survey conducted March 30-May 3, 2015.
"Americans and Cybersecurity"*

PEW RESEARCH CENTER

This 39% of the online population that has a hard time keeping track of passwords also expresses concerns about password management in other concrete ways. Compared with the 60% of online adults who do not express difficulties keeping up with their passwords, this "password challenged" group is more likely to ...

- Use the same or similar passwords across many different sites (45% vs. 36%)
- Worry about the security of their passwords (44% vs. 22%)
- Use simple passwords rather than complex ones (41% vs. 14%)

These "password challenged" individuals are also more likely to keep track of their passwords by writing them down on a piece of paper (56% vs. 44%), saving them in a digital note (31% vs. 20%), or by saving them in their internet browser (25% vs. 13%).

More than one-quarter of smartphone owners do not use a screen lock, and many fail to regularly update the apps or operating system on their phones

As smartphones have become increasingly prevalent – and as users engage in a wide range of sensitive behaviors on their phones – these devices have become the latest front in the battle over digital security. In general, smartphones can be compromised in two ways. The first is by gaining possession of the physical phone itself, and security experts recommend the use of a screen lock feature to prevent someone from accessing the contents of a smartphone that falls into the wrong hands. When smartphone owners were asked if they use some form of screen lock on their phones, around one-quarter (28%) reported that they do not.

Those smartphone owners who do utilize a screen lock take a wide range of approaches, with numeric PIN codes (used by 25% of smartphone owners) and thumbprint scanners (23%) being the most common. A smaller share uses passwords containing letters, numbers, or symbols (9%), or a connecting pattern of dots (9%).²

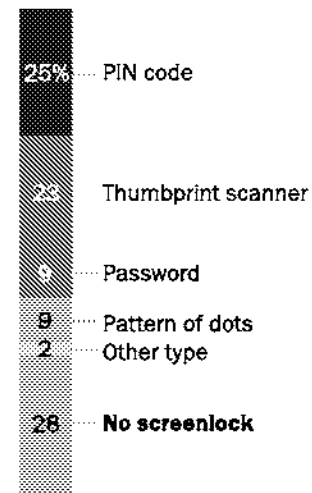
An especially large share of smartphone owners ages 65 and older (39%) say their devices do not have a lock screen, but it is not uncommon for younger smartphone owners to skip this security step either. Some 28% of smartphone owners ages 18 to 29, 24% of those ages 30 to 49, and 30% of those ages 50 to 64 indicate that their phones do not have any type of screen lock.

Those with lower levels of educational attainment are also relatively likely to forego using a screen lock on their smartphones. Some 80% of smartphone owners with college degrees indicate that they use a screen lock on their phones, but that share falls to 66% among those who have high school diplomas or less.

A second way that smartphones can be compromised is through software security flaws – either those that exist in the apps on users' phones or in the smartphone operating system itself. To

28% of smartphone owners have no lock screen on their phones

% of smartphone owners who say they access their phones using a ...



Source: Survey conducted March 20-May 3 2016.

"Americans and Cybersecurity"

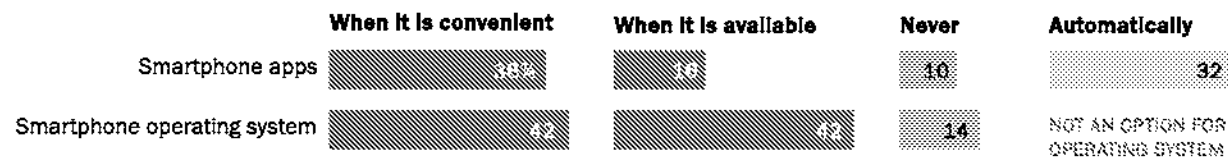
PEW RESEARCH CENTER

prevent this, security experts encourage users to regularly and promptly install updates for their apps and operating system, since these updates often contain important security patches.

But these survey findings indicate that many smartphone owners are slow to update their phones and the apps that come with them – and that in some cases, users are skipping these steps entirely. When it comes to the apps on their mobile devices, around half of smartphone owners indicate that they set them to update automatically (32%) or that they update them manually as soon as a new version is available (16%). However, a comparable share reports that they only update their apps when it happens to be convenient for them (38%) or that they never update the apps on their phones (10%).

Many smartphone owners do not immediately update the apps and operating system on their phones

% of smartphone owners who say they update the apps/operating system on their phone ...



Source: Survey conducted March 30-May 5, 2016.
 "Americans and Cybersecurity"

PEW RESEARCH CENTER

Smartphone owners are similarly divided when it comes to updating the actual operating system on their devices. Some 42% of smartphone owners say that they typically update their operating system as soon as a new version is available, but more than half say that they only update their operating system when it is convenient (42%) or that they never update their phones (14%).

As was the case with screen locks, older smartphone owners tend to update their phones much less consistently than younger users. Some 21% of smartphone owners ages 65 and older say they never update their smartphone apps, while 23% say they never update their operating system. By contrast, just 6% of 18- to 29-year-old smartphone owners never update their apps – indeed, 48% of younger users say they set them to update automatically as they are available – and 13% of these younger users never update their operating system.

Anti-virus software is commonplace on desktop and laptop computers, and the same type of software can be installed on smartphones: 32% of smartphone owners report installing some sort of anti-virus software on their devices.

Just over half of internet users utilize public Wi-Fi networks, including for tasks like online banking or e-commerce

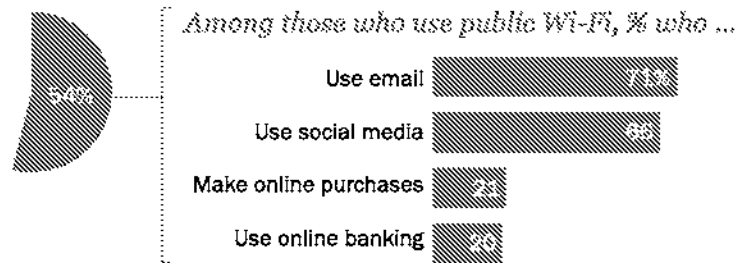
Along with users' passwords and the physical devices they carry, the networks their devices are connected to offer an additional avenue for potential cyberattacks. Public Wi-Fi networks (such as those in cafes, libraries or other public spaces) are an especially common target for hackers. The mechanics behind these attacks vary,³ and not all public networks are inherently insecure. But in general, security experts

recommend that users refrain from performing sensitive activities (such as banking or financial transactions) on public or otherwise unfamiliar Wi-Fi networks.

When asked about their use of public Wi-Fi networks, just over half of internet users (54%) report that they do access Wi-Fi networks in public places. Younger adults are especially likely to do this: 69% of internet users ages 18 to 29 use public Wi-Fi, compared with 54% of those ages 30 to 49, 51% of those ages 50 to 64 and 33% of those 65 and older.

54% of online adults utilize public Wi-Fi networks

54% of internet users use public Wi-Fi



Source: Survey conducted March 30-May 3 2016.
"Americans and Cybersecurity"

PEW RESEARCH CENTER

And when asked about some online activities they might engage in while connected to public Wi-Fi networks, most of these users indicate that they have gone online to access their social media accounts (66% of public Wi-Fi users have done this) or to check email (71%). However, around one-in-five of these users have used public Wi-Fi for more sensitive transactions such as online shopping (21%) or banking or other financial transactions (20%).

³ One approach involves hackers reading all of the information being transmitted on an unsecured Wi-Fi network. In a second approach, hackers can create malicious Wi-Fi networks that appear legitimate to unsuspecting users.

3. Attitudes about cybersecurity policy

Cybersecurity does not just impact Americans at an individual level: These issues have potentially profound implications for the U.S. government, law enforcement agencies and the companies and other entities that maintain the nation's infrastructure. On this front, Americans' views and perceptions of the national cybersecurity environment are complex and multifaceted. Although their knowledge of some major cyberattacks that have occurred in recent years is somewhat limited, there is a general public consensus that the coming years will likely see significant attacks on our public infrastructure and financial systems. And the public remains highly divided over the best way to approach issues such as encrypted communications in the context of law enforcement investigations.

A majority of Americans expect significant cyberattacks in the next five years

Many Americans expect that the coming five years will see significant cyberattacks on the country's public infrastructure and financial systems. Fully 70% of Americans expect that the United States will definitely (18%) or probably (51%) experience a significant cyberattack on its public infrastructure (such as air traffic control systems or power grids).

A similar share expects that a significant cyberattack on the country's banking and financial systems will definitely (18%) or probably (48%) happen over the same time frame. Only a small fraction of Americans think that major cyberattacks on our public infrastructure (3%) or financial systems (4%) will *definitely not* occur in the next five years.

Men are somewhat more likely than women to think that there will definitely be major cyberattacks on both our public infrastructure (22% vs. 15%) and financial systems (23% vs. 14%) in the next five years, but otherwise Americans' views on this subject do not differ substantially across demographic groups.

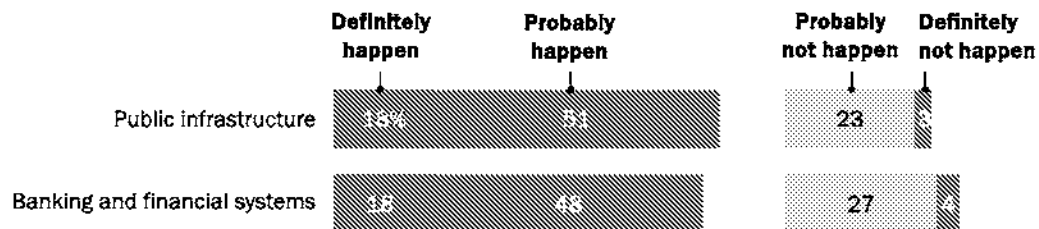
Although a majority of Americans think that significant cyberattacks on our public infrastructure and financial systems are likely in the next five years, they express mixed opinions about the extent to which the government and private industries are prepared to face these attacks.

When it comes to the U.S. government's preparedness to handle these attacks, around six-in-ten Americans feel that the government is very (13%) or somewhat (49%) prepared to prevent a cyberattack on our public infrastructure; a similar share feels that the government is very (18%) or somewhat (51%) prepared to prevent a cyberattack on U.S. government agencies themselves. At the same time, around one-in-ten Americans feel that the government is *not at all prepared* to handle a major cyberattack on public infrastructure (14%) or on government agencies (11%).

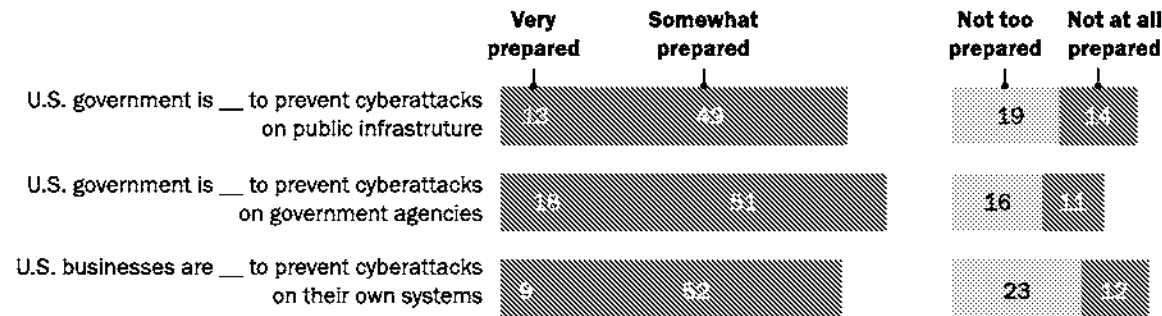
When it comes to their feelings about private industry, roughly six-in-ten Americans feel that U.S. businesses themselves are very (9%) or somewhat (52%) prepared to prevent cyberattacks on their own systems. But 12% think that the private sector is not at all prepared to prevent cyberattacks on their own systems.

Majority of Americans think major cyberattacks will happen in the next five years

% of U.S. adults who think a cyberattack on the following institutions will in the next five years



% of U.S. adults who think the following institutions are to prevent cyberattacks



Source: Survey conducted March 30-May 3, 2016.
 "Americans and Cybersecurity"

PEW RESEARCH CENTER

Americans' perceptions of how prepared the government and private sector are to defend against cyberattacks are largely consistent across demographic groups. However, those under the age of 50 are somewhat more optimistic than older Americans about the ability of these institutions to withstand future attacks. Those ages 18 to 49 are more likely than older Americans to say that the U.S. government is very prepared to handle cyberattacks on public infrastructure (17% vs. 9%) or

government agencies (24% vs. 12%), and they are also slightly more likely to say that U.S. businesses are very prepared to handle attacks on their own systems (11% vs. 7%).

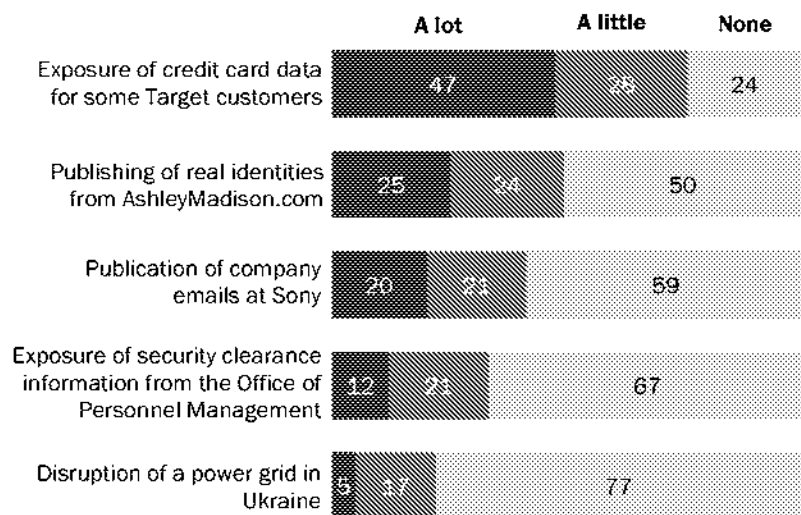
Americans show widespread awareness of 2011 Target credit card breach, less awareness of some other major cyberattacks

Americans' awareness of a number of high-profile cyberattacks that have occurred in the United States and abroad in recent years is decidedly mixed. The survey asked about five specific attacks and found that Americans are most aware of the breach of credit card data of Target store customers that occurred in 2011 (note: this survey was fielded prior to some more recent high-profile data breaches, including the hacking of the DNC email system and the breach of email accounts of Yahoo customers). A sizeable majority of Americans (75%) have heard at least something about the Target breach, and nearly half the public (47%) has heard a lot about it.

Americans are less familiar with two other recent cyberattacks involving private corporations. Around half the public (49%) has heard at least something about the 2015 data breach of the AshleyMadison.com website, with 25% indicating that they have heard a lot about this. And 40% of Americans have some awareness of the 2014 cyberattack on the Sony Corp. that exposed millions of internal corporate emails and documents and damaged the company's internal networks (with 20% indicating that they have heard a lot about it).

Half of Americans have heard "a lot" about the Target hack, less on other high-profile cyberattacks

% Americans who have heard about each of these events



Source: Survey conducted March 30-May 3 2015.
"Americans and Cybersecurity"

PEW RESEARCH CENTER

The public has much lower awareness of two other attacks that were arguably larger and more dangerous than those discussed above: the 2015 attack on the records of the U.S. government Office of Personnel Management (OPM) and another 2015 attack in which hackers took down a power grid in Ukraine by attacking the grid's computer systems. One-third (33%) of Americans are aware of the OPM attack (with only 12% having heard a lot about it), while around one-in-five (22%) have heard of the Ukraine attack (with just 5% having heard a lot about it). Roughly two-thirds of Americans have not heard anything about the OPM hack, and around three-quarters have no awareness of the Ukraine attack.

Americans remain divided over whether government should be able to access encrypted communications

The issue of encryption – specifically, whether or not the government should legally be able to bypass or decode encrypted communications when investigating criminal cases – has long been a hot-button topic in the ongoing debate over the appropriate balance between individual privacy concerns and the needs of law enforcement in the digital age. This issue again became front page news in 2016, when the FBI obtained a court order to compel Apple to unlock the iPhone of one of the perpetrators of the mass shooting in San Bernadino, California.

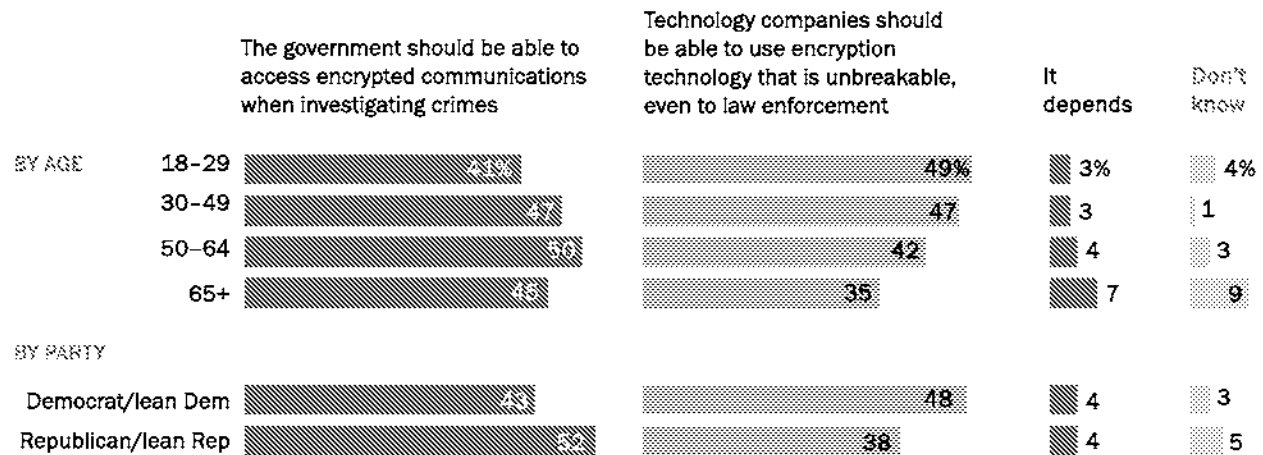
In a Pew Research Center survey conducted at that time, 51% of Americans felt that Apple should be required to unlock the iPhone at the FBI's request, while 38% felt that Apple should not be required to do this.

This survey posed a more general question (with two competing statements) about the tradeoffs between security and privacy, and it finds that Americans' views on this subject remain divided. Fully 46% of Americans agree with the statement: "The government should be able to access encrypted communications when investigating crimes." On the other hand, a comparable share (44%) agrees that "technology companies should be able to use encryption technology that is unbreakable, even to law enforcement." An additional 4% of Americans volunteer that their answer to this question depends on the circumstances.

Men are more likely than women (by a 49% to 39% margin) to say that technology companies should be able to use unbreakable encryption. Conversely, women (51%) are somewhat more likely than men (40%) to support the government's right to access encrypted information when investigating a crime. And although Americans of all ages are somewhat split on this issue, younger adults are more inclined to believe that encryption technologies should be unbreakable even to the government. Roughly half of 18- to 29-year-olds (49%) feel that technology companies should be able to use encryption that is unbreakable to law enforcement, but that figure falls to 35% among Americans 65 and older.

Younger Americans express more support for encryption than older adults

% of Americans who agree with each statement



Source: Survey conducted March 30-May 3, 2015.
 "Americans and Cybersecurity"

PEW RESEARCH CENTER

There is also a partisan element to these views. Democrats (including independents who lean towards the Democratic party) tend to support the notion that technology companies should be able to use encryption protocols that are unbreakable to law enforcement, although by a fairly close margin (48% vs. 43% who say the government should be able to bypass encryption). Meanwhile, Republicans tend to feel more strongly that the government should be able to access encrypted messages when investigating crimes (by a 53% to 38% margin).

Acknowledgments

This report was made possible by The Pew Charitable Trusts. It is a collaborative effort based on the input and analysis of the following individuals:

Primary researchers

Kenneth Olmstead, *Research Associate*

Aaron Smith, *Associate Director, Research*

Research team

Lee Rainie, *Director, Internet, Science and Technology Research*

Maeve Duggan, *Research Associate*

Monica Anderson, *Research Associate*

Andrew Perrin, *Research Assistant*

Editorial and graphic design

Margaret Porteus, *Information Graphics Designer*

Shannon Greenwood, *Copy editor*

Communications and web publishing

Dana Page, *Senior Communications Manager*

Shannon Greenwood, *Associate Digital Producer*

Travis Mitchell, *Digital Producer*

Methodology

The analysis in this report is based on a Pew Research Center survey conducted from March 30 to May 3, 2016, among a national sample of 1,040 adults, 18 years of age or older, living in all 50 U.S. states and the District of Columbia. Fully 262 respondents were interviewed on landline telephones, and 778 were interviewed on cellphones, including 477 who had no landline telephone. The survey was conducted by interviewers at Princeton Data Source under the direction of Princeton Survey Research Associates International. A combination of landline and cellphone random-digit-dial samples was used; both samples were provided by Survey Sampling International. Interviews were conducted in English and Spanish. Respondents in the landline sample were selected by randomly asking for the youngest adult male or female who was at home. For detailed information about our survey methodology, visit:

<http://www.pewresearch.org/methodology/u-s-survey-research/>

The combined landline and cellphone samples are weighted using an iterative technique that matches gender, age, education, race, Hispanic origin and nativity, and region to parameters from the 2013 Census Bureau's American Community Survey and population density to parameters from the Decennial Census. The sample also is weighted to match current patterns of telephone status (landline only, cellphone only or both landline and cellphone), based on extrapolations from the 2014 National Health Interview Survey. The weighting procedure also accounts for the fact that respondents with both landline phones and cellphones have a greater probability of being included in the combined sample and adjusts for household size among respondents with landline phones. The margins of error reported and statistical tests of significance are adjusted to account for the survey's design effect, a measure of how much efficiency is lost from the weighting procedures.

The margin of sampling error for the complete set of weighted data is ± 3.4 percentage points. Results based on the 926 internet users⁴ have a margin of sampling error of ± 3.6 percentage points.

The following table shows the unweighted sample sizes and the error attributable to sampling that would be expected at the 95% level of confidence for different groups in the survey:

⁴ Internet user is defined as those who access the internet or email at least occasionally, or those who access the internet on cellphones, tablets, or other mobile handheld devices at least occasionally.

Group	Unweighted sample size	Plus or minus ...
All adults 18+	1,040	3.4
Men	509	4.9
Women	531	4.8
18-29	170	8.4
30-49	283	6.5
50-64	325	6.1
65+	234	7.3
High school or less	303	6.3
Some college	265	6.7
Bachelor's degree or more	462	5.1

Sample sizes and sampling errors for other subgroups are available upon request.

In addition to sampling error, one should bear in mind that question wording and practical difficulties in conducting surveys can introduce error or bias into the findings of opinion polls. Pew Research Center undertakes all polling activity, including calls to mobile telephone numbers, in compliance with the Telephone Consumer Protection Act and other applicable laws.

Pew Research Center is a nonprofit, tax-exempt 501(c)(3) organization and a subsidiary of The Pew Charitable Trusts, its primary funder.

Topline questionnaire

EMINUSE Do you use the internet or email, at least occasionally?

INTMOB Do you access the internet on a cell phone, tablet or other mobile handheld device, at least occasionally?

	USES INTERNET	DOES NOT USE INTERNET
May 2016	87	13
April 2016	87	13
November 2015	87	13
July 2015	87	13
April 2015	85	15
September 2013	86	14

INTFREQ About how often do you use the internet? [READ]

Based on all internet users [N=926]

	MAY 2016		APRIL 2016	JULY 2015
%	25	Almost constantly	28	24
	50	Several times a day	49	49
	11	About once a day	10	11
	7	Several times a week, OR	7	7
	6	Less often?	6	8
	*	(VOL.) Don't know	*	*
	*	(VOL.) Refused	*	1

DEVICE1a Next, do you have a cell phone, or not?

	YES	NO	(VOL.) DON'T KNOW	(VOL.) REFUSED
May 2016	92	8	0	0
April 2016	92	8	0	0
November 2015	91	9	0	0
July 2015	92	8	*	*
April 2015	92	8	*	0

SMART1 Some cell phones are called "smartphones" because of certain features they have. Is your cell phone a smartphone such as an iPhone, Android, Blackberry or Windows phone, or are you not sure?

Based on cell phone owners

	YES, SMARTPHONE	NO, NOT A SMARTPHONE	NOT SURE/ DON'T KNOW	(VOL.) REFUSED
May 2016 [N=992]	76	17	7	0
April 2016 [N=1,535]	78	16	6	*
November 2015 [N=2,606]	76	17	7	*
July 2015 [N=1,903]	73	20	7	*
April 2015 [N=1,900]	73	21	5	*
September 2013 [N=5,763]	61	32	7	*
August 2013 [N=1,636]	60	33	6	*

SNSINT2 Do you ever use a social media site or app like Facebook, Twitter or LinkedIn?

Based on all internet users [N=926]

	YES	NO	(VOL.) DON'T KNOW	(VOL.) REFUSED
May 2016	74	26	0	*
November 2015	74	26	*	*
July 2015	76	23	*	0
September 2013	74	26	*	0
May 2013	72	28	0	*
December 2012	67	33	*	*
August 2012	69	31	0	*
February 2012	66	34	*	0

ACCT1 Do you have [INSERT ITEMS; RANDOMIZE; 'ANY OTHER ONLINE ACCOUNT' ALWAYS LAST], or not?

Based on all internet users [N=926]

	YES	NO	(VOL.) DOESN'T APPLY / DON'T HAVE THIS ACCT.	(VOL.) DK	(VOL.) REF.
a. Any ONLINE accounts with your bank or financial services provider	64	35	*	1	1
b. Any ONLINE accounts with your health care provider	37	61	*	2	*
c. Any ONLINE accounts with a household utility provider, such as your gas, water, or electric company	41	57	1	1	*
d. Any other online account that involves bill payments or transactions	45	54	0	1	*

ACCT2 Have you ever chosen to NOT use or NOT create an account with an online service because you were worried about how your personal information would be handled?

Based on all internet users [N=926]

MAY 2016		
%	69	Yes, have done this
	30	No, have not done this
	*	(VOL.) Don't know
	*	(VOL.) Refused

ACCT3 Thinking about some of the companies and organizations that you interact with, how confident are you that they will keep your personal records safe from hackers or unauthorized users? [FOR FIRST TWO RANDOMIZED ITEMS: Thinking about [INSERT ITEMS; RANDOMIZE; ALWAYS ASK ITEMS a AND b TOGETHER AND IN ORDER], how confident are you that these records will be safe from hackers and unauthorized users?

How about...[INSERT NEXT ITEM]? [READ FOR FIRST ITEM THEN AS NECESSARY: Would you say you are very confident, somewhat confident, not too confident, or not at all confident that these records will be safe from hackers and unauthorized users?]

	VERY CONFI- DENT	SOME- WHAT CONF- IDENT	NOT TOO CONFI- DENT	NOT AT ALL CONF- IDENT	(VOL.) DOESN'T APPLY	(VOL.) DK	(VOL.) REF.
<i>Items A-B: Based on cell phone owners [N=992]</i>							
a. The telephone company that provides your cell phone service	21	47	15	15	*	1	1
b. The company that manufactured your cell phone	27	43	13	13	1	3	*
<i>Item C: Based on all internet users [N=926]</i>							
c. Your email provider	20	46	17	13	2	1	*
<i>Item D: Based on social media users [N=665]</i>							
d. The social media sites you use	9	38	27	24	1	*	*
e. The federal government	12	37	21	28	1	1	*
f. Your credit card company	23	36	13	13	15	1	*
g. The companies or retailers you do business with	14	46	21	15	2	2	*

SECUR1 In general, how secure do you feel your personal information is compared with five years ago? Do you think it is [READ] [RANDOMIZE 1-2]

MAY 2016		
%	49	Less secure
	18	More secure
	31	Or about as secure as it was five years ago
	1	(VOL.) Don't know
	*	(VOL.) Refused

SECUR2 (To the best of your knowledge...) Have you ever...[INSERT ITEMS; RANDOMIZE; ASK ITEMS a AND b TOGETHER IN ORDER]?

	YES	NO	(VOL.) DON'T KNOW	(VOL.) REFUSED
a. Received a notice that your social security number had been compromised	15	84	1	0
b. Received a notice that other sensitive personal information, such as your account number, had been compromised	35	64	1	*
c. Noticed fraudulent charges on your debit or credit card	41	58	*	*
<i>Item D: Based on all internet users [N=926]</i>				
d. Had someone take over your email account without your permission	19	80	1	*
<i>Item E: Based on social media users [N=665]</i>				
e. Had someone take over your social media account without your permission	21	79	*	*
f. Had someone attempt to open a line of credit or apply for a loan using your name	14	84	1	*
g. Had someone attempt to receive a tax refund using your name	6	93	1	*

[READ TO ALL INTERNET USERS:] On a different subject...

HABITS1 Thinking about your online activities, do you ever keep track of your passwords by...[INSERT ITEMS; RANDOMIZE; ASK ITEMS c AND d TOGETHER IN ORDER; 'SOME OTHER WAY' ALWAYS LAST]? How about by...[INSERT NEXT ITEM]? [READ AS NECESSARY: Do you ever keep track of your passwords in this way?]

Based on all internet users [N=926]

	YES	NO	(VOL.) DON'T KNOW	(VOL.) REFUSED
a. Memorizing them in your head	86	14	*	*
b. Writing them down on a piece of paper	49	51	*	*
c. Using a password management program such as Dashlane, Lastpass, or Apple Keychain	12	87	1	*
d. Saving them in a note or document on your computer or mobile device	24	75	*	*
e. Saving them in your internet browser	18	81	*	*
f. Some other way that I haven't already mentioned (SPECIFY)	3	95	1	1

HABITS2 Thinking about the different ways you keep track of your online passwords, which one do you use the MOST? Is it [READ; ONLY INCLUDE "YES" RESPONSES FROM HABITS1; LIST RESPONSES IN SAME ORDER AS HABITS1]?⁵

Based on all internet users [N=926]

MAY 2016		
%	65	Memorizing them in your head
	18	Writing them down on a piece of paper
	6	Saving them in a note or document on your computer or mobile device
	3	Using a password management program such as Dashlane, Lastpass, or Apple Keychain
	2	Saving them in your internet browser
	1	Some other way
	1	(VOL.) Don't know
	*	(VOL.) Refused
	2	Don't keep track of passwords any of these ways

HABITS3 Thinking about all of the passwords you use to access your various online accounts, would you say that [RANDOMIZE: (most of your passwords are the same or very similar to each other) or that (most of your passwords are very different from each other)]?

Based on all internet users [N=926]

MAY 2016		
%	57	Most passwords are very different
	39	Most passwords are the same or very similar
	1	(VOL.) Don't know
	2	(VOL.) Refused

[RANDOMIZE HABITS4A THRU HABITS4C]

HABITS4A Do you ever have a hard time keeping track of your passwords, or is this not something that happens to you?

Based on all internet users [N=926]

MAY 2016		
%	39	Yes
	60	No
	1	(VOL.) Don't know
	*	(VOL.) Refused

⁵ Question was asked of respondents who said 'yes' to more than one item in HABITS1. Results shown here have been recalculated to include those who said 'yes' to only one item or said 'no/DK/Refused' to all items in HABITS1.

HABITS4B Do you ever worry about how secure your passwords are, or is this not something you worry about?

Based on all internet users [N=926]

MAY 2016		
%	30	Yes
	69	No
	*	(VOL.) Don't know
	*	(VOL.) Refused

HABITS4C Do you ever use passwords that are less secure than you'd like because complicated passwords are too hard to remember, or is this not something you do?

Based on all internet users [N=926]

MAY 2016		
%	25	Yes
	74	No
	1	(VOL.) Don't know
	1	(VOL.) Refused

HABITS5 Have you ever shared a password to one of your online accounts with a friend or family member?

Based on all internet users [N=926]

MAY 2016		
%	41	Yes
	59	No
	*	(VOL.) Don't know
	*	(VOL.) Refused

HABITS6 Do you use two-factor or two-step authentication for any of your online accounts? [IF RESPONDENT ASKS FOR DEFINITION OF "TWO FACTOR": Two-factor authentication is a feature where you are sent a one-time code via email, text message, or some other method that you would enter after first entering your username and password, and only works for a single login and for a limited amount of time.]

Based on all internet users [N=926]

MAY 2016		
%	52	Yes
	46	No
	1	(VOL.) Don't know
	1	(VOL.) Refused

HABITS7 Have you ever used your social media account information to log into another website, or have you never done this?

Based on social media users [N=665]

MAY 2016		
%	39	Yes, have done this
	60	No, have never done this
	1	(VOL.) Don't know
	*	(VOL.) Refused

[READ TO SMARTPHONE OWNER:] Now thinking specifically about your smartphone...

HABITS8 Do you have to use a code, password, or other security feature in order to access your phone?

Based on smartphone owners [N=746]

MAY 2016		
%	71	Yes
	28	No
	0	(VOL.) Don't know
	1	(VOL.) Refused

HABITS9 What kind of security feature do you use to access your phone? Is it [READ]

Based on those whose smartphone requires a bypass code [N=529]

MAY 2016		
%	35	A PIN CODE containing only numbers
	13	A PASSWORD containing numbers, letters, or symbols
	12	A pattern of dots you connect with your finger
	32	A thumbprint, OR
	3	Some other kind of screen lock I haven't mentioned yet? (SPECIFY)
	1	(VOL.) Don't know
	5	(VOL.) Refused

HABITS10 Thinking about the APPS on your smartphone, how frequently do you update them? Do you set them to update automatically, do you update them yourself as soon as you are notified that there is a new version available, do you update them yourself whenever it's convenient, or do you never update your apps?

Based on smartphone owners [N=746]

MAY 2016		
%	32	Set them to update automatically
	16	Update them yourself as soon as a new version is available
	38	Update them yourself whenever it is convenient
	10	Never install app updates
	2	(VOL.) Different settings for different apps
	1	(VOL.) Don't know
	1	(VOL.) Refused

HABITS11 And thinking about the OPERATING SYSTEM on your smartphone, how frequently do you update it? Do you usually update it as soon as you are notified that a new version is available, do you update it whenever it's convenient, or do you never update your smartphone operating system?

Based on smartphone owners [N=746]

MAY 2016		
%	42	Update as soon as new version is available
	42	Wait until it is convenient
	14	Never update operating system
	1	(VOL.) Don't know
	1	(VOL.) Refused

HABITS12 Have you installed any virus protection apps on your smartphone, or not?

Based on smartphone owners [N=746]

MAY 2016		
%	32	Yes
	66	No
	2	(VOL.) Don't know
	*	(VOL.) Refused

[READ TO ALL INTERNET USERS:] On a different subject...

WIFI1 Do you ever access public WiFi in places such as airports, cafes, hotels or libraries?

Based on all internet users [N=926]

MAY 2016		
%	54	Yes
	46	No
	0	(VOL.) Don't know
	*	(VOL.) Refused

WIFI2 Do you ever [INSERT ITEMS; RANDOMIZE] while connected to public WiFi, or not?

	YES	NO	(VOL.) NOT APPLICABLE	(VOL.) DON'T KNOW	(VOL.) REFUSED
<i>Items A-B: Based on internet users who ever access public WiFi [N=502]</i>					
a. Make online purchases	21	78	*	1	*
b. Do online banking or conduct other financial transactions	20	79	0	1	*
<i>Item C: Based on social media users who ever access public WiFi [N=412]</i>					
c. Use social media	80	19	0	1	*
<i>Item D: Based on internet users who ever access public WiFi [N=502]</i>					
d. Use email	71	28	0	*	0

[READ TO ALL:] Next...

POLICY1 Many technology services use encryption of their customers' data and communications. Encryption prevents other people from accessing users' data without their permission, but can also prevent government law enforcement agencies from accessing that data during criminal investigations. Which one of the following statements comes closer to your view, even if neither is exactly right? [READ AND RANDOMIZE]

MAY 2016		
%	46	The government should be able to access encrypted communications when investigating crimes
	44	Technology companies should be able to use encryption technology that is unbreakable, even to law enforcement
	4	(VOL.) It depends
	4	(VOL.) Don't know
	2	(VOL.) Refused

POLICY2a How likely do you think it is that in the next five years, the United States will experience a significant cyberattack on our public infrastructure, such as our air traffic control system or power grid? Do you think this will definitely happen, probably happen, probably NOT happen, or definitely NOT happen in the next five years?

MAY 2016		
%	18	Definitely happen
	51	Probably happen
	23	Probably NOT happen
	3	Definitely NOT happen
	4	(VOL.) Don't know
	*	(VOL.) Refused

POLICY2b How likely do you think it is that in the next five years, the United States will experience a significant cyberattack on the banking and financial system? Do you think this will definitely happen, probably happen, probably NOT happen, or definitely NOT happen in the next five years?

MAY 2016		
%	18	Definitely happen
	48	Probably happen
	27	Probably NOT happen
	4	Definitely NOT happen
	2	(VOL.) Don't know
	*	(VOL.) Refused

POLICY3 How well-prepared do you think the U.S. government is to prevent cyberattacks on our public infrastructure? Is it [READ]

MAY 2016		
%	13	Very prepared
	49	Somewhat prepared
	19	Not too prepared
	14	Not at all prepared
	4	(VOL.) Don't know
	1	(VOL.) Refused

POLICY4 How well-prepared do you think the U.S. government is to prevent cyberattacks on government agencies? Is it [READ]

MAY 2016		
%	18	Very prepared
	51	Somewhat prepared
	16	Not too prepared
	11	Not at all prepared
	3	(VOL.) Don't know
	1	(VOL.) Refused

POLICY5 How well-prepared do you think U.S. BUSINESSES are to prevent cyberattacks on their own systems? Are they [READ]

MAY 2016		
%	9	Very prepared
	52	Somewhat prepared
	23	Not too prepared
	12	Not at all prepared
	4	(VOL.) Don't know
	*	(VOL.) Refused

POLICY6 Thinking about some recent instances of cyberattacks, have you heard anything about [INSERT ITEMS; RANDOMIZE], or is this not something you have heard of? [IF YES, ASK: Have you heard a lot about this, or a little about it?]

Next, have you heard anything about...[INSERT NEXT ITEM]? [IF YES, ASK: Have you heard a lot about this, or a little about it?]

	NET YES, HAVE HEARD	YES, HAVE HEARD A LOT	YES, HAVE HEARD A LITTLE	NO, HAVE NOT HEARD OF THIS	(VOL.) DON'T KNOW	(VOL.) REFUSED
a. The publication of company emails at the Sony Corporation	40	20	21	59	*	*
b. The exposure of government security clearance information at the Office of Personnel Management	33	12	21	67	1	*
c. The exposure of credit card data of customers who shopped at Target stores	75	47	28	24	1	*
d. The disruption of the power grid in Ukraine	22	5	17	77	1	0
e. The publishing of the identities of AshleyMadison.com customers	49	25	24	50	1	*

Cofield, Valerie M. (DO) (FBI)

From: Cofield, Valerie M. (DO) (FBI)
Sent: Thursday, January 26, 2017 4:38 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: pew report on encryption attitudes

Thanks for passing this along. Is there a good time next week that I could set up a conference call with you to discuss GD?

From: Richman, Daniel C. (DO) (OGA)
Sent: Thursday, January 26, 2017 4:22 PM
To: Cofield, Valerie M. (DO) (FBI) [REDACTED] Littlehale, Richard
[REDACTED]
Subject: pew report on encryption attitudes

b6 -2
b7C -2
b7E -3

Dear Val, Rich and Kenn -- in case you missed it, attached is the Pew report on attitudes re cyber. PP. 27-28 is on encryption
dan r

[redacted] (DO) (FBI)

b6 -1
b7C -1

From: [redacted] (DO) (FBI)
Sent: Thursday, January 26, 2017 4:45 PM
To: Richman, Daniel C. (DO) (OGA); [redacted] (OGC) (FBI)
Subject: RE: OGE 450 Addendum

I will talk to OIC about it. Thanks.

From: Richman, Daniel C. (DO) (OGA)
Sent: Thursday, January 26, 2017 4:29 PM
To: [redacted] (OGC) (FBI); [redacted] (DO) (FBI)
[redacted]
Subject: OGE 450 Addendum

b6 -1
b7C -1
b7E -3

Dear [redacted] - Having just send you my OGE 450, I wanted to flag an arrangement that I didn't put in but maybe should have. At the end of last year (2016), a former AUSA friend asked me to consult for him on some motion papers in a federal criminal prosecution in the SDNY. I think the Bu may have had an investigative role, as its a corruption prosecution. I did no work on the case last year, so initially thought that disclosure comes in the next form. (I also took comfort in the guidance I got from OGC on [redacted])

b5 -1,2
b6 -1
b7C -1

I just want to make sure that was the right analysis. I'll be doing no fact work and do not intend to have my name on the motion papers. My only work will be help frame arguments some issues of federal criminal law.

should I do anything more on this?

thx

dan richman

[redacted] (DO) (FBI)

b6 -1
b7C -1

From: [redacted] (DO) (FBI)
Sent: Friday, January 27, 2017 11:45 AM
To: Richman, Daniel C. (DO) (OGA)
Subject: FW: OGE 450 Addendum

Hello Prof. Richman,

I received the question noted below. Can you provide more information on your proposed assistance in this matter? I ask because the Department of Justice has regulations, found at 5 C.F.R. 3801, that prohibit employees from engaging in outside employment that involves the practice of law, unless it is uncompensated and in the nature of community service (or on behalf of himself or family). Also prohibited is outside employment involving any criminal matters, be they federal, state or local. As an SGE, you are an employee, but the laws, rules and regulations often apply differently based on your SGE status. With respect to the DOJ regulations, there is no exception for SGEs, but waivers can be requested from DOJ under certain circumstances. Thanks.

[redacted]
OIC
[redacted]

b6 -1
b7C -1
b7E -3

From: [redacted] (OGC) (FBI)
Sent: Thursday, January 26, 2017 4:31 PM
To: [redacted] (DO) (FBI) [redacted]
Cc: [redacted] (DO) (FBI) [redacted]
Subject: FW: OGE 450 Addendum

b6 -1
b7C -1
b7E -3

Hi [redacted]

Please see Mr. Richman's note below. Any guidance you can provide is extremely appreciated!

Thank you,

[redacted]
Management and Program Analyst
Office of the General Counsel
Federal Bureau of Investigation
Office: [redacted]
Cell: [redacted]

b6 -1
b7C -1
b7E -3

Confidentiality Statement:

This message is transmitted to you by the Office of the General Counsel of the Federal Bureau of Investigation. The message, along with any attachments, may be confidential and legally privileged. If you are not the intended recipient of this message, please destroy it promptly without further retention or dissemination (unless otherwise required by law). Please notify the sender of the error by a separate e-mail or by calling [redacted]

From: Richman, Daniel C. (DO) (OGA)
Sent: Thursday, January 26, 2017 4:29 PM

FBI 18-CV-1833-7581

To: [redacted] (OGC) (FBI) [redacted] (DO) (FBI)

b6 -1
b7C -1
b7E -3

Subject: OGE 450 Addendum

Dear [redacted], Having just send you my OGE 450, I wanted to flag an arrangement that I didn't put in but maybe should have. At the end of last year (2016), a former AUSA friend asked me to consult for him on some motion papers in a federal criminal prosecution in the SDNY. I think the Bu may have had an investigative role, as its a corruption prosecution. I did no work on the case last year, so initially thought that disclosure comes in the next form. (I also took comfort in the guidance I got from OGC on [redacted])

b5 -1,2
b6 -1,4
b7C -1,4

I just want to make sure that was the right analysis. I'll be doing no fact work and do not intend to have my name on the motion papers. My only work will be help frame arguments some issues of federal criminal law.

should I do anything more on this?

thx

dan richman

Richard Littlehale

From: Richard Littlehale
Sent: Thursday, January 26, 2017 5:42 PM
To: Richman, Daniel C. (DO) (OGA); Cofield, Valerie M. (DO) (FBI);
[REDACTED]
Subject: RE: pew report on encryption attitudes

b6 -2
b7C -2

Thanks, Dan. We've been kicking this around on our end as well. I'll be interested to see if anyone wants to discuss it at the committee meeting on Monday. My suspicion is that this kind of survey isn't going to be terribly helpful because people's attitudes are going to be too dependent on the circumstances...i.e. do the case facts speak to them or not..."oppressed political dissident" vs "kidnapped child"....

Looks like the usual folks are digging in as the transition continues...

<https://threatpost.com/ag-noninsec-backs-law-enforcements-ability-to-overcome-encryption/123301/>

We are going to need to counter some of these reflexive talking points. Take that article, for example: The EFF countered, "this answer is a clear endorsement of backdooring the security we all rely on." Cardozo and Crocker wrote it is unfeasible for encryption to serve "many valuable and important purposes" and still be "overcome" when the government wants access to plaintext.

The usual tactic of casting exceptional access as a binary proposition, a zero-sum game...

Richard W. Littlehale
Special Agent in Charge
Technical Services Unit
Criminal Investigation Division
Tennessee Bureau of Investigation



901 R.S. Gass Boulevard
Nashville, TN 37216

Desk [REDACTED]

Fax [REDACTED]
[REDACTED]

b6 -2
b7C -2

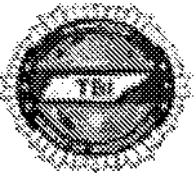
From: Richman, Daniel C. (DO) (OGA) [mailto:[REDACTED]]
Sent: Thursday, January 26, 2017 3:22 PM
To: Cofield, Valerie M. (DO) (FBI); [REDACTED]; Richard Littlehale
[REDACTED]
Subject: pew report on encryption attitudes

b6 -2
b7C -2
b7E -3

*** This is an EXTERNAL email. Please exercise caution. DO NOT open attachments or click links from unknown senders or unexpected email - STS-Security. ***

Dear Val, Rich and Kenn -- in case you missed it, attached is the Pew report on attitudes re cyber. PP.
27-28 is on encryption
dan r

FBI 18-CV-1833-7583



Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Friday, January 27, 2017 12:05 PM
To: [REDACTED] (DO) (FBI)
Subject: Re: OGE 450 Addendum
Attachments: Engagement Letter - Daniel Richman, Columbia Law.doc; US v. Percoco et al Indictment - Foreperson Signed (1).pdf

b6 -1,2
b7C -1,2

Dear [REDACTED] a pal from the SDNY asked me to assist him in his work representing a corporate executive in US v. Percoco et al. I am attaching the retainer letter, which i signed about 2 weeks ago. (It's a Word glitch that gives today's date.) Also the indictment. Since I am lawyer, who occasionally gets involved in cases; have no case involvement at the Bu; and have a unpaid SGE status that focuses on only encryption or cyber policy matters, my assumption and read of the SGE reg was that this would be OK. But i do want to be very careful. My work on this case will be limited to behind the scenes discussion of legal issues (not matters relating to litigating the facts), some drafts of legal arguments. and I don't plan to have my name on any motion papers.
thx so much for your help on this
dan r

From: [REDACTED] (DO) (FBI)
Sent: Friday, January 27, 2017 11:44 AM
To: Richman, Daniel C. (DO) (OGA)
Subject: FW: OGE 450 Addendum

b6 -1
b7C -1

Hello Prof. Richman,
I received the question noted below. Can you provide more information on your proposed assistance in this matter? I ask because the Department of Justice has regulations, found at 5 C.F.R. 3801, that prohibit employees from engaging in outside employment that involves the practice of law, unless it is uncompensated and in the nature of community service (or on behalf of himself or family). Also prohibited is outside employment involving any criminal matters, be they federal, state or local. As an SGE, you are an employee, but the laws, rules and regulations often apply differently based on your SGE status. With respect to the DOJ regulations, there is no exception for SGEs, but waivers can be requested from DOJ under certain circumstances. Thanks.

[REDACTED]
OIC
[REDACTED]

b6 -1
b7C -1
b7E -3

From: [REDACTED] (OGC) (FBI)
Sent: Thursday, January 26, 2017 4:31 PM
To: [REDACTED] (DO) (FBI) [REDACTED]
Cc: [REDACTED] (DO) (FBI) [REDACTED]
Subject: FW: OGE 450 Addendum

b6 -1
b7C -1
b7E -3

Hi [REDACTED]

FBI 18-CV-1833-7585

Please see Mr. Richman's note below. Any guidance you can provide is extremely appreciated!

Thank you,

[redacted]
Management and Program Analyst
Office of the General Counsel
Federal Bureau of Investigation
Office: [redacted]
Cell: [redacted]

b6 -1
b7C -1
b7E -3

Confidentiality Statement:

This message is transmitted to you by the Office of the General Counsel of the Federal Bureau of Investigation. The message, along with any attachments, may be confidential and legally privileged. If you are not the intended recipient of this message, please destroy it promptly without further retention or dissemination (unless otherwise required by law). Please notify the sender of the error by a separate e-mail or by calling [redacted]

From: Richman, Daniel C. (DO) (OGA)

Sent: Thursday, January 26, 2017 4:29 PM

To: [redacted] (OGC) (FBI) [redacted] (DO) (FBI)

[redacted]
Subject: OGE 450 Addendum

b6 -1
b7C -1
b7E -3

Dear [redacted], Having just send you my OGE 450, I wanted to flag an arrangement that I didn't put in but maybe should have. At the end of last year (2016), a former AUSA friend asked me to consult for him on some motion papers in a federal criminal prosecution in the SDNY. I think the Bu may have had an investigative role, as its a corruption prosecution. I did no work on the case last year, so initially thought that disclosure comes in the next form. (I also took comfort in the guidance I got from OGC on [redacted])

b5 -1,2
b6 -1,4
b7C -1,4

I just want to make sure that was the right analysis. I'll be doing no fact work and do not intend to have my name on the motion papers. My only work will be help frame arguments some issues of federal criminal law.

should I do anything more on this?

thx

dan richman

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

- - - - - x

UNITED STATES OF AMERICA

- v. -

JOSEPH PERCOCO,
a/k/a "Herb,"
ALAIN KALOYEROS,
a/k/a "Dr. K,"
PETER GALBRAITH KELLY, JR.,
a/k/a "Braith,"
STEVEN AIELLO,
JOSEPH GERARDI,
LOUIS CIMINELLI,
MICHAEL LAIPPLE, and
KEVIN SCHULER,

Defendants.

- - - - - x

OVERVIEW

1. As described more fully below, the charges in this Indictment stem from two wide-ranging and overlapping criminal schemes involving bribery, corruption, and fraud in the award of hundreds of millions of dollars in New York State (the "State") contracts and other official benefits. The first scheme concerned the payment of hundreds of thousands of dollars as directed by STEVEN AIELLO, JOSEPH GERARDI, LOUIS CIMINELLI, MICHAEL LAIPPLE, and KEVIN SCHULER, the defendants, to Todd Howe, who, among other things, was an agent and representative of SUNY Polytechnic Institute ("SUNY Poly"), a State-funded

public university. In exchange, Howe worked with ALAIN KALOYEROS, a/k/a "Dr. K," the defendant, who was the head of SUNY Poly, to secretly rig the bidding process for State contracts worth hundreds of millions of dollars in favor of the companies owned and managed by AIELLO, GERARDI, CIMINELLI, LAIPPLE, and SCHULER. The second scheme involved the payment of hundreds of thousands of dollars in bribes by two of Howe's clients - the company run by AIELLO and GERARDI, and an energy company, for which PETER GALBRAITH KELLY, the defendant, was the head of External Affairs - to JOSEPH PERCOCO, a/k/a "Herb," the defendant, who served as the Executive Deputy Secretary to the Governor of the State, in exchange for PERCOCO's assistance in obtaining official State action, including benefits worth millions of dollars to the clients.

RELEVANT INDIVIDUALS AND ENTITIES

New York State Government and the Office of the Governor

2. The State's executive branch is headed by the Governor, who serves as the State's chief executive, managing various State agencies, including those charged with overseeing economic development, environmental conservation, transportation and energy. The Governor's closest advisors and aides are referred to as working in the "Executive Chamber." In each year relevant to this Indictment, the government of the State

received funds from the federal government in excess of \$10,000 per year.

SUNY Poly and Fort Schuyler

3. SUNY Poly is a public institution of higher education that is part of the New York State University system (the "SUNY System"). The SUNY System is funded in part by the State, and also receives federal funds in excess of \$10,000 per year.

4. In or around 2009, Fort Schuyler Management Corporation ("Fort Schuyler") was created as a non-profit real estate corporation affiliated with SUNY Poly that could enter into contracts with private companies on SUNY Poly's behalf, for the purpose of carrying out development projects paid for with State funding. Fort Schuyler was governed by a Board of Directors, which, among other things, was charged with selecting private companies to partner with Fort Schuyler in SUNY Poly-related development projects. Certain public funding for SUNY Poly came through the Research Foundation for the State University of New York (the "Research Foundation"), which paid the salaries of many individuals associated with SUNY Poly and Fort Schuyler, including ALAIN KALOYEROS, a/k/a "Dr. K," the defendant, and Todd Howe (as a retained consultant), during the times relevant to this Indictment. During each year relevant to

this Indictment, the Research Foundation received more than \$10,000 in federal funding.

Todd Howe

5. Todd Howe has held several public positions, including working for the Governor of the State of New York when the Governor was United States Secretary of Housing and Urban Development, and for the Former Governor (the father of the Governor) when the Former Governor was Governor of New York.

6. During all times relevant to this Indictment, Howe was the president and primary employee of a government relations and lobbying firm (the "Government Relations Firm").

7. Beginning in or about 2012, Howe was retained as a consultant to the College of Nanoscale Science and Engineering ("CNSE"). CNSE was a public institution of higher education that was funded in part by the State. In or around September 2014, CNSE merged with the State University of New York Institute of Technology to become a new public university known as the SUNY Polytechnic Institute ("SUNY Poly"). In his role as a consultant for CNSE and SUNY Poly (hereinafter, "SUNY Poly"), Howe served as a close advisor to ALAIN KALOYEROS, a/k/a "Dr. K," the defendant, who was the head of SUNY Poly at all times relevant to this Indictment. Howe acted as an agent of SUNY Poly with respect to, among other things, SUNY Poly's

development projects, including large, State-funded development projects in Syracuse and Buffalo, New York. Howe also served as a primary liaison between SUNY Poly and the Governor's senior staff.

8. At various times relevant to this Indictment, Howe also was retained by and received payments from (a) a large real estate development firm located in Syracuse, New York (the "Syracuse Developer"); (b) a large Buffalo-based construction and development company (the "Buffalo Developer"); and (c) a privately-owned electric power generation development and asset management company (the "Energy Company").

ALAIN KALOYEROS

9. ALAIN KALOYEROS, a/k/a "Dr. K," the defendant, served as the head of SUNY Poly at all times relevant to this Indictment. KALOYEROS also served as a member of the Board of Directors of Fort Schuyler. KALOYEROS selected and provided direction to Fort Schuyler's officers and others working on behalf of Fort Schuyler.

STEVEN AIELLO, JOSEPH GERARDI, and the Syracuse Developer

10. At all times relevant to this Indictment, the Syracuse Developer, through various corporate affiliates, built, owned, and managed real estate in and around New York State. In or around December 2013, the Syracuse Developer was awarded a

contract with Fort Schuyler to serve as the preferred developer for projects of SUNY POLY to be created in Syracuse, New York. This contract permitted the Syracuse Developer to be chosen for SUNY Poly development projects of any size in or around Syracuse without further competitive bidding, and, indeed, shortly thereafter, the Syracuse Developer received a contract worth approximately \$15 million to build a film studio, and in or around October 2015, the Syracuse Developer received a contract worth approximately \$90 million to build a manufacturing plant, both in Syracuse, New York.

11. STEVEN AIELLO, the defendant, was a founder of the Syracuse Developer and has been its President since in or about 1998.

12. JOSEPH GERARDI, the defendant, was a founder of the Syracuse Developer and has been its General Counsel since in or about 1998.

*LOUIS CIMINELLI, MICHAEL LAIPPLE, KEVIN SCHULER, and
the Buffalo Developer*

13. At all times relevant to this Indictment, the Buffalo Developer provided construction management and general contracting services on various public and private projects in the State. In or around January 2014, the Buffalo Developer was named by Fort Schuyler as a preferred developer for projects of

SUNY Poly to be built in Buffalo, New York. This award permitted the Buffalo Developer to be chosen for SUNY Poly development projects of any size in or around Buffalo without further competitive bidding, and, indeed, in or around March 2014, as a result of its position as a preferred developer, the Buffalo Developer received a contract worth approximately \$225 million to build a manufacturing plant in Buffalo, New York. That contract ultimately expanded to be worth approximately \$750 million.

14. LOUIS CIMINELLI, the defendant, was the Chairman and CEO of the Buffalo Developer, and served in that role at all times relevant to this Indictment.

15. MICHAEL LAIPPLE, the defendant, was the President of a division of the Buffalo Developer that focused, among other things, on initiatives involving public-private infrastructure projects, and served in that role at all times relevant to this Indictment.

16. KEVIN SCHULER, the defendant, was a Senior Vice President for the Buffalo Developer, and served in that role at all times relevant to this Indictment.

PETER GALBRAITH KELLY and the Energy Company

17. As is relevant to this Indictment, since in or about 2008, the Energy Company had been working to develop a

power plant in Wawayanda, New York (the "New York Power Plant"), that was estimated to cost approximately \$900 million. At around the same time, the Energy Company also was developing a Power Plant in New Jersey (the "New Jersey Power Plant").

18. At all times relevant to this Indictment, PETER GALBRAITH KELLY, JR., a/k/a "Braith," the defendant, was the Senior Vice President of External Affairs at the Energy Company.

JOSEPH PERCOCO

19. In or about January 2011, JOSEPH PERCOCO, a/k/a "Herb," the defendant, was appointed to be the Executive Deputy Secretary to the Governor. As Executive Deputy Secretary, PERCOCO worked in the Executive Chamber and was a high-ranking, senior, and influential part of the Governor's Executive staff. PERCOCO also had a longstanding personal relationship with the Governor and the Governor's family, and was generally seen as the Governor's "right-hand man," who coordinated access to the Governor and often spoke for him on a broad array of substantive and administrative matters. PERCOCO also served as a primary "gatekeeper" of opportunities to speak or meet with the Governor, oversaw logistics of the Governor's events and travel, and supervised appointments and administrative matters for the Executive Chamber. During all times relevant to this Indictment, PERCOCO's primary work location was in Manhattan,

New York, although he typically traveled to Albany, New York approximately several times per month and was an almost constant presence with the Governor during the Governor's official duties.

20. On or about April 21, 2014, JOSEPH PERCOCO, a/k/a "Herb," the defendant, officially left New York State employment to serve as campaign manager for the Governor's reelection campaign, and returned to State employment on or about December 8, 2014. However, during the time period that PERCOCO was the manager of the Governor's reelection campaign, he continued to function in a senior advisory and supervisory role with regard to the Governor's Office, and continued to be involved in the hiring of staff and the coordination of the Governor's official events and priorities, and to travel with the Governor on official business, among other responsibilities. PERCOCO permanently left his position as Executive Deputy Secretary in or about January 2016.

21. JOSEPH PERCOCO, a/k/a "Herb," the defendant, has known Todd Howe since PERCOCO was a college student, when HOWE hired PERCOCO to work for the Former Governor.

THE BUFFALO BILLION FRAUD AND BRIBERY SCHEME

22. As part of the first criminal scheme alleged in

this Indictment, Todd Howe arranged for the Syracuse Developer, at the direction of STEVEN AIELLO and JOSEPH GERARDI, the defendants, and the Buffalo Developer, at the direction of LOUIS CIMINELLI, MICHAEL LAIPPLE and KEVIN SCHULER, the defendants, to obtain official State favors through Howe's position at SUNY Poly. More specifically, in exchange for hundreds of thousands of dollars in payments to Howe from the Syracuse Developer and the Buffalo Developer, respectively, Howe and ALAIN KALOYEROS, a/k/a "Dr. K," the defendant, devised a plan to secretly rig Fort Schuyler's bidding process so that State contracts that were ultimately worth hundreds of millions of dollars would be awarded to the Syracuse Developer and the Buffalo Developer.

23. As part of their plan, Todd Howe and ALAIN KALOYEROS, a/k/a "Dr. K," the defendant, had Fort Schuyler issue two requests for proposals (the "RFPs"), one for Syracuse (the "Syracuse RFP") and one for Buffalo (the "Buffalo RFP"), that would give the appearance of an open competition to choose "preferred developers" in Syracuse and Buffalo, respectively. However, the Syracuse Developer and the Buffalo Developer had been preselected by Howe and KALOYEROS to become the preferred developers, after the Syracuse Developer and the Buffalo Developer had each made sizeable contributions to the Governor

and had begun paying Howe in exchange for Howe's influence over the RFP processes.' These preferred developer contracts were particularly lucrative for the Syracuse Developer and the Buffalo Developer, as the Syracuse Developer and the Buffalo Developer were then entitled to be awarded future development contracts of any size in Syracuse or Buffalo, respectively, without additional competitive bidding, and thus without competing on price or qualifications for particular projects.

24. To carry out their criminal scheme, Todd Howe and ALAIN KALOYEROS, a/k/a "Dr. K," provided secret information concerning the Syracuse RFP and Buffalo RFP to STEVEN AIELLO, JOSEPH GERARDI, LOUIS CIMINELLI, MICHAEL LAIPPLE, and KEVIN SCHULER, the defendants, including advance copies of the RFPs that were provided to no other developers, and, in the case of the Buffalo RFP, provided CIMINELLI, LAIPPLE, and SCHULER with the location and purpose of the first preferred developer project - information that was provided to no other developer. Howe and KALOYEROS also worked with AIELLO and GERARDI to secretly tailor the Syracuse RFP to include qualifications that would favor the Syracuse Developer in Fort Schuyler's selection process for the Syracuse RFP; and worked with CIMINELLI, LAIPPLE, and SCHULER to secretly tailor the Buffalo RFP to

include qualifications that would favor the Buffalo Developer in Fort Schuyler's selection process for the Buffalo RFP.

25. As part of their criminal scheme, Todd Howe and ALAIN KALOYEROS, a/k/a "Dr. K," STEVEN AIELLO, JOSEPH GERARDI, LOUIS CIMINELLI, MICHAEL LAIPPLE, and KEVIN SCHULER, the defendants, deceived and concealed material information from Fort Schuyler and its Board of Directors in the following ways, among others:

a. KALOYEROS falsely represented to Fort Schuyler that the bidding processes for the Syracuse RFP and the Buffalo RFP were fair, open, and competitive, when in truth and in fact, KALOYEROS and Howe had predetermined that the Syracuse Developer would be awarded the Syracuse RFP and the Buffalo Developer would be awarded the Buffalo RFP.

b. The Syracuse Developer falsely certified that no one was retained, employed, or designated by or on behalf of the Syracuse Developer to attempt to influence the procurement process, when, in truth and in fact, the Syracuse Developer had retained Howe to influence the procurement process.

c. The Buffalo Developer falsely certified that no one was retained, employed, or designated by or on behalf of the Buffalo Developer to attempt to influence the procurement process, when, in truth and in fact, the Buffalo

Developer had retained Howe to influence the procurement process.

26. As a result of the criminal conduct alleged herein, the Syracuse Developer was awarded two State contracts worth a total of approximately \$105 million, and the Buffalo Developer was awarded a State contract that was ultimately worth approximately \$750 million.

The PERCOCO Bribery Scheme

27. The second scheme alleged in this Indictment involved Todd Howe arranging for two of his clients - the Syracuse Developer and the Energy Company - to pay bribes to JOSEPH PERCOCO, a/k/a "Herb," the defendant, in exchange for PERCOCO's use of his official position as Executive Deputy Secretary to the Governor and his far-reaching influence within the Executive Chamber to provide official State favors to the Syracuse Developer and the Energy Company worth millions of dollars.

PERCOCO's Receipt of Bribes from the Energy Company

28. From at least in or about 2012 up through and including at least in or about 2016, Todd Howe and PETER GALBRAITH KELLY, JR., a/k/a "Braith," the defendant, arranged for the Energy Company to pay more than \$287,000 in bribes to JOSEPH PERCOCO, a/k/a "Herb," the defendant, in exchange for

PERCOCO'S official assistance to benefit the Energy Company on an as-needed basis.

29. Beginning in or about 2010, PETER GALBRAITH KELLY, JR., a/k/a "Braith," the defendant, began offering and providing things of value to JOSEPH PERCOCO, a/k/a "Herb," the defendant, in an effort to obtain PERCOCO's official assistance on behalf of the Energy Company. Beginning in or about 2012, in response to repeated pressure from PERCOCO, KELLY arranged for the Energy Company to create a "low-show" job for PERCOCO's wife that resulted in payment to the PERCOCOs of \$7,500 per month. To conceal the nature and source of the payments, PERCOCO, KELLY, and Howe took the following steps, among others:

a. A consultant who worked for the Energy Company ("Consultant-1") was used as a pass-through to conceal the payments to the PERCOCOs.

b. KELLY, and others at KELLY's direction, purposefully kept PERCOCO's wife's last name and photograph out of certain work related documents and directed PERCOCO's wife to refer to herself by her first name when dealing with certain individuals when doing work for the Energy company.

c. KELLY falsely claimed to other executives

at the Energy Company that he had obtained an ethics opinion from the Governor's office approving the Energy Company's arrangement with PERCOCO's wife.

d. In his required financial disclosure statements for the years 2012 and 2014, PERCOCO represented that his wife was employed by a limited liability company in the name of Consultant-1, and did not list the Energy Company.

30. In exchange for the bribe payments paid through PERCOCO's wife as directed by PETER GALBRAITH KELLY, a/k/a "Braith," the defendant, JOSEPH PERCOCO, a/k/a "Herb," the defendant, agreed to take, and in fact took, official actions for the benefit of the Energy Company as the opportunity arose. Official actions taken by PERCOCO for the benefit of the Energy Company included, but were not limited to, the following:

a. PERCOCO exerted pressure on and provided advice to other State officials, with the intent that those officials secure for the Energy Company an agreement between a New Jersey state agency and the New York State Department of Environmental Conservation ("DEC") that would allow the Energy Company to purchase emissions credits in New York worth millions of dollars to the Energy Company in connection with the New Jersey Power Plant.

b. PERCOCO exerted pressure on and provided

advice to other State officials, with the intent that those officials work to secure for the Energy Company a lucrative long-term power purchase agreement (the "PPA") with the State guaranteeing a buyer for the power to be produced by the New York Power Plant.

31. After JOSEPH PERCOCO, a/k/a "Herb," the defendant, learned that the Energy Company would not be awarded the PPA, PERCOCO worked with Todd Howe to continue to extort payments from the Energy Company by promising KELLY that PERCOCO would continue to take official action to help the Energy Company obtain the PPA and taking steps to make KELLY believe PERCOCO was continuing to take such action.

PERCOCO'S Receipt of Bribes from the Syracuse Developer

32. From at least in or about August 2014 up through and including at least in or about October 2014, Todd Howe arranged for the Syracuse Developer to pay approximately \$35,000 in bribe payments to JOSEPH PERCOCO, a/k/a "Herb," the defendant, in exchange for PERCOCO's official assistance to the Syracuse Developer on an as-needed basis.

33. To conceal the nature and source of the payments, the Syracuse Developer and Todd Howe arranged to pay JOSEPH PERCOCO, a/k/a "Herb," the defendant, through a shell company controlled by Howe.

34. In exchange for the bribe payments paid to JOSEPH PERCOCO, a/k/a "Herb," the defendant, by STEVEN AIELLO and JOSEPH GERARDI, the defendants, through Todd Howe's shell company, PERCOCO agreed to take, and in fact took, official actions for the benefit of the Syracuse Developer as the opportunity arose. Official actions taken by PERCOCO for the benefit of the Syracuse Developer included, but were not limited to, the following:

a. PERCOCO exerted pressure on and provided advice to other State officials, with the intent that those officials reverse an adverse decision by the Empire State Development Corporation, which is the State's main economic development agency, that would have required the Syracuse Developer to enter into a costly agreement with labor unions.

b. PERCOCO exerted pressure on and provided advice to other State officials, with the intent that those officials secure the release of millions of dollars in State funds that were owed to the Syracuse Developer.

c. PERCOCO exerted pressure on and provided advice to other State officials, with the intent that those officials secure a raise for the son of STEVEN AIELLO, the defendant, who worked in the Executive Chamber.

COUNT ONE

(Wire Fraud Conspiracy - The Preferred Developer RFPs)

The Grand Jury further charges:

35. The allegations contained in paragraphs 1 through 34 above are hereby repeated, realleged, and incorporated by reference as if fully set forth herein.

36. From at least in or about 2013, up to and including in or about 2015, in the Southern District of New York and elsewhere, ALAIN KALOYEROS, a/k/a "Dr. K," STEVEN AIELLO, JOSEPH GERARDI, LOUIS CIMINELLI, MICHAEL LAIPPLE, and KEVIN SCHULER, the defendants, and others known and unknown, willfully and knowingly did combine, conspire, confederate, and agree together and with each other to commit wire fraud in violation of Section 1343 of Title 18, United States Code.

37. It was a part and an object of the conspiracy that ALAIN KALOYEROS, a/k/a "Dr. K," STEVEN AIELLO, JOSEPH GERARDI, LOUIS CIMINELLI, MICHAEL LAIPPLE, and KEVIN SCHULER, the defendants, and others known and unknown, willfully, and knowingly, having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, would and did transmit and cause to be transmitted by means of wire and radio communication in interstate and foreign

commerce, writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice, in violation of Title 18, United States Code, Section 1343, to wit, KALOYEROS, AIELLO, GERARDI, CIMINELLI, LAIPPLE, SCHULER, and their co-conspirators, devised a scheme to defraud Fort Schuyler in its award of significant taxpayer-funded development contracts by representing to Fort Schuyler that the bidding process for those contracts was fair, open, and competitive, when, in truth and in fact, KALOYEROS and Todd Howe used their official positions to secretly tailor the requests for proposals ("RFPs") for those contracts so that companies that were owned, controlled, and managed by AIELLO, GERARDI, CIMINELLI, LAIPPLE, and SCHULER would be favored to win in the selection process for the contracts.

(Title 18, United States Code, Section 1349.)

COUNT TWO

(Wire Fraud - The Syracuse RFP)

The Grand Jury further charges:

38. The allegations contained in paragraphs 1 through 34 above are hereby repeated, realleged, and incorporated by reference as if fully set forth herein.

39. From in or about 2013, up to and including in or

about 2015, in the Southern District of New York and elsewhere, ALAIN KALOYEROS, a/k/a "Dr. K," STEVEN AIELLO, and JOSEPH GERARDI, the defendants, willfully and knowingly, having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, did transmit and cause to be transmitted by means of wire and radio communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice, to wit, KALOYEROS, AIELLO, and GERARDI devised a scheme to defraud Fort Schuyler in its award of the Syracuse RFP by representing to Fort Schuyler that the bidding process for that contract was fair, open, and competitive, when, in truth and in fact, and as AIELLO and GERARDI well knew, KALOYEROS and Todd Howe used their official positions to secretly tailor the RFP for the Syracuse Preferred Developer contract so that the Syracuse Developer would be favored to win in the selection process for the contract.

(Title 18, United States Code, Sections 1343 and 2.)

COUNT THREE

(Payments of Bribes and Gratuities - The Syracuse RFP)

The Grand Jury further charges:

40. The allegations contained in paragraphs 1

through 34 above are hereby repeated, realleged, and incorporated by reference as if fully set forth herein.

41. From at least in or about 2013 to at least in or about 2015, in the Southern District of New York and elsewhere, STEVEN AIELLO and JOSEPH GERARDI, the defendants, willfully and knowingly did corruptly give, offer, and agree to give a thing of value to a person, with intent to influence an agent of a State government agency in connection with business, transactions, and series of transactions of such State agency involving a thing of value of \$5,000 and more, while such government and agency was in receipt of, in any one year period, benefits in excess of \$10,000 under a Federal program involving a grant, contract, subsidy, loan, guarantee, insurance, and other form of Federal assistance, to wit, AIELLO and GERARDI paid bribes to Todd Howe in exchange for, to influence, and to reward the taking of official action in his capacity as an agent and representative of SUNY Poly, in connection with obtaining the Syracuse RFP.

(Title 18, United States Code, Sections 666(a)(2) and 2.)

COUNT FOUR

(Wire Fraud - The Buffalo RFP)

The Grand Jury further charges:

42. The allegations contained in paragraphs 1

through 34 above are hereby repeated, realleged, and incorporated by reference as if fully set forth herein.

43. From in or about 2013, up to and including in or about 2015, in the Southern District of New York and elsewhere, ALAIN KALOYEROS, a/k/a "Dr. K," LOUIS CIMINELLI, MICHAEL LAIPPLE, and KEVIN SCHULER, the defendants, willfully and knowingly, having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, did transmit and cause to be transmitted by means of wire and radio communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice, to wit, KALOYEROS, CIMINELLI, LAIPPLE, and SCHULER devised a scheme to defraud Fort Schuyler in its award of the Buffalo RFP by representing to Fort Schuyler that the bidding process for those contracts was fair, open, and competitive, when, in truth and in fact, and as CIMINELLI, LAIPPLE, and SCHULER well knew, KALOYEROS and Todd Howe secretly used their official positions to tailor the RFP for the Buffalo Preferred Developer contract so that the Buffalo Developer would be favored to win in the selection process for the contract.

(Title 18, United States Code, Sections 1343 and 2.)

COUNT FIVE

(Payments of Bribes and Gratuities - The Buffalo RFP)

The Grand Jury further charges:

44. The allegations contained in paragraphs 1 through 34 above are hereby repeated, realleged, and incorporated by reference as if fully set forth herein.

45. From at least in or about 2013 to at least in or about 2015, in the Southern District of New York and elsewhere, LOUIS CIMINELLI, MICHAEL LAIPPLE, and KEVIN SCHULER, the defendants, willfully and knowingly did corruptly give, offer, and agree to give a thing of value to a person, with intent to influence an agent of a State government agency in connection with business, transactions, and series of transactions of such State agency involving a thing of value of \$5,000 and more, while such government and agency was in receipt of, in any one year period, benefits in excess of \$10,000 under a Federal program involving a grant, contract, subsidy, loan, guarantee, insurance, and other form of Federal assistance, to wit, CIMINELLI, LAIPPLE, and SCHULER paid bribes to Todd Howe in exchange for, to influence, and to reward the taking of official action in his capacity as an agent and representative of SUNY Poly, in connection with obtaining the Buffalo RFP.

(Title 18, United States Code, Sections 666(a)(2) and 2.)

COUNT SIX

(Conspiracy to Commit Extortion Under Color of Official Right)

The Grand Jury further charges:

46. The allegations contained in paragraphs 1 through 34 above are hereby repeated, realleged, and incorporated by reference as if fully set forth herein.

47. From at least in or about 2012, up to and including in or about 2016, in the Southern District of New York and elsewhere, JOSEPH PERCOCO, a/k/a "Herb," the defendant, while serving in the Office of the Governor, and others known and unknown, willfully and knowingly did combine, conspire, confederate, and agree together and with each other to commit extortion as that term is defined in Title 18, United States Code, Section 1951(b)(2), that is, by obtaining cash payments from the Energy Company and the Syracuse Developer, with their consent, such consent having been induced under color of official right, and thereby did obstruct, delay, and affect commerce, as that term is defined in Title 18, United States Code, Section 1951(b)(3), to wit, PERCOCO would and did cause companies with business before the State - namely, the Energy Company and the Syracuse Developer - to direct payments to PERCOCO in exchange for official actions taken or to be taken by PERCOCO for the benefit of the companies paying him.

(Title 18, United States Code, Sections 1951).

COUNT SEVEN

(Extortion Under Color of Official Right - The Energy Company)

The Grand Jury further charges:

48. The allegations contained in paragraphs 1 through 34 above are hereby repeated, realleged, and incorporated by reference as if fully set forth herein.

49. From at least in or about 2012, up to and including in or about 2016, in the Southern District of New York and elsewhere, JOSEPH PERCOCO, a/k/a "Herb," the defendant, while serving in the Office of the Governor, willfully and knowingly, did commit extortion as that term is defined in Title 18, United States Code, Section 1951(b)(2), that is, by obtaining cash payments from the Energy Company, with its consent, such consent having been induced under color of official right, and thereby did obstruct, delay, and affect commerce, as that term is defined in Title 18, United States Code, Section 1951(b)(3), to wit, PERCOCO used his official State position and power and authority within the Office of the Governor to cause the Energy Company to make and direct payments to PERCOCO's wife in exchange for official actions taken and agreed to be taken by PERCOCO.

(Title 18, United States Code, Sections 1951 and 2).

COUNT EIGHT

(Extortion Under Color of Official Right - The Syracuse Developer)

The Grand Jury further charges:

50. The allegations contained in paragraphs 1 through 34 above are hereby repeated, realleged, and incorporated by reference as if fully set forth herein.

51. From at least in or about 2014, up to and including in or about 2015, in the Southern District of New York and elsewhere, JOSEPH PERCOCO, a/k/a "Herb," the defendant, while serving in the Office of the Governor, willfully and knowingly, did commit extortion as that term is defined in Title 18, United States Code, Section 1951(b)(2), that is, by obtaining cash payments from the Syracuse Developer, with its consent, such consent having been induced under color of official right, and thereby did obstruct, delay, and affect commerce, as that term is defined in Title 18, United States Code, Section 1951(b)(3), to wit, PERCOCO used his official State position and power and authority within the Office of the Governor to cause the Syracuse Developer to make and direct payments to PERCOCO in exchange for official actions taken and agreed to be taken by PERCOCO.

(Title 18, United States Code, Sections 1951 and 2.)

COUNT NINE

(Conspiracy to Commit Honest Services Fraud)

The Grand Jury further charges:

52. The allegations contained in paragraphs 1 through 34 above are hereby repeated, realleged, and incorporated by reference as if fully set forth herein.

53. From at least in or about 2012, up to and including in or about 2015, in the Southern District of New York and elsewhere, JOSEPH PERCOCO, a/k/a "Herb," PETER GALBRAITH KELLY, JR., a/k/a "Braith," STEVEN AIELLO, and JOSEPH GERARDI, the defendants, Todd Howe, and others known and unknown, willfully and knowingly did combine, conspire, confederate and agree together and with each other to violate Title 18, United States Code, Sections 1343 and 1346.

54. It was a part and an object of the conspiracy that JOSEPH PERCOCO, a/k/a "Herb," PETER GALBRAITH KELLY, JR., a/k/a "Braith," STEVEN AIELLO, and JOSEPH GERARDI, the defendants, Todd Howe, and others known and unknown, willfully and knowingly, having devised and intending to devise a scheme and artifice to defraud, and to deprive the public of its intangible right to PERCOCO's honest services as a senior official in the Office of the Governor, would and did transmit

and cause to be transmitted by means of wire communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice, in violation of Title 18, United States Code, Sections 1343 and 1346, to wit, PERCOCO, while serving as Executive Deputy Secretary to the Governor, would and did take official action in exchange for bribes paid at the direction of KELLY, AIELLO, and GERARDI.

(Title 18, United States Code, Section 1349.)

COUNT TEN

(Solicitation of Bribes and Gratuities from The Energy Company)

The Grand Jury further charges:

55. The allegations contained in paragraphs 1 through 34 above are hereby repeated, realleged, and incorporated by reference as if fully set forth herein.

56. From at least in or about 2012, up to and including in or about 2016, in the Southern District of New York and elsewhere, JOSEPH PERCOCO, a/k/a "Herb," the defendant, being an agent and representative of a State government, to wit, a senior official in the Office of the Governor, corruptly solicited and demanded for the benefit of a person, and accepted and agreed to accept, a thing of value from a person, intending to be influenced and rewarded in connection with a business,

transaction, and series of transactions of such government involving a thing of value of \$5,000 and more, while such government was in receipt of, in any one year period, benefits in excess of \$10,000 under a Federal program involving a grant, contract, subsidy, loan, guarantee, insurance, and other form of Federal assistance, to wit, PERCOCO solicited and accepted cash and things of value from the Energy Company in exchange for official actions by PERCOCO and with the intent that PERCOCO be influenced and rewarded.

(Title 18, United States Code, Sections 666(a)(1)(B) and 2.)

COUNT ELEVEN

(Solicitation of Bribes and Gratuities from the Syracuse Developer)

The Grand Jury further charges:

57. The allegations contained in paragraphs 1 through 34 above are hereby repeated, realleged, and incorporated by reference as if fully set forth herein.

58. From at least in or about 2014, up to and including in or about 2015, in the Southern District of New York and elsewhere, JOSEPH PERCOCO, a/k/a "Herb," the defendant, being an agent and representative of a State government, to wit, a senior official in the Office of the Governor, corruptly solicited and demanded for the benefit of a person, and accepted

and agreed to accept, a thing of value from a person, intending to be influenced and rewarded in connection with a business, transaction, and series of transactions of such government involving a thing of value of \$5,000 and more, while such government was in receipt of, in any one year period, benefits in excess of \$10,000 under a Federal program involving a grant, contract, subsidy, loan, guarantee, insurance, and other form of Federal assistance, to wit, PERCOCO solicited and accepted cash and things of value from the Syracuse Developer in exchange for official actions by PERCOCO and with the intent that PERCOCO be influenced and rewarded.

(Title 18, United States Code, Sections 666(a)(1)(B) and 2.)

COUNT TWELVE

(Payments of Bribes and Gratuities - The Energy Company)

The Grand Jury further charges:

59. The allegations contained in paragraphs 1 through 34 above are hereby repeated, realleged, and incorporated by reference as if fully set forth herein.

60. From at least in or about 2012 to at least in or about 2016, in the Southern District of New York and elsewhere, PETER GALBRAITH KELLY, JR., a/k/a "Braith," the defendant, who was an executive at the Energy Company, willfully and knowingly did corruptly give, offer, and agree to give a thing of value to

a person, with intent to influence an agent of a State government, in connection with business, transactions, and series of transactions of such government, involving a thing of value of \$5,000 and more, while such government was in receipt of, in any one year period, benefits in excess of \$10,000 under a Federal program involving a grant, contract, subsidy, loan, guarantee, insurance, and other form of Federal assistance, to wit, KELLY paid JOSEPH PERCOCO, a/k/a "Herb," the defendant, in exchange for, to influence, and to reward the taking of official action to benefit the Energy Company, including to advance the development of the New York and New Jersey Power Plants.

(Title 18, United States Code, Sections 666(a)(2) and 2.)

COUNT THIRTEEN

(Payments of Bribes and Gratuities - The Syracuse Developer)

The Grand Jury further charges:

61. The allegations contained in paragraphs 1 through 34 above are hereby repeated, realleged, and incorporated by reference as if fully set forth herein.

62. From at least in or about 2014 to at least in or about 2015, in the Southern District of New York and elsewhere, STEVEN AIELLO and JOSEPH GERARDI, the defendants, who were executives at the Syracuse Developer, willfully and knowingly did corruptly give, offer, and agree to give a thing of value to

a person, with intent to influence an agent of a State government, in connection with business, transactions, and series of transactions of such government, involving a thing of value of \$5,000 and more, while such government was in receipt of, in any one year period, benefits in excess of \$10,000 under a Federal program involving a grant, contract, subsidy, loan, guarantee, insurance, and other form of Federal assistance, to wit, AIELLO and GERARDI paid JOSEPH PERCOCO, a/k/a "Herb," the defendant, in exchange for, to influence, and to reward the taking of official action to benefit the Syracuse Developer, including advancing its development projects in the State.

(Title 18, United States Code, Sections 666(a)(2) and 2.)

COUNT FOURTEEN

(False Statements to Federal Officers)

The Grand Jury further charges:

63. The allegations contained in paragraphs 1 through 34 above are hereby repeated, realleged, and incorporated by reference as if fully set forth herein.

64. On or about June 21, 2016, in the Southern District of New York and elsewhere, STEVEN AIELLO and JOSEPH GERARDI, the defendants, willfully and knowingly did make materially false, fictitious, and fraudulent statements and representations in a matter within the jurisdiction of the

executive branch of the Government of the United States, to wit, AIELLO and GERARDI, while meeting with federal agents and representatives of the United States Attorney's Office for the Southern District of New York, each made statements denying involvement in paying JOSEPH PERCOCO, a/k/a "Herb," the defendant, and in tailoring a request for proposal for the benefit of their company, the Syracuse Developer, when, in truth and in fact, AIELLO and GERARDI directed payments to PERCOCO and conspired to tailor a request for proposal for the benefit of their company.

(Title 18, United States Code, Section 1001(a)(2).)

FORFEITURE ALLEGATIONS

65. As the result of committing the offenses charged in Counts One through Thirteen of this Indictment, JOSEPH PERCOCO, a/k/a "Herb," ALAIN KALOYEROS, a/k/a "Dr. K," PETER GALBRAITH KELLY, JR., a/k/a "Braith," STEVEN AIELLO, JOSEPH GERARDI, LOUIS CIMINELLI, MICHAEL LAIPPLE, and KEVIN SCHULER, the defendants, shall forfeit to the United States, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), any and all property, real and personal, that constitutes or is derived from proceeds traceable to the commission of said offenses, including but not limited to a sum of money in United States currency representing

the amount of proceeds traceable to the commission of said offenses.

Substitute Asset Provision

66. If any of the above-described forfeitable property, as a result of any act or omission of the defendants:

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third person;

c. has been placed beyond the jurisdiction of the Court;

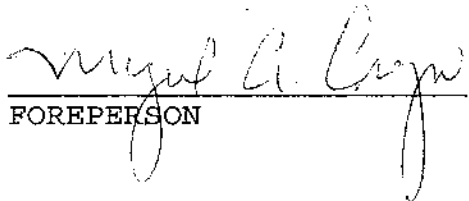
d. has been substantially diminished in value;
or

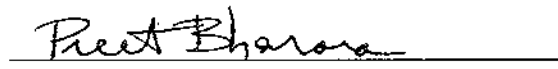
e. has been commingled with other property that cannot be subdivided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), and Title 28, United States Code, Section 2461(c), to seek forfeiture of any other property

of said defendant up to the value of the above forfeitable
property.

(Title 18, United States Code, Sections 981; Title 21, United
States Code, Section 853(p); Title 28, United States Code,
Section 2461.)


FOREPERSON


PREET BHARARA
United States Attorney

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

- v. -

JOSEPH PERCOCO, a/k/a "Herb,"
ALAIN KALOYEROS, a/k/a "Dr. K,"
PETER GALBRAITH KELLY, JR., a/k/a
"Braith," STEVEN AIELLO, JOSEPH GERARDI,
LOUIS CIMINELLI, MICHAEL LAIPPLE, and
KEVIN SCHULER

Defendants.

INDICTMENT

16 Cr.

(18 U.S.C. Sections 1951, 1349, 1343,
666(a)(1)(B), 666(a)(2), 1001(a)(2) and
2.)

PREET BHARARA

United States Attorney.

Miguel A. Cruz

FEDERAL BUREAU OF INVESTIGATION
 FOI/PA
 DELETED PAGE INFORMATION SHEET
 18th Interim Release
 Civil Action# 18-cv-1833, FOIA 1404359-0

Total Withheld Page(s) =90

Bates Page Reference	Reason for Withholding (i.e., exemptions with coded rationale, duplicate, sealed by order of court, etc.)
18-cv-1833 - 7630	Duplicate to Bates Page-7628
7633	Duplicate of Bates Page-7628
7648	Duplicate of Bates Page-7628
7651	Duplicate of Bates Page-7628
7655	Duplicate of Bates Page-7628
7662	Duplicate of Bates Page-7628
7667-7670	Referral Consult
7675	Duplicate of Bates Page-7628
7676	Referral Consult
7680	Duplicate of Bates Page-7628
7685	Duplicate of Bates Page-7628
7688	Referral Consult
7722-7723, 7725-7726, 7729-7731	(b)(5)-1
7724, 7727-7728	(b)(5)-1, and (b)(7)(E)-6
7751-7774	(b)(7)(E)-5, 11
7798-7819, 7821-7831	(b)(7)(E)-11
7820	(b)(7)(E)-3, 11
7854-7857	Duplicate of Bates Pages 7842-7845
7860-7863	Duplicate of Bates Pages 7842-7845

XXXXXXXXXXXXXXXXXXXXXXXXX
 X Deleted Page(s) X
 X No Duplication Fee X
 X For this Page X
 XXXXXXXXXXXXXXXXXXXXXXXXX

Richard Littlehale

From: Richard Littlehale
Sent: Friday, January 27, 2017 12:34 PM
To: Richman, Daniel C. (DO) (OGA); Cofield, Valerie M. (DO) (FBI)
Subject: RE: pew report on encryption attitudes

While I'm thinking of it, anything I should add to my reading list as I head out to Silicon Valley?

Dan, in particular, any suggestions on the best way to get current on the "code as speech" case law?

I'll keep you posted...

Richard W. Littlehale
Special Agent in Charge
Technical Services Unit
Criminal Investigation Division
Tennessee Bureau of Investigation



901 R.S. Gass Boulevard
Nashville, TN 37216

Desk [REDACTED]
Fax [REDACTED]
[REDACTED]

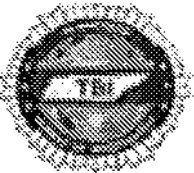
b6 -2
b7C -2

From: Richman, Daniel C. (DO) (OGA) [mailto:[REDACTED]]
Sent: Thursday, January 26, 2017 3:22 PM
To: Cofield, Valerie M. (DO) (FBI) [REDACTED] Richard Littlehale
[REDACTED]
Subject: pew report on encryption attitudes

b6 -2
b7C -2
b7E -3

*** This is an EXTERNAL email. Please exercise caution. DO NOT open attachments or click links from unknown senders or unexpected email - STS-Security. ***

Dear Val, Rich and Kenn – in case you missed it, attached is the Pew report on attitudes re cyber. PP. 27-28 is on encryption
dan r



Richard Littlehale

From: Richard Littlehale
Sent: Friday, January 27, 2017 12:54 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: quick question

Oh, and what I call "lawful hacking" when expressed as an alternative to regulation of encryption, you call something else...can you remind me what that is?

Richard W. Littlehale
Special Agent in Charge
Technical Services Unit
Criminal Investigation Division
Tennessee Bureau of Investigation

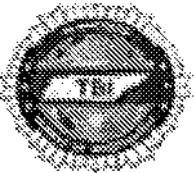


901 R.S. Gass Boulevard
Nashville, TN 37216

Desk [REDACTED]

Fax [REDACTED]
[REDACTED]

b6 -2
b7C -2



Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Friday, January 27, 2017 1:25 PM
To: Littlehale, Richard
Subject: Re: quick question

do you mean "network exploitation" or "vulnerability exploitation" ??

From: Richard Littlehale [REDACTED]
Sent: Friday, January 27, 2017 12:54 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: quick question

b6 -2
b7C -2

Oh, and what I call "lawful hacking" when expressed as an alternative to regulation of encryption, you call something else...can you remind me what that is?

Richard W. Littlehale
Special Agent in Charge
Technical Services Unit
Criminal Investigation Division
Tennessee Bureau of Investigation



901 R.S. Gass Boulevard
Nashville, TN 37216

Desk [REDACTED]

Fax [REDACTED]

[REDACTED]

Richard Littlehale

From: Richard Littlehale
Sent: Friday, January 27, 2017 1:27 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: Re: quick question

That's the one, thanks. I'm working on some framework materials...

Richard W. Littlehale
Special Agent in Charge
Criminal Investigation Division
Tennessee Bureau of Investigation

901 R.S. Gass Boulevard
Nashville, TN 37216

Desk [REDACTED]

Fax [REDACTED]

[REDACTED]

b6 -2
b7C -2
b7E -3

On Jan 27, 2017, at 12:26 PM, Richman, Daniel C. (DO) (OGA) [REDACTED] wrote:

*** This is an EXTERNAL email. Please exercise caution. DO NOT open attachments or click links from unknown senders or unexpected email - STS-Security. ***

do you mean "network exploitation" or "vulnerability exploitation" ??

From: Richard Littlehale [REDACTED]
Sent: Friday, January 27, 2017 12:54 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: quick question

b6 -2
b7C -2

Oh, and what I call "lawful hacking" when expressed as an alternative to regulation of encryption, you call something else...can you remind me what that is?

Richard W. Littlehale

Special Agent in Charge
Technical Services Unit

Criminal Investigation Division
Tennessee Bureau of Investigation

FBI 18-CV-1833-7631

<image001.png>

901 R.S. Gass Boulevard

Nashville, TN 37216

Desk

Fax

b6 -2
b7C -2

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Friday, January 27, 2017 1:28 PM
To: Littlehale, Richard; Cofield, Valerie M. (DO) (FBI)
Subject: Re: pew report on encryption attitudes
Attachments: Encryption Source Code and the First Amendment.pdf

good code as speech article attached. By the now dean of Yale Law School

From: Richard Littlehale [REDACTED]
Sent: Friday, January 27, 2017 12:33 PM
To: Richman, Daniel C. (DO) (OGA); Cofield, Valerie M. (DO) (FBI)
Subject: RE: pew report on encryption attitudes

b6 -2
b7C -2

While I'm thinking of it, anything I should add to my reading list as I head out to Silicon Valley?

Dan, in particular, any suggestions on the best way to get current on the "code as speech" case law?

I'll keep you posted...

Richard W. Littlehale
Special Agent in Charge
Technical Services Unit
Criminal Investigation Division
Tennessee Bureau of Investigation



901 R.S. Gass Boulevard

Nashville, TN 37216

Desk [REDACTED]

Fax [REDACTED]
[REDACTED]

From: Richman, Daniel C. (DO) (OGA) [mailto:[REDACTED]]
Sent: Thursday, January 26, 2017 3:22 PM
To: Cofield, Valerie M. (DO) (FBI) [REDACTED] Richard Littlehale
[REDACTED]
Subject: pew report on encryption attitudes

b6 -2
b7C -2
b7E -3

*** This is an EXTERNAL email. Please exercise caution. DO NOT open attachments or click links from unknown senders or unexpected email - STS-Security. ***

Dear Val, Rich and Kenn -- in case you missed it, attached is the Pew report on attitudes re cyber. PP. 27-28 is on encryption
dan r

FBI 18-CV-1833-7634

March 2000

Encryption Source Code and the First Amendment

Robert Post

Follow this and additional works at: <http://scholarship.law.berkeley.edu/btlj>

Recommended Citation

Robert Post, *Encryption Source Code and the First Amendment*, 15 BERKELEY TECH. L.J. 713 (2000).
Available at: <http://scholarship.law.berkeley.edu/btlj/vol15/iss2/5>

Link to publisher version (DOI)

<https://dx.doi.org/doi:10.15779/Z389X6C>

This Article is brought to you for free and open access by the Law Journals and Related Materials at Berkeley Law Scholarship Repository. It has been accepted for inclusion in Berkeley Technology Law Journal by an authorized administrator of Berkeley Law Scholarship Repository. For more information, please contact journals@law.berkeley.edu.

ENCRYPTION SOURCE CODE AND THE FIRST AMENDMENT

By Robert Post[†]

ABSTRACT

The First Amendment does not cover all speech acts. It instead extends constitutional protection to media for the communication of ideas, which are forms of social interaction that realize First Amendment values. The constitutional question, therefore, is whether particular uses of encryption source code are embedded within such media. It is insufficient to distinguish, as do current federal regulations, the publication of encryption source code in electronic form from its publication in written form. Instead it is necessary to focus on the social contexts within which encryption source code is used, whether in electronic or written form. From a constitutional perspective, it is one thing to use source code to convey ideas to an audience, and it is quite another to use source code to run a computer. The article suggests how each of these situations might be constitutionally analyzed.

Source code is a high level computer language typically used by programmers to compose computer software.¹ Federal regulations prohibit the unlicensed export of computer software, including source code, designed to encrypt messages.² To post encryption source code to the Internet is in most circumstances to "export" it under the terms of the regulations.³ Federal regulations do not seek to prohibit the unlicensed export of "a printed book or other printed material setting forth encryption source code," but

© 2000 Robert Post.

[†] Alexander F. and May T. Morrison Professor of Law, Boalt Hall School of Law, University of California, Berkeley.

1. See *Bernstein v. United States Dep't of Justice*, 176 F.3d 1132, 1140 (9th Cir. 1999), *withdrawn pending en banc reh'g*, 192 F.3d 1308 (9th Cir. 1999), *appeal dismissed without prejudice and remanded*, No. 97-16686 (9th Cir. April 11, 2000) [hereinafter *Bernstein IV*].

2. See *Bernstein v. United States Dep't of State*, 974 F. Supp. 1288, 1294-96 (N.D. Cal. 1997) [hereinafter *Bernstein I*]. To encrypt a message is to make it incomprehensible to someone who does not have the encryption code. Encryption code applies to messages that are sent in digital form. See ANDREW L. SHAPIRO, *THE CONTROL REVOLUTION* 73 (1999) ("Encryption tools . . . are the locks and keys of the digital age.").

3. See *Junger v. Daley*, 8 F. Supp. 2d 708, 713 (N.D. Ohio 1998), *rev'd and remanded*, No. 98-4045, 2000 U.S. App. LEXIS 6161 (6th Cir. April 4, 2000) ("Almost any posting of software on the Internet is an export.").

they do extend to "encryption source code in electronic form or media (e.g., computer diskette or CD ROM)."⁴

Daniel J. Bernstein, a professor of mathematics, statistics, and computer science, composed an encryption program called Snuffle in source code.⁵ He wished to "present his work on Snuffle within the academic and scientific communities."⁶ Bernstein brought suit challenging the federal regulations as a prior restraint on his ability to speak. The *Bernstein* case raises the fascinating and controversial question of whether computer programs written in source code can be a form of expression for purposes of the First Amendment. Lee Tien's rich and complex article substantially contributes to our understanding of this question.⁷

Tien's distinction between "coverage" and "protection," for example, is exactly right.⁸ To conclude that the First Amendment "covers" conduct, like the export of encryption source code, is to assert that the constitutionality of the conduct's regulation must be determined by reference to First Amendment doctrine and analysis. To conclude that the conduct is "protected" by the First Amendment, on the other hand, is to assert that the regulation of the conduct is unconstitutional. The question of First Amendment coverage goes to the threshold issue of the kind of analysis that should be brought to bear in evaluating the constitutionality of state regulations; the question of First Amendment protection goes to the ultimate judgments that we ought to reach in a particular case.

The threshold question posed by the *Bernstein* case is whether federal regulation of encryption source code is to be assessed under the doctrines of the First Amendment. This is a question of coverage, and it shall be my focus in this brief comment. *Bernstein* answered this question in the affirmative, holding that the constitutionality of the federal regulations was to be determined by First Amendment principles. A closely analogous case, however, has seemingly reached the contrary conclusion.⁹

4. 15 C.F.R. § 734.3 (1999), note to paras. (B)(2) and (B)(3).

5. See *Bernstein IV*, 176 F.3d at 1135-36.

6. *Id.* at 1136.

7. Lee Tien, *Publishing Software as a Speech Act*, 15 BERKELEY TECH. L.J. 629 (2000).

8. See Tien, *supra* note 7, at n.10. Tien draws this distinction from Frederick Schauer, *Categories and the First Amendment: A Play in Three Acts*, 34 VAND. L. REV. 265, 267 (1981).

9. See *Junger v. Daley*, 8 F. Supp. 2d 708, 708 (N.D. Ohio 1998), *rev'd and remanded*, No. 98-4045, 2000 U.S. App. LEXIS 6161 (6th Cir. Apr. 4, 2000). As this article was going to press, however, the District Court Opinion in *Junger* was reversed by the Sixth Circuit. *Junger v. Daley*, No. 98-4045, 2000 U.S. App. LEXIS 6161 (6th Cir. Apr. 4, 2000). In the *Junger* case, Peter Junger, a law professor teaching courses on computer

In his article, Tien argues that First Amendment coverage should presumptively extend to all speech acts, by which he means all acts of communication in which a speaker intends “to produce understanding in a hearer by resort to or in virtue of the conventional meaning of what the speaker says.”¹⁰ Thus for Tien the question of whether the publication of encryption code ought to be covered by the First Amendment depends upon whether publishing source code is a speech act.¹¹

For reasons I have articulated elsewhere, I believe that the premise of Tien’s argument is untenable.¹² There are many forms of speech acts that the First Amendment does not cover. Product warnings are clearly speech acts according to Tien’s definition, for example, and yet they are universally regulated in ways that are not covered by the First Amendment.¹³ Contracts are certainly speech acts, and yet contract law proceeds without the interference of First Amendment analysis. The general point is that social life largely occurs through language; social life is thus filled—one might even say composed of—interactions that meet Tien’s definition of speech acts. A First Amendment that covered all these aspects of social life would be nothing like the First Amendment which we currently possess. The presence of a speech act is therefore not sufficient to justify First Amendment coverage.¹⁴

law, challenged the federal export regulations as violating his First Amendment right to post encryption programs to his web site in order to use them as teaching materials. See *Junger*, 8 F. Supp. 2d at 714. The federal government had specifically allowed Junger to publish encryption programs in his textbook, *COMPUTERS AND THE LAW*. See *id.* The District Court in *Junger* appeared to hold that because encryption source code in electronic form was “inherently functional . . . indistinguishable from dedicated computer hardware that does encryption,” *id.* at 716, the electronic source code was not covered by the First Amendment. The holding is ambiguous, however, because the Court spoke in terms of First Amendment “protection,” *id.* at 716-18, and it in fact purported to apply various First Amendment doctrines.

10. Tien, *supra* note 7, at 637 n.29. Tien seems to accept the possibility of “defining out” certain kinds of speech acts, like fighting words, from First Amendment coverage.

11. This is essentially the position of the Sixth Circuit decision reversing the District Court opinion in *Junger*. See *Junger*, 2000 U.S. App. LEXIS 6161. The Court holds that “[b]ecause computer source code is an expressive means for the exchange of information and ideas about computer programming, we hold that it is protected by the First Amendment.” *Id.* at *10.

12. For the full development of the analysis set forth in this paragraph see Robert Post, *Recuperating First Amendment Doctrine*, 47 STAN. L. REV. 1249 (1995).

13. For a typical case, see, for example, *Hahn v. Sterling Drug, Inc.*, 805 F.2d 1480 (11th Cir. 1986).

14. I should also note that the presence of a speech act is also not *necessary* to justify First Amendment coverage. Campaign expenditures, for example, do not meet Tien’s definition of a speech act, and yet they are covered by the First Amendment. See Buckley

First Amendment coverage is sometimes triggered by *what* a legal rule regulates, and sometimes it is triggered by *why* a legal rule seeks to regulate.¹⁵ These inquiries are logically and practically independent of each other, and in this comment I shall focus exclusively on the first. I shall address the question whether the regulation of encryption source code ought to be subject to First Amendment scrutiny, but I shall not discuss whether the purpose of the federal regulations at issue in *Bernstein* would independently warrant First Amendment coverage.

If the presence of a speech act is not a sufficient condition for First Amendment coverage, how are we to specify the class of actions that does trigger First Amendment analysis? The view I have defended elsewhere is that First Amendment coverage is triggered by those forms of social interaction that realize First Amendment values.¹⁶ If we believe that the function of the First Amendment is to protect a marketplace of ideas, we will extend First Amendment coverage to those forms of social interaction that constitute such a marketplace. If we believe that the function of the First Amendment is to protect the communications necessary for democratic self-determination, we will extend First Amendment coverage to social interactions that instantiate the value of self-government.

From this perspective, Tien is fundamentally misguided to believe that he can explain First Amendment coverage "without appealing to a grand theoretical framework of First Amendment values."¹⁷ If First Amendment coverage does not extend to all speech acts, then such a framework is at a minimum necessary in order to provide the criteria by which to select the subset of speech acts that merit constitutional attention.

Actually the situation is more complicated than this, because First Amendment coverage is not limited to speech acts. It extends to forms of interaction that realize First Amendment values. In work published elsewhere I have used the term "medium" to designate such forms of interaction.¹⁸ The Court has held that "motion pictures are a significant medium for the communication of ideas,"¹⁹ for example, which signifies that film, considered as a genre, serves First Amendment values.

v. Valeo, 424 U.S. 1 (1976). In general, First Amendment coverage can be triggered by certain justifications for government regulations, whether or not those regulations are addressed to speech acts. See Post, *supra* note 12, at 1255-60.

15. See Post, *supra* note 12, at 1255-60.

16. See *id.* at 1254-55.

17. Tien, *supra* note 7, at 636.

18. See Post, *supra* note 12, at 1250-57.

19. Joseph Burstyn, Inc. v. Wilson, 343 U.S. 495, 501 (1952).

The genre of the cinema, however, encompasses far more than speech acts. It includes materials, like celluloid; functional machines, like projectors; buildings, like movie houses; social organizations, like studios; and so forth. If the state were to prohibit the use of projectors without a license, First Amendment coverage would undoubtedly be triggered. This is not because projectors constitute speech acts, but because they are integral to the forms of interaction that comprise the genre of the cinema. The licensing of projectors would have important effects on that genre, effects that would be quite pertinent to the very First Amendment values that lead us to protect motion pictures in the first place. That is why First Amendment coverage would likely extend to a law requiring projectors to be licensed.

First Amendment coverage, therefore, depends upon how the object of regulation is integrated into First Amendment media. Although a state may without First Amendment scrutiny prohibit public nudity, a First Amendment question would surely be raised if a state were to prohibit nudity within the cinema.²⁰ It would even raise a First Amendment question if a state were to attempt to apply a general prohibition of nudity to motion pictures.²¹ First Amendment coverage, in other words, does not attach to nudity considered as an isolated kind of conduct, but rather to the relationship between nudity and the forms of social interaction that the First Amendment seeks to protect.

Some judges and commentators, however, have sought to determine whether the First Amendment covers encryption source code by deciding whether such code, viewed as an isolated thing, is "inherently a functional device."²² But if the analysis I have suggested is correct, Tien is certainly right to conclude that one cannot "answer the coverage question by looking at software as a thing."²³ Although projectors are unambiguously a functional thing, the First Amendment might well cover their regulation

20. See, e.g., *Erznoznik v. City of Jacksonville*, 422 U.S. 205 (1975).

21. See *Post. supra* note 12, at 1259 (discussing *Barnes v. Glenn Theatre, Inc.*, 501 U.S. 560 (1991)); cf. *Cohen v. California*, 403 U.S. 15 (1971) (holding that California cannot prohibit the wearing of a jacket bearing an obscenity in an effort to remove the word from the public vocabulary).

22. *Bernstein IV*, 176 F.3d 1132, 1148 (9th Cir. 1999) (Nelson, J., dissenting); see also *Junger v. Daley*, 8 F. Supp. 2d 708, 716 (N.D. Ohio 1998), *rev'd and remanded*, No. 98-4045, 2000 U.S. App. LEXIS 6161 (6th Cir. April 4, 2000); Patrick Ian Ross, *Bernstein v. United States Department of State*, 13 *BERKELEY TECH. L.J.* 405, 410-15 (1998); John P. Collins, Jr., Note, *Speaking in Code*, 106 *YALE L.J.* 2691, 2696 (1997). But see *Thinh Nguyen, Cryptography, Export Controls, and the First Amendment in Bernstein v. United States Department of State*, 10 *HARV. J.L. & TECH.* 667, 677-78 (1997).

23. Tien, *supra* note 7, at 688.

because of the potential impact on motion pictures. The correct focus of constitutional inquiry is, therefore, as Tien properly asserts, "how software is used in an act."²⁴ The coverage question depends upon how the licensing of encryption source code affects First Amendment media.

It is clear that the federal regulations at issue in *Bernstein* attempt roughly to acknowledge this point by distinguishing between encryption source code in "a printed book or other printed material setting forth encryption source code," and "encryption source code in electronic form or media (e.g., computer diskette or CD ROM)."²⁵ The regulations do not require a license for reproducing source code in printed material.²⁶ This exception would be incomprehensible if preventing disclosure of the information contained in encryption source code were the only concern of the regulations. Evidently the regulations were also concerned with protecting First Amendment values.

We can identify one source of these values by attending to Tien's conclusion that "a computer program in source code form is a procedure written in a programming language."²⁷ Authors routinely write books and articles in which they communicate procedures to each other. Examples might be articles that explain the procedures necessary for medical diagnoses, or books that explain the procedures necessary for experiments in the physical sciences. Because we regard books and articles as a medium for the communication of ideas, such writings are unambiguously covered by the First Amendment.

For purposes of the First Amendment, the language in which books and articles are written is without importance. So long as books and articles communicate ideas to others, it makes no difference whether they are written in French, or in mathematical symbols, or in computer source code. Just as the First Amendment would cover a law requiring authors to obtain a license before publishing in an article the mathematical equations describing nuclear fusion, so would it cover regulations requiring a license before printing in an article the source code for an encryption program.

Some analysis roughly like this must explain why federal regulations permit encryption source code to be published without interference in book form. Why, then, do the regulations forbid the unlicensed publication of the identical source code in "electronic form or media (e.g., computer

24. Tien, *supra* note 7, at 691.

25. 15 C.F.R. § 734.3 (1999), note to paras. (B)(2) and (B)(3).

26. Hence Peter Junger was able without interference to publish encryption software in his textbook. See *Junger v. Daley*, F. Supp. 2d 708, 714 (N.D. Ohio 1998), *rev'd and remanded*, No. 98-4045, 2000 U.S. App. LEXIS 6161 (6th Cir. April 4, 2000).

27. Tien, *supra* note 7, at 667.

diskette or CD ROM)”? The federal government defended this distinction by arguing that when source code is published in electronic form, it does not implicate First Amendment concerns. In *Bernstein*, the federal government contended that source code in electronic form is a form of software “used to control directly the operation of a computer without conveying information to the user. In the government’s view, by targeting this unique functional aspect of source code, rather than the content of the ideas that may be expressed therein, the export regulations manage to skirt entirely the concerns of the First Amendment.”²⁸

The government’s argument, however, can not be correct. Publishing software in print is covered by the First Amendment because it forms part of public discourse and debate. We know that this same discourse and debate can occur over the Internet and in electronic form.²⁹ So long as the publication of encryption source code forms part of this public discourse and debate, it will be covered by the First Amendment, whether it is set forth in a printed article or in an online discussion. The government’s analysis leads directly to the absurd conclusion that an article about encryption code that would unambiguously be covered by the First Amendment when published in *Scientific American*, would somehow lose that coverage when scanned and posted to the Internet.

It may be the case, of course, that there are stronger justifications for prohibiting the publication of encryption code in electronic form than in printed form, a question about which I intimate no view. I observe only that this question goes to the issue of First Amendment *protection*; it is relevant to whether or not electronically reproduced encryption software may be regulated when analyzed under applicable First Amendment doctrines. It does not go to the question of First Amendment *coverage*.³⁰

The decisive question for coverage is whether or not the publication of the source code forms part of a First Amendment medium, and this question can be affirmatively answered even if the publication of the source code is in electronic form. For purposes of First Amendment coverage, it

28. *Bernstein IV*, 176 F.3d 1132, 1141-42 (9th Cir. 1999).

29. See *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997) (holding that the Communications Decency Act of 1996 was a constitutionally impermissible content based restriction on First Amendment speech).

30. This point is made by the Sixth Circuit decision in *Junger*, 2000 U.S. App. LEXIS 6161, at *10-11 (“The functional capabilities of source code, and particularly those of encryption source code, should be considered when analyzing the governmental interest in regulating the exchange of this form of speech. . . . We recognize that national security interests can outweigh the interests of protected speech and require the regulation of speech.”)

makes no difference whether an author wishes to discuss an encryption program written in source code in an article published in hard copy, or in an article electronically distributed through the Internet.

Suppose, however, that a person does not wish to discuss an encryption program written in source code, but to use an encryption program. We might imagine a consumer who buys a disk containing encryption software, intending to insert the disk into his computer to employ the software to encrypt his messages. In this situation, the content of the source code is not a subject of discussion or debate.³¹ The consumer does not know what the source code says; the code speaks directly to the consumer's computer.

The author of encryption software who distributes encryption source code to consumers to be used in this fashion is therefore not participating in public dialogue or debate. For this reason, regulation of encryption software in such contexts would seem to raise very different constitutional questions than any we have so far discussed. Such regulation appears, on its face, no different than the regulation of hardware in computers.

No doubt this is the paradigmatic situation that the government had in mind when it argued that the publication of encryption source code in electronic form was "used to control directly the operation of a computer without conveying information to the user."³² The difficulty with the government's position, however, is that for encryption source code to function in this way, it is a necessary but not sufficient condition for it to be written in electronic, rather than printed form. To know whether encryption source code forms part of a dialogue between humans or instead serves as instructions to computers, we must know more than that it is written in electronic form; we must also know the social circumstances of its sale and application.

For purposes of First Amendment coverage, therefore, the relevant distinction is not between encryption source code published in electronic as opposed to printed form, but rather between encryption source code that is itself part of public dialogue and encryption source code that is meant merely to be used. This latter distinction is surely messier—more difficult to formulate and enforce—than that presently contained in federal regulations. But it is the only constitutionally defensible distinction.

Unfortunately the distinction does not completely settle the question of First Amendment coverage. This is because encryption software can affect

31. Most likely, of course, the disk would be written in object code, not source code. See Mark A. Lemley and Eugene Volokh, *Freedom of Speech and Injunctions in Intellectual Property Cases*, 48 DUKE L.J. 147, 236-37 (1998).

32. *Bernstein IV*, 176 F.3d at 1142.

First Amendment media in various different ways. If encryption source code is itself a subject of discussion within a First Amendment medium, First Amendment coverage clearly ought to apply to attempts to regulate the publication of the code. That is why the Court in *Bernstein* was assuredly correct to hold that in the circumstances of the case the validity of the federal regulations had to be determined by reference to applicable First Amendment principles.³³ But even if encryption source code is not itself a subject of public discussion, its regulation might nevertheless affect public discussion in ways that ought to trigger First Amendment coverage.

To see how this might be so, recall our earlier discussion of movie projectors. Such projectors form no part of the speech content of movies. But a law forbidding the screening of films without a licensed projector would probably be covered by the First Amendment. We would be concerned about the law's potential impact on the medium of movies, in exactly the same way that we would be concerned about the potential impact on the press of a law that required all books to be printed on presses that were licensed by the state.³⁴

The First Amendment concerns that immediately spring to mind in these examples are those of viewpoint discrimination. We know that certain kinds of licensing schemes can be used to distort the ideas expressed through the media of film or books. Because we wish ideas to be freely and fully expressed through these media, we are alert to scrutinize licensing schemes under First Amendment standards to ensure that they do not compromise this constitutional value. The licensing scheme challenged in *Bernstein*, applied to the public discussion at issue in that case, raises analogous constitutional concerns.

State regulation, however, can compromise First Amendment media in ways that do not involve viewpoint discrimination. An obvious instance might be a law that prohibits newsprint in order to save trees. Newsprint is a material necessary for the publication of most newspapers. Although a law proscribing newsprint would be viewpoint (and content) neutral, it

33. Even the dissenting opinion of T.G. Nelson conceded that "*Bernstein* may very well have a claim under an as-applied First Amendment analysis." *Id.* at 1149. It is for this same reason that the District Court in *Junger* was almost certainly incorrect to hold that the First Amendment did not apply to the circumstances of that case. *See Junger v. Daley*, F. Supp. 2d 708 (N.D. Ohio 1998), *rev'd and remanded*, No. 98-4045, 2000 U.S. App. LEXIS 6161 (6th Cir. April 4, 2000).

34. *See* THOMAS I. EMERSON, *THE SYSTEM OF FREEDOM OF EXPRESSION* 504 (1970) (noting that prior restraint originated in part in opposition to laws forbidding books to be printed except by printing presses licensed by the state); *see also Talley v. California*, 362 U.S. 60, 64 (1960) (discussing effects of press licensing law).

would carry the potential for so significantly affecting the First Amendment medium of newspapers that we would certainly review it under First Amendment principles. We would want to assure ourselves that it would not compromise the constitutional value we attribute to newspapers.

Such review, including the threshold question of whether to engage in such review (which is the coverage question), will always rest upon a constitutional sociology by which we specify the social aspects of the medium that carry constitutional significance. This sociology can often prove difficult and puzzling, especially when it involves new and evolving technologies.

Consider, for example, a viewpoint (and content) neutral law that prohibits CD players. We know that music is a First Amendment medium.³⁵ CD players are machines that do not form part of the content of that medium, and yet today most music is distributed and heard through the technology of compact disks. Prohibiting CD players would materially disrupt the pattern of social relationships that comprise the contemporary medium of music. The First Amendment question would be whether this disruption threatens to undermine the constitutional values that have led us to classify music as a First Amendment medium. In such circumstances, the extension of First Amendment coverage would signify that we find this a sufficiently close or important question as to require us to decide it under First Amendment principles.

An analogous argument might be made to justify extending First Amendment coverage to encryption software. Even when such software functions purely as a "machine"³⁶ to make digital messages secret, we must ask whether its regulation might compromise the constitutional values we attribute to particular First Amendment media. The empirical and normative aspects of such an inquiry are, to say the least, formidable. First, we would have to assess the effects of federal regulation of encryption source code on the production and use of encryption software. Second, we would have to specify the impact of these effects on the various First Amendment media that employ encryption software. Finally we would have to face the normative question of whether this impact would raise sufficient constitutional concerns as to merit First Amendment coverage.

35. See *Ward v. Rock Against Racism*, 491 U.S. 781, 790 (1989).

36. See Pamela Samuelson et al., *A Manifesto Concerning the Legal Protection of Computer Programs*, 94 COLUM. L. REV. 2308, 2320-24 (1994); see also Ross, *supra* note 22, at 410-11; Lemley & Volokh, *supra* note 31, at 236.

Tien offers the valuable suggestion that encryption software might be conceived as providing the equivalent of envelopes which protect the privacy of underlying digital messages.³⁷ In some circumstances, a law that strips speech of privacy would certainly merit First Amendment coverage. Consider, for example, a regulation prohibiting mail from using envelopes and requiring that the contents of all letters be made legible to mail handlers. I have no doubt that courts would scrutinize such a law under relevant First Amendment doctrine. This is because the chill on participating in a First Amendment medium that comes from exposure is a well-recognized First Amendment interest.³⁸ Laws prohibiting anonymous political leaflets have thus been struck down because of their potential impact on speakers.³⁹

Encryption software is a way of preventing an analogous chill within digital media. It is probable that First Amendment coverage would extend to a law requiring a live operator to monitor all phone conversations.⁴⁰ We might imagine an analogous argument for First Amendment coverage of federal regulations of encryption source code *if* the world were such that digital phone conversations were routinely monitored, and *if* the effect of the regulations were essentially to deprive us of the ability to avoid such eavesdropping. It is not difficult to think up analogous arguments about communication over the Internet.

It is far beyond the ambition of this brief comment to make or to evaluate any such arguments. Digital First Amendment media, like the Internet, are so new and have such labile patterns of social interaction, that it seems to me enormously difficult to acquire reliable normative or descriptive traction on the relevant questions. My point in raising this line of inquiry is not to suggest a final resolution of the problem, but instead to indicate that it will be necessary to pursue this line of inquiry if we ever aspire to a more complete understanding of the issue of First Amendment coverage of federal regulation of encryption source code.

37. See Tien, *supra* note 7, at 673.

38. See *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449, 460-64 (1958).

39. See *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334 (1995); see also *Talley*, 362 U.S. at 60.

40. See generally *Sable Communications of California v. FCC*, 492 U.S. 115 (1989) (applying strict scrutiny under the First Amendment to a state law prohibiting certain kinds of sexual telephone conversation).

Richard Littlehale

From: Richard Littlehale
Sent: Sunday, January 29, 2017 10:09 AM
To: Richman, Daniel C. (DO) (OGA); Cofield, Valerie M. (DO) (FBI)
Subject: RE: pew report on encryption attitudes

Sorry to bother you everyone over the weekend, but I thought I would send this before hopping on my flight to San Jose to beard the lion in his den. As time permits next week, I'd be interested in your thoughts about how to discuss what it is becoming increasingly clear to me will be a central talking point in the next phase of the encryption conversation, from the other side at least - perceived problems with the wiretap reports to the USAOC.

<https://cyberlaw.stanford.edu/blog/2017/01/wiretap-reports-not-so-transparent>

Al Gidari has fired the opening salvo - a drum he has been beating for some time now -but the Keys Under Doormats folks see this as a way to challenge the Going Dark narrative...

My guess is it is going to run something like this: what is the government hiding? Why don't reported wiretaps match up with service provider disclosures? Why aren't some agencies reporting? If they can't be trusted to comply with a simple public disclosure requirement, how can we trust them with the keys to encryption?

Richard W. Littlehale
Special Agent in Charge
Technical Services Unit
Criminal Investigation Division
Tennessee Bureau of Investigation



901 R.S. Gass Boulevard
Nashville, TN 37216

Desk [redacted]
Fax [redacted]
[redacted]

b6 -2
b7C -2

From: Richman, Daniel C. (DO) (OGA) [mailto:[redacted]]
Sent: Friday, January 27, 2017 12:28 PM
To: Richard Littlehale [redacted]; Cofield, Valerie M. (DO) (FBI)
[redacted]
Subject: Re: pew report on encryption attitudes

b6 -2
b7C -2
b7E -3

good code as speech article attached. By the now dean of Yale Law School

From: Richard Littlehale [redacted]
Sent: Friday, January 27, 2017 12:33 PM

FBI 18-CV-1833-7649

To: Richman, Daniel C. (DO) (OGA); Cofield, Valerie M. (DO) (FBI)

Subject: RE: pew report on encryption attitudes

While I'm thinking of it, anything I should add to my reading list as I head out to Silicon Valley?

Dan, in particular, any suggestions on the best way to get current on the "code as speech" case law?

I'll keep you posted...

Richard W. Littlehale
Special Agent in Charge
Technical Services Unit
Criminal Investigation Division
Tennessee Bureau of Investigation



901 R.S. Gass Boulevard

Nashville, TN 37216

Desk [REDACTED]

Fax [REDACTED]

b6 -2

b7C -2

From: Richman, Daniel C. (DO) (OGA) [mailto:[REDACTED]]

Sent: Thursday, January 26, 2017 3:22 PM

To: Cofield, Valerie M. (DO) (FBI) [REDACTED]

Richard Littlehale

b6 -2

b7C -2

b7E -3

Subject: pew report on encryption attitudes

*** This is an EXTERNAL email. Please exercise caution. DO NOT open attachments or click links from unknown senders or unexpected email - STS-Security. ***

Dear Val, Rich and Kenn -- in case you missed it, attached is the Pew report on attitudes re cyber. PP. 27-28 is on encryption

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Sunday, January 29, 2017 4:37 PM
To: [REDACTED] (ITCRMD) (FBI); [REDACTED] (DO) (OGA)
Subject: never mind :)

b6 -1
b7C -1

Dear [REDACTED] and [REDACTED] - The internet gods heard my gnashing of teeth and made it so that when I just went to the 324 site, i didn't get the "authentication" pop-up; was able to get into 324mail using my passcode; and am using it now.
so thanks!
dan r

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Sunday, January 29, 2017 4:34 PM
To: Littlehale, Richard; Cofield, Valerie M. (DO) (FBI)
Subject: Re: pew report on encryption attitudes

Since I don't know much about the reporting protocol, I'll let Val bring people from OEO or EAOUSA to address this issue. But, not to be nasty, but do those making this argument realize that increased reliance on vulnerability exploitation will likely push the system even further from transparency?

From: Richard Littlehale [REDACTED]
Sent: Sunday, January 29, 2017 10:08 AM
To: Richman, Daniel C. (DO) (OGA); Cofield, Valerie M. (DO) (FBI)
Subject: RE: pew report on encryption attitudes

b6 -2
b7C -2

Sorry to bother you everyone over the weekend, but I thought I would send this before hopping on my flight to San Jose to beard the lion in his den. As time permits next week, I'd be interested in your thoughts about how to discuss what it is becoming increasingly clear to me will be a central talking point in the next phase of the encryption conversation, from the other side at least -- perceived problems with the wiretap reports to the USAOC.

<https://cyberlaw.stanford.edu/blog/2017/01/wiretap-reports-not-so-transparent>

Al Gidari has fired the opening salvo -- a drum he has been beating for some time now --but the Keys Under Doormats folks see this as a way to challenge the Going Dark narrative...

My guess is it is going to run something like this: what is the government hiding? Why don't reported wiretaps match up with service provider disclosures? Why aren't some agencies reporting? If they can't be trusted to comply with a simple public disclosure requirement, how can we trust them with the keys to encryption?

Richard W. Littlehale
Special Agent in Charge
Technical Services Unit
Criminal Investigation Division
Tennessee Bureau of Investigation



901 R.S. Gass Boulevard
Nashville, TN 37216

Desk [REDACTED]
Fax [REDACTED]
[REDACTED]

b6 -2
b7C -2
b7E -3

From: Richman, Daniel C. (DO) (OGA) [mailto:[REDACTED]]

FBI 18-CV-1833-7653

Sent: Friday, January 27, 2017 12:28 PM

To: Richard Littlehale [REDACTED] Cofield, Valerie M. (DO) (FBI)

b6 -2
b7C -2
b7E -3

Subject: Re: pew report on encryption attitudes

good code as speech article attached. By the now dean of Yale Law School

From: Richard Littlehale [REDACTED]

b6 -2
b7C -2

Sent: Friday, January 27, 2017 12:33 PM

To: Richman, Daniel C. (DO) (OGA); Cofield, Valerie M. (DO) (FBI)

Subject: RE: pew report on encryption attitudes

While I'm thinking of it, anything I should add to my reading list as I head out to Silicon Valley?

Dan, in particular, any suggestions on the best way to get current on the "code as speech" case law?

I'll keep you posted...

Richard W. Littlehale
Special Agent in Charge
Technical Services Unit
Criminal Investigation Division
Tennessee Bureau of Investigation



901 R.S. Gass Boulevard

Nashville, TN 37216

Desk [REDACTED]

Fax [REDACTED]
[REDACTED]

From: Richman, Daniel C. (DO) (OGA) [mailto:[REDACTED]]

b6 -2
b7C -2
b7E -3

Sent: Thursday, January 26, 2017 3:22 PM

To: Cofield, Valerie M. (DO) (FBI) [REDACTED]; Richard Littlehale

Subject: pew report on encryption attitudes

*** This is an EXTERNAL email. Please exercise caution. DO NOT open attachments or click links from unknown senders or unexpected email - STS-Security. ***

Dear Val, Rich and Kenn -- in case you missed it, attached is the Pew report on attitudes re cyber. PP. 27-28 is on encryption

[redacted] (DO) (OGA)

b6 -1
b7C -1

From: [redacted] (DO) (OGA)
Sent: Sunday, January 29, 2017 4:38 PM
To: Richman, Daniel C. (DO) (OGA); [redacted] (ITCRMD) (FBI)
Subject: RE: never mind :)

Glad it was resolved!

--

----- Original message -----

From: "Richman, Daniel C. (DO) (OGA)" [redacted]
Date: 01/29/2017 4:37 PM (GMT-05:00)
To: [redacted] (ITCRMD) (FBI)" [redacted] (DO) (OGA)"
[redacted]
Subject: never mind :)

b6 -1
b7C -1
b7E -3

Dear [redacted] and [redacted]: The internet gods heard my gnashing of teeth and made it so that when I just went to the 324 site, i didn't get the "authentication" pop-up; was able to get into 324mail using my passcode; and am using it now.
so thanks!
dan r

[redacted] (DO) (OGA)

b6 -1
b7C -1

From: [redacted] (DO) (OGA)
Sent: Monday, January 30, 2017 2:06 PM
To: [redacted] (DO) (FBI)
Cc: Richman, Daniel C. (DO) (OGA)
Subject: Crime Data

b6 -1
b7C -1

[redacted]

As part of a law journal publication, Dan Richman (cced) is trying to track down official statistics on murder and shootings, both nationally and for the nation's 30-50 largest cities from 2014-16. Would there be a good POC for him to speak with for the best source(s) of data?

[redacted]

Richard Littlehale

From: Richard Littlehale
Sent: Sunday, January 29, 2017 6:47 PM
To: Richman, Daniel C. (DO) (OGA)
Cc: Cofield, Valerie M. (DO) (FBI)
Subject: Re: pew report on encryption attitudes

Copy that, I defer to your superior command of acronyms...I'm curious about the purpose behind the reporting requirements..."safeguard of liberty" vs. "administrative tracking" if anyone wrote about it at the time

To your point: I think in their world, all of those exploits will be fed into a robust civilian vulnerabilities equities process which will keep an eye on us, and then money and new exploits will magically appear to replace them...

Richard W. Littlehale
Special Agent in Charge
Criminal Investigation Division
Tennessee Bureau of Investigation

901 R.S. Gass Boulevard
Nashville, TN 37216

Desk [REDACTED]

Fax [REDACTED]
[REDACTED]

b6 -2
b7C -2
b7E -3

On Jan 29, 2017, at 1:35 PM, Richman, Daniel C. (DO) (OGA) <[REDACTED]> wrote:

Since I don't know much about the reporting protocol, I'll let Val bring people from OEO or EAOUSA to address this issue. But, not to be nasty, but do those making this argument realize that increased reliance on vulnerability exploitation will likely push the system even further from transparency?

From: Richard Littlehale [REDACTED]
Sent: Sunday, January 29, 2017 10:08 AM
To: Richman, Daniel C. (DO) (OGA); Cofield, Valerie M. (DO) (FBI)
Subject: RE: pew report on encryption attitudes

b6 -2
b7C -2

Sorry to bother you everyone over the weekend, but I thought I would send this before hopping on my flight to San Jose to beard the lion in his den. As time permits next week, I'd be interested in your thoughts about how to discuss what it is becoming increasingly clear to me will be a central talking point in the next phase of the encryption conversation, from the other side at least -- perceived problems with the wiretap reports to the USAOC.

FBI 18-CV-1833-7658

<https://cyberlaw.stanford.edu/blog/2017/01/wiretap-reports-not-so-transparent>

Al Gidari has fired the opening salvo – a drum he has been beating for some time now –but the Keys Under Doormats folks see this as a way to challenge the Going Dark narrative...

My guess is it is going to run something like this: what is the government hiding? Why don't reported wiretaps match up with service provider disclosures? Why aren't some agencies reporting? If they can't be trusted to comply with a simple public disclosure requirement, how can we trust them with the keys to encryption?

Richard W. Littlehale

Special Agent in Charge
Technical Services Unit

Criminal Investigation Division
Tennessee Bureau of Investigation

<image001.png>

901 R.S. Gass Boulevard

Nashville, TN 37216

Desk [REDACTED]

Fax [REDACTED]

[REDACTED]

b6 -2
b7C -2

From: Richman, Daniel C. (DO) (OGA) [mailto:[REDACTED]]
Sent: Friday, January 27, 2017 12:28 PM
To: Richard Littlehale [REDACTED]; Cofield, Valerie M. (DO) (FBI)
[REDACTED]

b6 -2
b7C -2
b7E -3

FBI 18-CV-1833-7659

Subject: Re: pew report on encryption attitudes

good code as speech article attached. By the now dean of Yale Law School

From: Richard Littlehale [redacted]
Sent: Friday, January 27, 2017 12:33 PM
To: Richman, Daniel C. (DO) (OGA); Cofield, Valerie M. (DO) (FBI)
Subject: RE: pew report on encryption attitudes

b6 -2
b7C -2

While I'm thinking of it, anything I should add to my reading list as I head out to Silicon Valley?

Dan, in particular, any suggestions on the best way to get current on the "code as speech" case law?

I'll keep you posted...

Richard W. Littlehale

Special Agent in Charge
Technical Services Unit

Criminal Investigation Division
Tennessee Bureau of Investigation

<image001.png>

901 R.S. Gass Boulevard

Nashville, TN 37216

Desk [redacted]

Fax [redacted]

[redacted]

b6 -2
b7C -2

From: Richman, Daniel C. (DO) (OGA) [mailto:[redacted]]
Sent: Thursday, January 26, 2017 3:22 PM

b7E -3

FBI 18-CV-1833-7660

To: Cofield, Valerie M. (DO) (FBI)

Richard Littlehale

b6 -2

b7C -2

b7E -3

Subject: pew report on encryption attitudes

*** This is an EXTERNAL email. Please exercise caution. DO NOT open attachments or click links from unknown senders or unexpected email - STS Security. ***

Dear Val, Rich and Kenn -- in case you missed it, attached is the Pew report on attitudes re cyber. PP. 27-28 is on encryption

dan r

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)

Sent: Thursday, February 02, 2017 3:08 PM

To: [REDACTED] (DO) (OGA); Littlehale, Richard; Cofield, Valerie M. (DO) (FBI);

b6 -1,2
b7C -1,2

Subject: new [REDACTED] draft on encryption

Attachments: Encryption WorkaroundsJanDraft.pdf

Attached is a draft on encryption work arounds that [REDACTED] just sent me. It's preliminary and can't be quoted but [REDACTED] is OK with my sharing it with you and would love to hear your comments.

I've not read it and can't yet comment on its quality etc. But since so many courts look to [REDACTED] work for guidance, this is worth reading regardless

dan r

[redacted] (DO) (OGA)

b6 -1,2
b7C -1,2

From: [redacted] (DO) (OGA)
Sent: Thursday, February 02, 2017 3:10 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: new [redacted] draft on encryption

Would you be okay if I shared with CCIPS? (Happy to keep it to us if not.)

From: Richman, Daniel C. (DO) (OGA)
Sent: Thursday, February 02, 2017 3:08 PM

To: [redacted] (DO) (OGA) [redacted] Littlehale, Richard

b6 -1,2
b7C -1,2
b7E -3

[redacted] Cofield, Valerie M. (DO) (FBI) [redacted]

Subject: new [redacted] draft on encryption

Attached is a draft on encryption work arounds that [redacted] just sent me. It's preliminary and can't be quoted but [redacted] is OK with my sharing it with you and would love to hear your comments. I've not read it and can't yet comment on its quality etc. But since so many courts look to [redacted] work for guidance, this is worth reading regardless
dan r

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Thursday, February 02, 2017 3:15 PM
To: [REDACTED] (DO) (OGA)
Subject: Re: new [REDACTED] draft on encryption

b6 -1,2
b7C -1,2

more than happy. And they really should feel free to pass on comments thru me to [REDACTED]

From: [REDACTED] (DO) (OGA)
Sent: Thursday, February 2, 2017 3:09 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: new [REDACTED] draft on encryption

b6 -1,2
b7C -1,2

Would you be okay if I shared with CCIPS? (Happy to keep it to us if not.)

From: Richman, Daniel C. (DO) (OGA)
Sent: Thursday, February 02, 2017 3:08 PM
To: [REDACTED] (DO) (OGA) [REDACTED] Littlehale, Richard
[REDACTED] Cofield, Valerie M. (DO) (FBI) [REDACTED]
[REDACTED]
Subject: new [REDACTED] draft on encryption

b6 -1,2
b7C -1,2
b7E -3

Attached is a draft on encryption work arounds that [REDACTED] just sent me. It's preliminary and can't be quoted but [REDACTED] is OK with my sharing it with you and would love to hear your comments. I've not read it and can't yet comment on its quality etc. But since so many courts look to [REDACTED] work for guidance, this is worth reading regardless
dan r

[redacted] (DO) (OGA)

b6 -1,2
b7C -1,2

From: [redacted] (DO) (OGA)
Sent: Thursday, February 02, 2017 3:15 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: new [redacted] draft on encryption

Great, I'll let them know.

From: Richman, Daniel C. (DO) (OGA)
Sent: Thursday, February 02, 2017 3:15 PM
To: [redacted] (DO) (OGA) [redacted]
Subject: Re: new [redacted] draft on encryption

b6 -1,2
b7C -1,2
b7E -3

more than happy. And they really should feel free to pass on comments thru me to [redacted]

From: [redacted] (DO) (OGA)
Sent: Thursday, February 2, 2017 3:09 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: new [redacted] draft on encryption

b6 -1,2
b7C -1,2

Would you be okay if I shared with CCIPS? (Happy to keep it to us if not.)

From: Richman, Daniel C. (DO) (OGA)
Sent: Thursday, February 02, 2017 3:08 PM
To: [redacted] (DO) (OGA) [redacted] littlehale, Richard
[redacted] Cofield, Valerie M. (DO) (FBI) [redacted]
[redacted]
Subject: new [redacted] draft on encryption

b6 -1,2
b7C -1,2
b7E -3

Attached is a draft on encryption work arounds that [redacted] just sent me. It's preliminary and can't be quoted but [redacted] is OK with my sharing it with you and would love to hear your comments. I've not read it and can't yet comment on its quality etc. But since so many courts look to [redacted] work for guidance, this is worth reading regardless
dan r

[redacted] (DO) (FBI)

b6 -1
b7C -1

From: [redacted] (DO) (FBI)
Sent: Friday, February 03, 2017 9:35 AM
To: Rybicki, James E. (DO) (FBI)
Cc: Richman, Daniel C. (DO) (OGA); [redacted] (DO) (FBI)
Subject: Professor Richman's contact(s)

Mr. Rybicki: good morning. Would you happen to have a way for me to contact Professor Richman today (e.g., an alternative email from the one CCed or possibly his phone number)?

I checked first with OGC's [redacted] but she only had his Bureau contact info. I also fully understand if you have such info, but would prefer to forward my name/number so Prof. Richman can call me at his convenience if he prefers. He contacted our office last Friday (1/27) on a matter which required a bit of research and discussion with OIC AD Kelley. We did so last night, and I was hoping to relay some initial thoughts, and follow-up with an email from which he wrote.

b6 -1
b7C -1

My final request and related question. Do you happen to know how many days Prof. Richman has worked for the FBI in the last 365 days (e.g., from 1/27/2016 to 2017)? Specifically, it's important to know whether it was more than 60 days? Even if only for one hour, that would count as a day.

The context is that, as you know, Prof. Richman is a Special Government Employee (SGE). There are conflict of interest laws, 18 U.S.C. §§ 203 and 205 regarding representational services on matters affecting the Government, which apply to all FBI employees. However, those statutes apply differently to SGEs. I'll gladly elaborate as necessary. Meanwhile, I was hoping to talk with Prof. Richman at his convenience, although the matter can wait until next week.

Thank you for your time and any available assistance.

[redacted]

[redacted]

Chief, Ethics and Integrity Unit (EIU)
Office of Integrity and Compliance (OIC)

Desk: [redacted]; Mobile: [redacted]

b6 -1
b7C -1
b7E -3

Richard Littlehale

From: Richard Littlehale
Sent: Friday, February 03, 2017 8:48 AM
To: Richman, Daniel C. (DO) (OGA); Cofield, Valerie M. (DO) (FBI)
Subject: [REDACTED] 2.0

Good morning! Fresh back from Silicon Valley, where efforts to convert me to pro-crypto absolutism have once again failed...

Here is the next [REDACTED] and then some:
[https://en.wikipedia.org/wiki/\[REDACTED\]](https://en.wikipedia.org/wiki/[REDACTED])

b6 -2
b7C -2

Some history. [REDACTED] was apparently the guy who developed the [REDACTED] crypto used back in the day for [REDACTED]. back then, as he anticipates now, he experienced some backlash.

Interesting perspective. [REDACTED] basically says that we can secure exceptional access mechanisms for all three categories (devices, real-time, and messaging) through the mechanism used for software updates. He says that the companies would act as the gatekeeper, so law enforcement wouldn't have independent access (in other words, it would be like CALEA). He says it would not degrade security at all.

So, game change...but [REDACTED] says he only wants to talk about this because he thinks that the absolutist position taken by his colleagues is wrong. So, if asked formally, at this point he will basically say "this is technically just fine, but I'm not convinced we should do it as a policy matter." I'm going to work on that with him...

Nobody had a direct challenge...everyone who heard it, including the EFF, basically said "well, we'll have to take a look and let you know". That said, everyone at this meeting, whatever their perspective, is asking the question "does the new administration change the way I feel" -- so, we may have a rough time getting talks to continue at a productive level.

I'm going to reach out to [REDACTED] after the fact and take his comfort level on talking to the law enforcement community, but we talked briefly after the presentation, and he said he was perfectly willing to chat about things.

I would love to have seen what he would have said in that room at Columbia...

RWL

From: Richman, Daniel C. (DO) (OGA) [mailto:[REDACTED]]
Sent: Sunday, January 29, 2017 3:34 PM
To: Richard Littlehale [REDACTED]; Cofield, Valerie M. (DO) (FBI)
[REDACTED]
Subject: Re: pew report on encryption attitudes

b6 -2
b7C -2
b7E -3

Since I don't know much about the reporting protocol, I'll let Val bring people from OEO or EAOUSA to address this issue. But, not to be nasty, but do those making this argument realize that increased reliance on vulnerability exploitation will likely push the system even further from transparency?

FBI 18-CV-1833-7672

From: Richard Littlehale [REDACTED]
Sent: Sunday, January 29, 2017 10:08 AM
To: Richman, Daniel C. (DO) (OGA); Cofield, Valerie M. (DO) (FBI)
Subject: RE: pew report on encryption attitudes

b6 -2
b7C -2

Sorry to bother you everyone over the weekend, but I thought I would send this before hopping on my flight to San Jose to beard the lion in his den. As time permits next week, I'd be interested in your thoughts about how to discuss what it is becoming increasingly clear to me will be a central talking point in the next phase of the encryption conversation, from the other side at least -- perceived problems with the wiretap reports to the USAOC.

<https://cyberlaw.stanford.edu/blog/2017/01/wiretap-reports-not-so-transparent>

Al Gidari has fired the opening salvo -- a drum he has been beating for some time now --but the Keys Under Doormats folks see this as a way to challenge the Going Dark narrative...

My guess is it is going to run something like this: what is the government hiding? Why don't reported wiretaps match up with service provider disclosures? Why aren't some agencies reporting? If they can't be trusted to comply with a simple public disclosure requirement, how can we trust them with the keys to encryption?

Richard W. Littlehale
Special Agent in Charge
Technical Services Unit
Criminal Investigation Division
Tennessee Bureau of Investigation



901 R.S. Gass Boulevard
Nashville, TN 37216

Desk [REDACTED]
Fax [REDACTED]
[REDACTED]

b6 -2
b7C -2

From: Richman, Daniel C. (DO) (OGA) [mailto:[REDACTED]]
Sent: Friday, January 27, 2017 12:28 PM
To: Richard Littlehale [REDACTED]; Cofield, Valerie M. (DO) (FBI)
[REDACTED]
Subject: Re: pew report on encryption attitudes

b6 -2
b7C -2
b7E -3

good code as speech article attached. By the now dean of Yale Law School

From: Richard Littlehale [REDACTED]
Sent: Friday, January 27, 2017 12:33 PM
To: Richman, Daniel C. (DO) (OGA); Cofield, Valerie M. (DO) (FBI)
Subject: RE: pew report on encryption attitudes

b6 -2
b7C -2

While I'm thinking of it, anything I should add to my reading list as I head out to Silicon Valley?

FBI 18-CV-1833-7673

Dan, in particular, any suggestions on the best way to get current on the "code as speech" case law?

I'll keep you posted...

Richard W. Littlehale
Special Agent in Charge
Technical Services Unit
Criminal Investigation Division
Tennessee Bureau of Investigation



901 R.S. Gass Boulevard
Nashville, TN 37216

Desk [REDACTED]

Fax [REDACTED]

[REDACTED]

b6 -2
b7C -2

From: Richman, Daniel C. (DO) (OGA) [mailto:[REDACTED]]
Sent: Thursday, January 26, 2017 3:22 PM
To: Cofield, Valerie M. (DO) (FBI) [REDACTED]; Richard Littlehale
[REDACTED]
Subject: pew report on encryption attitudes

b6 -2
b7C -2
b7E -3

*** This is an EXTERNAL email. Please exercise caution. DO NOT open attachments or click links from unknown senders or unexpected email - STS-Security. ***

Dear Val, Rich and Kenn -- in case you missed it, attached is the Pew report on attitudes re cyber. PP. 27-28 is on encryption

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Friday, February 03, 2017 12:52 PM
To: Littlehale, Richard; Cofield, Valerie M. (DO) (FBI); [REDACTED] (DO) (OGA) b6 -1,2
Subject: Re: [REDACTED] 2.0 b7C -1,2

completely interesting! Please keep us posted. Maybe we'll need to arrange a small workshop for him with some small crypto group

From: Richard Littlehale [REDACTED]
Sent: Friday, February 3, 2017 8:48 AM
To: Richman, Daniel C. (DO) (OGA); Cofield, Valerie M. (DO) (FBI)
Subject: [REDACTED] 2.0

b6 -2
b7C -2

Good morning! Fresh back from Silicon Valley, where efforts to convert me to pro-crypto absolutism have once again failed...

Here is the next [REDACTED] and then some:
[https://en.wikipedia.org/wiki/\[REDACTED\]](https://en.wikipedia.org/wiki/[REDACTED])

b6 -2
b7C -2

Some history [REDACTED] was apparently the guy who developed the [REDACTED] crypto used back in the day for [REDACTED]. back then, as he anticipates now, he experienced some backlash.

Interesting perspective [REDACTED] basically says that we can secure exceptional access mechanisms for all three categories (devices, real-time, and messaging) through the mechanism used for software updates. He says that the companies would act as the gatekeeper, so law enforcement wouldn't have independent access (in other words, it would be like CALEA). He says it would not degrade security at all.

So, game change...but [REDACTED] says he only wants to talk about this because he thinks that the absolutist position taken by his colleagues is wrong. So, if asked formally, at this point he will basically say "this is technically just fine, but I'm not convinced we should do it as a policy matter." I'm going to work on that with him...

Nobody had a direct challenge...everyone who heard it, including the EFF, basically said "well, we'll have to take a look and let you know". That said, everyone at this meeting, whatever their perspective, is asking the question "does the new administration change the way I feel" - so, we may have a rough time getting talks to continue at a productive level.

I'm going to reach out to [REDACTED] after the fact and take his comfort level on talking to the law enforcement community, but we talked briefly after the presentation, and he said he was perfectly willing to chat about things.

I would love to have seen what he would have said in that room at Columbia...

RWL

From: Richman, Daniel C. (DO) (OGA) [mailto:[REDACTED]]
Sent: Sunday, January 29, 2017 3:34 PM

b7E -3

FBI 18-CV-1833-7677

To: Richard Littlehale [REDACTED] Cofield, Valerie M. (DO) (FBI)

b6 -2

b7C -2

b7E -3

Subject: Re: pew report on encryption attitudes

Since I don't know much about the reporting protocol, I'll let Val bring people from OEO or EAOUSA to address this issue. But, not to be nasty, but do those making this argument realize that increased reliance on vulnerability exploitation will likely push the system even further from transparency?

From: Richard Littlehale [REDACTED]

b6 -2

b7C -2

Sent: Sunday, January 29, 2017 10:08 AM

To: Richman, Daniel C. (DO) (OGA); Cofield, Valerie M. (DO) (FBI)

Subject: RE: pew report on encryption attitudes

Sorry to bother you everyone over the weekend, but I thought I would send this before hopping on my flight to San Jose to beard the lion in his den. As time permits next week, I'd be interested in your thoughts about how to discuss what it is becoming increasingly clear to me will be a central talking point in the next phase of the encryption conversation, from the other side at least - perceived problems with the wiretap reports to the USAOC.

<https://cyberlaw.stanford.edu/blog/2017/01/wiretap-reports-not-so-transparent>

Al Gidari has fired the opening salvo - a drum he has been beating for some time now - but the Keys Under Doormats folks see this as a way to challenge the Going Dark narrative...

My guess is it is going to run something like this: what is the government hiding? Why don't reported wiretaps match up with service provider disclosures? Why aren't some agencies reporting? If they can't be trusted to comply with a simple public disclosure requirement, how can we trust them with the keys to encryption?

Richard W. Littlehale
Special Agent in Charge
Technical Services Unit
Criminal Investigation Division
Tennessee Bureau of Investigation



901 R.S. Gass Boulevard
Nashville, TN 37216

Desk [REDACTED]

Fax [REDACTED]
[REDACTED]

b6 -2

b7C -2

From: Richman, Daniel C. (DO) (OGA) [mailto:[REDACTED]]

b6 -2

b7C -2

b7E -3

Sent: Friday, January 27, 2017 12:28 PM

To: Richard Littlehale [REDACTED]; Cofield, Valerie M. (DO) (FBI)

Subject: Re: pew report on encryption attitudes

good code as speech article attached. By the now dean of Yale Law School

From: Richard Littlehale [REDACTED]
Sent: Friday, January 27, 2017 12:33 PM
To: Richman, Daniel C. (DO) (OGA); Cofield, Valerie M. (DO) (FBI)
Subject: RE: pew report on encryption attitudes

b6 -2
b7C -2

While I'm thinking of it, anything I should add to my reading list as I head out to Silicon Valley?

Dan, in particular, any suggestions on the best way to get current on the "code as speech" case law?

I'll keep you posted...

Richard W. Littlehale
Special Agent in Charge
Technical Services Unit
Criminal Investigation Division
Tennessee Bureau of Investigation



901 R.S. Gass Boulevard
Nashville, TN 37216
Des [REDACTED]
Fax [REDACTED]
[REDACTED]

From: Richman, Daniel C. (DO) (OGA) [mailto:[REDACTED]]
Sent: Thursday, January 26, 2017 3:22 PM
To: Cofield, Valerie M. (DO) (FBI) [REDACTED]; Richard Littlehale
[REDACTED]
Subject: pew report on encryption attitudes

b6 -2
b7C -2
b7E -3

*** This is an EXTERNAL email. Please exercise caution. DO NOT open attachments or click links from unknown senders or unexpected email - STS-Security. ***

Dear Val, Rich and Kenn -- in case you missed it, attached is the Pew report on attitudes re cyber. PP. 27-28 is on encryption

Richard Littlehale

From: Richard Littlehale
Sent: Friday, February 03, 2017 12:56 PM
To: Richman, Daniel C. (DO) (OGA); Cofield, Valerie M. (DO) (FBI); [REDACTED]
(DO) (OGA)
Subject: RE: [REDACTED] 2.0

b6 -1,2
b7C -1,2

Absolutely ...starting with [REDACTED] and [REDACTED] for example...I'll keep you posted...

Richard W. Littlehale
Special Agent in Charge
Technical Services Unit
Criminal Investigation Division
Tennessee Bureau of Investigation



901 R.S. Gass Boulevard
Nashville, TN 37216

Desk [REDACTED]

Fax [REDACTED]

From: Richman, Daniel C. (DO) (OGA) [mailto:[REDACTED]]
Sent: Friday, February 03, 2017 11:52 AM
To: Richard Littlehale [REDACTED]; Cofield, Valerie M. (DO) (FBI)
[REDACTED] (DO) (OGA) [REDACTED]
Subject: Re: [REDACTED] 2.0

b6 -1,2
b7C -1,2
b7E -3

completely interesting! Please keep us posted. Maybe we'll need to arrange a small workshop for him with some small crypto group

From: Richard Littlehale [REDACTED]
Sent: Friday, February 3, 2017 8:48 AM
To: Richman, Daniel C. (DO) (OGA); Cofield, Valerie M. (DO) (FBI)
Subject: [REDACTED] 2.0

b6 -2
b7C -2

Good morning! Fresh back from Silicon Valley, where efforts to convert me to pro-crypto absolutism have once again failed...

Here is the next [REDACTED] and then some:
[https://en.wikipedia.org/wiki/\[REDACTED\]](https://en.wikipedia.org/wiki/[REDACTED])

Some history [REDACTED] was apparently the guy who developed the [REDACTED] crypto used back in the day for [REDACTED] back then, as he anticipates now, he experienced some backlash.

Interesting perspective. [REDACTED] basically says that we can secure exceptional access mechanisms for all three categories (devices, real-time, and messaging) through the mechanism used for software updates. He says that the companies would act as the gatekeeper, so law enforcement wouldn't have independent access (in

other words, it would be like CALEA). He says it would not degrade security at all.

So, game change...but [redacted] says he only wants to talk about this because he thinks that the absolutist position taken by his colleagues is wrong. So, if asked formally, at this point he will basically say "this is technically just fine, but I'm not convinced we should do it as a policy matter." I'm going to work on that with him...

b6 -2
b7C -2

Nobody had a direct challenge...everyone who heard it, including the EFF, basically said "well, we'll have to take a look and let you know". That said, everyone at this meeting, whatever their perspective, is asking the question "does the new administration change the way I feel" – so, we may have a rough time getting talks to continue at a productive level.

I'm going to reach out to [redacted] after the fact and take his comfort level on talking to the law enforcement community, but we talked briefly after the presentation, and he said he was perfectly willing to chat about things.

I would love to have seen what he would have said in that room at Columbia...

RWL

From: Richman, Daniel C. (DO) (OGA) [mailto:[redacted]]
Sent: Sunday, January 29, 2017 3:34 PM
To: Richard Littlehale [redacted]; Cofield, Valerie M. (DO) (FBI)
[redacted] >
Subject: Re: pew report on encryption attitudes

b6 -2
b7C -2
b7E -3

Since I don't know much about the reporting protocol, I'll let Val bring people from OEO or EAOUSA to address this issue. But, not to be nasty, but do those making this argument realize that increased reliance on vulnerability exploitation will likely push the system even further from transparency?

From: Richard Littlehale [redacted]
Sent: Sunday, January 29, 2017 10:08 AM
To: Richman, Daniel C. (DO) (OGA); Cofield, Valerie M. (DO) (FBI)
Subject: RE: pew report on encryption attitudes

b6 -2
b7C -2

Sorry to bother you everyone over the weekend, but I thought I would send this before hopping on my flight to San Jose to beard the lion in his den. As time permits next week, I'd be interested in your thoughts about how to discuss what it is becoming increasingly clear to me will be a central talking point in the next phase of the encryption conversation, from the other side at least – perceived problems with the wiretap reports to the USAOC.

<https://cyberlaw.stanford.edu/blog/2017/01/wiretap-reports-not-so-transparent>

Al Gidari has fired the opening salvo – a drum he has been beating for some time now –but the Keys Under Doormats folks see this as a way to challenge the Going Dark narrative...

My guess is it is going to run something like this: what is the government hiding? Why don't reported wiretaps match up with service provider disclosures? Why aren't some agencies reporting? If they can't be trusted to comply with a simple public disclosure requirement, how can we trust them with the keys to encryption?

Richard W. Littlehale
Special Agent in Charge
Technical Services Unit
Criminal Investigation Division
Tennessee Bureau of Investigation



901 R.S. Gass Boulevard
Nashville, TN 37216

Desk [REDACTED]

Fax [REDACTED]
[REDACTED]

b6 -2
b7C -2

From: Richman, Daniel C. (DO) (OGA) [mailto:[REDACTED]]
Sent: Friday, January 27, 2017 12:28 PM
To: Richard Littlehale [REDACTED]; Cofield, Valerie M. (DO) (FBI)
[REDACTED]

b6 -2
b7C -2
b7E -3

Subject: Re: pew report on encryption attitudes

good code as speech article attached. By the now dean of Yale Law School

From: Richard Littlehale [REDACTED]
Sent: Friday, January 27, 2017 12:33 PM
To: Richman, Daniel C. (DO) (OGA); Cofield, Valerie M. (DO) (FBI)
Subject: RE: pew report on encryption attitudes

b6 -2
b7C -2

While I'm thinking of it, anything I should add to my reading list as I head out to Silicon Valley?

Dan, in particular, any suggestions on the best way to get current on the "code as speech" case law?

I'll keep you posted...

Richard W. Littlehale
Special Agent in Charge
Technical Services Unit
Criminal Investigation Division
Tennessee Bureau of Investigation



901 R.S. Gass Boulevard
Nashville, TN 37216

Desk [REDACTED]

Fax [REDACTED]
[REDACTED]

b6 -2
b7C -2

From: Richman, Daniel C. (DO) (OGA) [mailto:[REDACTED]]
Sent: Thursday, January 26, 2017 3:22 PM
To: Cofield, Valerie M. (DO) (FBI) [REDACTED]; Richard Littlehale

b7E -3

Subject: pew report on encryption attitudes

*** This is an EXTERNAL email. Please exercise caution. DO NOT open attachments or click links from unknown senders or unexpected email - STS-Security. ***

Dear Val, Rich and Kenn -- in case you missed it, attached is the Pew report on attitudes re cyber. PP. 27-28 is on encryption

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Friday, February 03, 2017 5:18 PM
To: Rybicki, James E. (DO) (FBI); [REDACTED] (DO) (OGA)
Subject: More hassles from/for your problem child

b6 -1
b7C -1

Just want to keep you both posted that I had a nice talk with [REDACTED] see below, about whether my policy work as an SGE precludes the (paid) consulting i've been asked to do (and have done a bit) on a criminal case out of the SDNY. I'm just helping a bit on the law side, but it's an interesting case.

[REDACTED] et al are looking into this, but he has expressed concern that an SGE, even one doing what I do, might not be able to work on any crim case that that the bu is involved in. (I'm not sure, but i think the bureau was involved in this case.) He noted that there is a waiver procedure, but didn't give me odds on my likelihood of success.

This is -- to use the bureaucratic expression a bummer: I'm really hoping that the unpaid/policy nature of my work will help me stay on the team as Going Dark starts moving to the front burner. Anything you guys can do to help me (1) act with complete propriety; (2) help you guys and (3) do some fun & well-paid work on unrelated matters would be greatly appreciated thx
d

From: [REDACTED] (DO) (FBI)
Sent: Friday, February 3, 2017 9:35 AM
To: Rybicki, James E. (DO) (FBI)
Cc: Richman, Daniel C. (DO) (OGA); [REDACTED] (DO) (FBI)
Subject: Professor Richman's contact(s)

b6 -1
b7C -1

Mr. Rybicki: good morning. Would you happen to have a way for me to contact Professor Richman today (e.g., an alternative email from the one CCed or possibly his phone number)?

I checked first with OGC's [REDACTED] but she only had his Bureau contact info. I also fully understand if you have such info, but would prefer to forward my name/number so Prof. Richman can call me at his convenience if he prefers. He contacted our office last Friday (1/27) on a matter which required a bit of research and discussion with OIC AD Kelley. We did so last night, and I was hoping to relay some initial thoughts, and follow-up with an email from which he wrote.

My final request and related question. Do you happen to know how many days Prof. Richman has worked for the FBI in the last 365 days (e.g., from 1/27/2016 to 2017)? Specifically, it's important to know whether it was more than 60 days? Even if only for one hour, that would count as a day.

The context is that, as you know, Prof. Richman is a Special Government Employee (SGE). There are conflict of interest laws, 18 U.S.C. §§ 203 and 205 regarding representational services on matters affecting the Government, which apply to all FBI employees. However, those statutes apply differently

FBI 18-CV-1833-7686

to SGEs. I'll gladly elaborate as necessary. Meanwhile, I was hoping to talk with Prof. Richman at his convenience, although the matter can wait until next week.

Thank you for your time and any available assistance.

[REDACTED]

b6 -1
b7C -1
b7E -3

[REDACTED]

Chief, Ethics and Integrity Unit (EIU)
Office of Integrity and Compliance (OIC)

Desk: [REDACTED] Mobile: [REDACTED]

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Friday, February 03, 2017 6:24 PM
To: [REDACTED] (DO) (OGA)
Subject: Re: More hassles from/for your problem child

b6 -1
b7C -1

Thanks. Have a lovely weekend.

I always see this weekend as adding an extra day to my life, 'cause i don't care about football (or any spectator sports)

From: [REDACTED] (DO) (OGA)
Sent: Friday, February 3, 2017 6:19 PM
To: Richman, Daniel C. (DO) (OGA); Rybicki, James E. (DO) (FBI)
Subject: RE: More hassles from/for your problem child

b6 -1
b7C -1

Dan--

I'll follow up on this next week.

[REDACTED]

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

From: Richman, Daniel C. (DO) (OGA)
Sent: Friday, February 03, 2017 5:18 PM
To: Rybicki, James E. (DO) (FBI); [REDACTED] (DO) (OGA)
[REDACTED]
Subject: More hassles from/for your problem child

b6 -1
b7C -1
b7E -3

Just want to keep you both posted that I had a nice talk with [REDACTED] see below, about whether my policy work as an SGE precludes the (paid) consulting i've been asked to do (and have done a bit) on a criminal case out of the SDNY. I'm just helping a bit on the law side, but it's an interesting case.

[REDACTED] et al are looking into this, but he has expressed concern that an SGE, even one doing what I do, might not be able to work on any crim case that that the bu is involved in. (I'm not sure, but i think the bureau was involved in this case.) He noted that there is a waiver procedure, but didn't give me odds on my likelihood of success.

This is -- to use the bureaucratic expression a bummer: I'm really hoping that the unpaid/policy nature of my work will help me stay on the team as Going Dark starts moving to the front burner. Anything you guys can do to help me (1) act with complete propriety; (2) help you guys and (3) do some fun & well-paid work on unrelated matters would be greatly appreciated thx d

From: [REDACTED] (DO) (FBI)
Sent: Friday, February 3, 2017 9:35 AM

b6 -1
b7C -1

FBI 18-CV-1833-7689

To: Rybicki, James E. (DO) (FBI)
Cc: Richman, Daniel C. (DO) (OGA); [REDACTED] (DO) (FBI)
Subject: Professor Richman's contact(s)

b6 -1
b7C -1

Mr. Rybicki: good morning. Would you happen to have a way for me to contact Professor Richman today (e.g., an alternative email from the one CCed or possibly his phone number)?

I checked first with OGC's [REDACTED] but she only had his Bureau contact info. I also fully understand if you have such info, but would prefer to forward my name/number so Prof. Richman can call me at his convenience if he prefers. He contacted our office last Friday (1/27) on a matter which required a bit of research and discussion with OIC AD Kelley. We did so last night, and I was hoping to relay some initial thoughts, and follow-up with an email from which he wrote.

My final request and related question. Do you happen to know how many days Prof. Richman has worked for the FBI in the last 365 days (e.g., from 1/27/2016 to 2017)? Specifically, it's important to know whether it was more than 60 days? Even if only for one hour, that would count as a day.

The context is that, as you know, Prof. Richman is a Special Government Employee (SGE). There are conflict of interest laws, 18 U.S.C. §§ 203 and 205 regarding representational services on matters affecting the Government, which apply to all FBI employees. However, those statutes apply differently to SGEs. I'll gladly elaborate as necessary. Meanwhile, I was hoping to talk with Prof. Richman at his convenience, although the matter can wait until next week.

Thank you for your time and any available assistance.

[REDACTED]

b6 -1
b7C -1
b7E -3

[REDACTED]

Chief, Ethics and Integrity Unit (EIU)

Office of Integrity and Compliance (OIC)

Desk: [REDACTED] Mobile: [REDACTED]

[redacted] (DO) (OGA)

b6 -1
b7C -1

From: [redacted] (DO) (OGA)
Sent: Friday, February 03, 2017 6:19 PM
To: Richman, Daniel C. (DO) (OGA); Rybicki, James E. (DO) (FBI)
Subject: RE: More hassles from/for your problem child

Dan--

I'll follow up on this next week.

[redacted]
-----Original Message-----

From: Richman, Daniel C. (DO) (OGA)
Sent: Friday, February 03, 2017 5:18 PM
To: Rybicki, James E. (DO) (FBI); [redacted] (DO) (OGA)
[redacted]
Subject: More hassles from/for your problem child

b6 -1
b7C -1
b7E -3

Just want to keep you both posted that I had a nice talk with [redacted] see below, about whether my policy work as an SGE precludes the (paid) consulting i've been asked to do (and have done a bit) on a criminal case out of the SDNY. I'm just helping a bit on the law side, but it's an interesting case.

[redacted] et al are looking into this, but he has expressed concern that an SGE, even one doing what I do, might not be able to work on any crim case that that the bu is involved in. (I'm not sure, but i think the bureau was involved in this case.) He noted that there is a waiver procedure, but didn't give me odds on my likelihood of success.

This is -- to use the bureaucratic expression a bummer: I'm really hoping that the unpaid/policy nature of my work will help me stay on the team as Going Dark starts moving to the front burner. Anything you guys can do to help me (1) act with complete propriety; (2) help you guys and (3) do some fun & well-paid work on unrelated matters would be greatly appreciated thx d

From: [redacted] (DO) (FBI)
Sent: Friday, February 3, 2017 9:35 AM
To: Rybicki, James E. (DO) (FBI)
Cc: Richman, Daniel C. (DO) (OGA); [redacted] (DO) (FBI)
Subject: Professor Richman's contact(s)

b6 -1
b7C -1

Mr. Rybicki: good morning. Would you happen to have a way for me to contact Professor Richman today (e.g., an alternative email from the one CCed or possibly his phone number)?

I checked first with OGC's [redacted] but she only had his Bureau contact info. I also fully

FBI 18-CV-1833-7691

understand if you have such info, but would prefer to forward my name/number so Prof. Richman can call me at his convenience if he prefers. He contacted our office last Friday (1/27) on a matter which required a bit of research and discussion with OIC AD Kelley. We did so last night, and I was hoping to relay some initial thoughts, and follow-up with an email from which he wrote.

My final request and related question. Do you happen to know how many days Prof. Richman has worked for the FBI in the last 365 days (e.g., from 1/27/2016 to 2017)? Specifically, it's important to know whether it was more than 60 days? Even if only for one hour, that would count as a day.

The context is that, as you know, Prof. Richman is a Special Government Employee (SGE). There are conflict of interest laws, 18 U.S.C. §§ 203 and 205 regarding representational services on matters affecting the Government, which apply to all FBI employees. However, those statutes apply differently to SGEs. I'll gladly elaborate as necessary. Meanwhile, I was hoping to talk with Prof. Richman at his convenience, although the matter can wait until next week.

Thank you for your time and any available assistance.

[Redacted]

b6 -1
b7C -1
b7E -3

[Redacted]

Chief, Ethics and Integrity Unit (EIU)

Office of Integrity and Compliance (OIC)

Desk: [Redacted] Mobile: [Redacted]

Richard Littlehale

From: Richard Littlehale
Sent: Friday, February 03, 2017 5:25 PM
To: Richman, Daniel C. (DO) (OGA); [REDACTED] (DO) (OGA); Cofield, Valerie M. (DO) (FBI); [REDACTED]
Subject: RE: new [REDACTED] draft on encryption

b6 -1,2
b7C -1,2

Just digging into this now, but this is a fantastic opportunity, thanks for passing along. As you say, lots of folks pay close attention to [REDACTED] scholarship, so I don't want to squander the opportunity for feedback.

Also, a long-dormant Bluebooking reflex has kicked in, but I'm going to keep that tamped down, because that is some other poor soul's problem this time around...

Richard W. Littlehale
Special Agent in Charge
Technical Services Unit
Criminal Investigation Division
Tennessee Bureau of Investigation



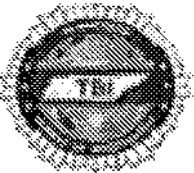
901 R.S. Gass Boulevard
Nashville, TN 37216
Desk [REDACTED]
Fax [REDACTED]
[REDACTED]

From: Richman, Daniel C. (DO) (OGA) [mailto:[REDACTED]]
Sent: Thursday, February 02, 2017 2:08 PM
To: [REDACTED] (DO) (OGA); [REDACTED] Richard Littlehale
[REDACTED] Cofield, Valerie M. (DO) (FBI) [REDACTED]
[REDACTED]
Subject: new [REDACTED] draft on encryption

b6 -1,2
b7C -1,2
b7E -3

*** This is an EXTERNAL email. Please exercise caution. DO NOT open attachments or click links from unknown senders or unexpected email - STS-Security. ***

Attached is a draft on encryption work arounds that [REDACTED] just sent me. It's preliminary and can't be quoted but [REDACTED] is OK with my sharing it with you and would love to hear your comments. I've not read it and can't yet comment on its quality etc. But since so many courts look to [REDACTED] work for guidance, this is worth reading regardless
dan r



[REDACTED] (DO) (OGA)

b6 -1
b7C -1

From: [REDACTED] (DO) (OGA)
Sent: Sunday, February 05, 2017 3:51 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: GD

If you're still considering long term GD staffing issues, you and Val Cofield should connect over the phone at some point soon so you can get a sense of the current challenges.

[redacted] (DO) (OGA)

b6 -1
b7C -1

From: [redacted] (DO) (OGA)
Sent: Friday, February 03, 2017 6:38 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: More hassles from/for your problem child

You too. The law is not a spectator sport.

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

From: Richman, Daniel C. (DO) (OGA)
Sent: Friday, February 03, 2017 6:24 PM
To: [redacted] (DO) (OGA) [redacted]
Subject: Re: More hassles from/for your problem child

b6 -1
b7C -1

Thanks. Have a lovely weekend.

I always see this weekend as adding an extra day to my life, 'cause i don't care about football (or any spectator sports) _____
From: [redacted] (DO) (OGA)
Sent: Friday, February 3, 2017 6:19 PM
To: Richman, Daniel C. (DO) (OGA); Rybicki, James E. (DO) (FBI)
Subject: RE: More hassles from/for your problem child

Dan--

I'll follow up on this next week.

[redacted]

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

From: Richman, Daniel C. (DO) (OGA)
Sent: Friday, February 03, 2017 5:18 PM
To: Rybicki, James E. (DO) (FBI) [redacted] (DO) (OGA)
[redacted]
Subject: More hassles from/for your problem child

b6 -1
b7C -1
b7E -3

Just want to keep you both posted that I had a nice talk with [redacted] see below, about whether my policy work as an SGE precludes the (paid) consulting i've been asked to do (and have done a bit) on a criminal case out of the SDNY. I'm just helping a bit on the law side, but it's an interesting case.

[redacted] et al are looking into this, but he has expressed concern that an SGE, even one doing what I do, might not be able to work on any crim case that that the bu is involved in. (I'm not sure, but i think the bureau was involved in this case.) He noted that there is a waiver procedure, but didn't give me odds on my likelihood of success.

This is -- to use the bureaucratic expression a bummer: I'm really hoping that the unpaid/policy nature of my work will help me stay on the team as Going Dark starts moving to the front burner. Anything you guys can do to help me (1) act with complete propriety; (2) help you guys and (3) do some fun & well-paid work on unrelated matters would be greatly appreciated thx d

FBI 18-CV-1833-7696

From: [REDACTED] (DO) (FBI)
Sent: Friday, February 3, 2017 9:35 AM
To: Rybicki, James E. (DO) (FBI)
Cc: Richman, Daniel C. (DO) (OGA); [REDACTED] (DO) (FBI)
Subject: Professor Richman's contact(s)

b6 -1
b7C -1

Mr. Rybicki: good morning. Would you happen to have a way for me to contact Professor Richman today (e.g., an alternative email from the one CCed or possibly his phone number)?

I checked first with OGC's [REDACTED] but she only had his Bureau contact info. I also fully understand if you have such info, but would prefer to forward my name/number so Prof. Richman can call me at his convenience if he prefers. He contacted our office last Friday (1/27) on a matter which required a bit of research and discussion with OIC AD Kelley. We did so last night, and I was hoping to relay some initial thoughts, and follow-up with an email from which he wrote.

My final request and related question. Do you happen to know how many days Prof. Richman has worked for the FBI in the last 365 days (e.g., from 1/27/2016 to 2017)? Specifically, it's important to know whether it was more than 60 days? Even if only for one hour, that would count as a day.

The context is that, as you know, Prof. Richman is a Special Government Employee (SGE). There are conflict of interest laws, 18 U.S.C. §§ 203 and 205 regarding representational services on matters affecting the Government, which apply to all FBI employees. However, those statutes apply differently to SGEs. I'll gladly elaborate as necessary. Meanwhile, I was hoping to talk with Prof. Richman at his convenience, although the matter can wait until next week.

Thank you for your time and any available assistance.

[REDACTED]

[REDACTED]

Chief, Ethics and Integrity Unit (EIU)
Office of Integrity and Compliance (OIC)

Desk: [REDACTED] Mobile: [REDACTED]

b6 -1
b7C -1
b7E -3

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Monday, February 06, 2017 10:16 AM
To: [REDACTED] (DO) (OGA)
Subject: Re: GD

b6 -1
b7C -1

i suspect you and I should talk first by phone, right?

From: [REDACTED] (DO) (OGA)
Sent: Sunday, February 5, 2017 3:50 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: GD

b6 -1
b7C -1

If you're still considering long term GD staffing issues, you and Val Cofield should connect over the phone at some point soon so you can get a sense of the current challenges.

[redacted] (DO) (OGA)

b6 -1
b7C -1

From: [redacted] (DO) (OGA)
Sent: Monday, February 06, 2017 10:18 AM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: GD

Feel free to give me a call----I'm around until 11:15 ish.

[redacted]
Special Counsel to the Director
Federal Bureau of Investigation
[redacted]

From: Richman, Daniel C. (DO) (OGA)
Sent: Monday, February 06, 2017 10:17 AM
To: [redacted] (DO) (OGA) [redacted]
Subject: Re: GD

b6 -1
b7C -1
b7E -3

i suspect you and I should talk first by phone, right?

From: [redacted] (DO) (OGA)
Sent: Sunday, February 5, 2017 3:50 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: GD

b6 -1
b7C -1

If you're still considering long term GD staffing issues, you and Val Cofield should connect over the phone at some point soon so you can get a sense of the current challenges.

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Monday, February 06, 2017 10:20 AM
To: [REDACTED] (DO) (OGA)
Subject: Re: GD

b6 -1
b7C -1

about to teach til 12. Would some time in the afternoon work?

From: [REDACTED] (DO) (OGA)
Sent: Monday, February 6, 2017 10:17 AM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: GD

b6 -1
b7C -1
b7E -3

Feel free to give me a call—I'm around until 11:15 ish.

[REDACTED]
Special Counsel to the Director
Federal Bureau of Investigation
[REDACTED]

From: Richman, Daniel C. (DO) (OGA)
Sent: Monday, February 06, 2017 10:17 AM
To: [REDACTED] (DO) (OGA) [REDACTED]
Subject: Re: GD

b6 -1
b7C -1
b7E -3

i suspect you and I should talk first by phone, right?

From: [REDACTED] (DO) (OGA)
Sent: Sunday, February 5, 2017 3:50 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: GD

If you're still considering long term GD staffing issues, you and Val Cofield should connect over the phone at some point soon so you can get a sense of the current challenges.

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Monday, February 06, 2017 12:11 PM
To: [REDACTED] (DO) (OGA)
Subject: Re: Crime Article

b6 -1
b7C -1

thx. Helpful

From: [REDACTED] (DO) (OGA)
Sent: Monday, February 6, 2017 11:24 AM
To: Richman, Daniel C. (DO) (OGA)
Subject: Crime Article

b6 -1
b7C -1

Thought you might find this interesting, given the CLR mini-symposium. (Seemed also to link to some interesting surveys, etc):

<http://www.latimes.com/local/california/la-me-lapd-crime-trust-20170203-story.html>

[REDACTED] (DO) (OGA)

b6 -1
b7C -1

From: [REDACTED] (DO) (OGA)
Sent: Monday, February 06, 2017 11:24 AM
To: Richman, Daniel C. (DO) (OGA)
Subject: Crime Article

Thought you might find this interesting, given the CLR mini-symposium. (Seemed also to link to some interesting surveys, etc):

<http://www.latimes.com/local/california/la-me-lapd-crime-trust-20170203-story.html>

[redacted] (DO) (OGA)

b6 -1
b7C -1
b7E -3

From: [redacted] (DO) (OGA)
Sent: Monday, February 06, 2017 4:25 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: GD

Accidentally dropped the call. Am around until 6 if you'd like to call back after your discussion with the ethics folks.

[redacted]

From: Richman, Daniel C. (DO) (OGA)
Sent: Monday, February 06, 2017 10:20 AM
To: [redacted] (DO) (OGA) [redacted]
Subject: Re: GD

b6 -1
b7C -1
b7E -3

about to teach til 12. Would some time in the afternoon work?

From: [redacted] (DO) (OGA)
Sent: Monday, February 6, 2017 10:17 AM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: GD

b6 -1
b7C -1
b7E -3

Feel free to give me a call—I'm around until 11:15 ish.

[redacted]
Special Counsel to the Director
Federal Bureau of Investigation
[redacted]

From: Richman, Daniel C. (DO) (OGA)
Sent: Monday, February 06, 2017 10:17 AM
To: [redacted] (DO) (OGA) [redacted]
Subject: Re: GD

b6 -1
b7C -1
b7E -3

i suspect you and I should talk first by phone, right?

From: [redacted] (DO) (OGA)
Sent: Sunday, February 5, 2017 3:50 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: GD

If you're still considering long term GD staffing issues, you and Val Cofield should connect over the

FBI 18-CV-1833-7703

phone at some point soon so you can get a sense of the current challenges.

[redacted] (DO) (OGA)

b6 -1
b7C -1

From: [redacted] (DO) (OGA)
Sent: Monday, February 06, 2017 2:35 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: GD

Yes, I'm around, except 3:30-4:00

From: Richman, Daniel C. (DO) (OGA)
Sent: Monday, February 06, 2017 10:20 AM
To: [redacted] (DO) (OGA) [redacted]
Subject: Re: GD

b6 -1
b7C -1

about to teach til 12. Would some time in the afternoon work?

From: [redacted] (DO) (OGA)
Sent: Monday, February 6, 2017 10:17 AM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: GD

b6 -1
b7C -1
b7E -3

Feel free to give me a call—I'm around until 11:15 ish.

[redacted]
Special Counsel to the Director
Federal Bureau of Investigation
[redacted]

From: Richman, Daniel C. (DO) (OGA)
Sent: Monday, February 06, 2017 10:17 AM
To: [redacted] (DO) (OGA) [redacted]
Subject: Re: GD

b6 -1
b7C -1
b7E -3

i suspect you and I should talk first by phone, right?

From: [redacted] (DO) (OGA)
Sent: Sunday, February 5, 2017 3:50 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: GD

If you're still considering long term GD staffing issues, you and Val Cofield should connect over the phone at some point soon so you can get a sense of the current challenges.

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Monday, February 06, 2017 4:26 PM
To: [REDACTED] (DO) (OGA)
Subject: Re: GD

b6 -1
b7C -1

i'll do that. Ugh

From: [REDACTED] (DO) (OGA)
Sent: Monday, February 6, 2017 4:25 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: GD

b6 -1
b7C -1
b7E -3

Accidentally dropped the call. Am around until 6 if you'd like to call back after your discussion with the ethics folks.

[REDACTED]

From: Richman, Daniel C. (DO) (OGA)
Sent: Monday, February 06, 2017 10:20 AM
To: [REDACTED] (DO) (OGA) [REDACTED]
Subject: Re: GD

b6 -1
b7C -1
b7E -3

about to teach til 12. Would some time in the afternoon work?

From: [REDACTED] (DO) (OGA)
Sent: Monday, February 6, 2017 10:17 AM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: GD

b6 -1
b7C -1
b7E -3

Feel free to give me a call—I'm around until 11:15 ish.

[REDACTED]
Special Counsel to the Director
Federal Bureau of Investigation
[REDACTED]

From: Richman, Daniel C. (DO) (OGA)
Sent: Monday, February 06, 2017 10:17 AM
To: [REDACTED] (DO) (OGA) [REDACTED]
Subject: Re: GD

b6 -1
b7C -1
b7E -3

i suspect you and I should talk first by phone, right?

FBI 18-CV-1833-7706

From: [REDACTED] (DO) (OGA)
Sent: Sunday, February 5, 2017 3:50 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: GD

b6 -1
b7C -1

If you're still considering long term GD staffing issues, you and Val Cofield should connect over the phone at some point soon so you can get a sense of the current challenges.

O'CONNELL, SASHA (DO) (FBI)

From: O'CONNELL, SASHA (DO) (FBI)
Sent: Tuesday, July 07, 2015 3:42 PM
To: RICHMAN, DANIEL C (DO)(OGA)
Cc: [REDACTED] (DO)(FBI)
Subject: Going Dark Documents [REDACTED] - UNCLASSIFIED
Attachments: 10.16.14 Director's Remarks for Brookings Institution PRESS VERSION.docx; Encryption_Public_Safety_and_Going_Dark.docx; Wall_Street_Journal_Article_4-20-2015.jpeg; SOR.Hess.4.29.15.Encryption.Cybersecurity.pdf; SFR AD Steinbach Committee on Homeland Security.pdf; Going Dark Initiative - AG Pres - Update - 0407 - 335 PM.pptx

b6 -1
b7C -1
b7E -1

Classification: UNCLASSIFIED
=====

TRANSITORY RECORD

To follow up on our meeting, I have attached a snapshot of documents for your reference. Also, the following is a link to the [REDACTED] which contains additional Going Dark documents from the past year: [REDACTED]

[REDACTED] If you have any trouble with [REDACTED] access please contact [REDACTED] from my office cc'd here. Please let me know if you need any additional information or background on the included documents. We very much look forward to working with you!

b6 -1
b7C -1
b7E -1,3

Going Dark Document Appendix

- 1) Director's Brookings Institute Speech
- 2) Director's Blog Article Lawfare
- 3) Executive Assistant Director of the Science and Technology Branch Amy Hess - WSJ Article
- 4) Congressional Statement for the Record - EAD Amy Hess
- 5) Congressional Statement for the Record - AD Steinbach
- 6) DOJ Attorney General Transition PowerPoint on Going Dark

<<10.16.14 Director's Remarks for Brookings Institution PRESS VERSION.docx>> <<Encryption_Public_Safety_and_Going_Dark.docx>> <<Wall_Street_Journal_Article_4-20-2015.jpeg>>
<<SOR.Hess.4.29.15.Encryption.Cybersecurity.pdf>> <<SFR AD Steinbach Committee on Homeland Security.pdf>> <<Going Dark Initiative - AG Pres - Update - 0407 - 335 PM.pptx>>

=====
Classification: UNCLASSIFIED

=====
Classification: UNCLASSIFIED

**Remarks Prepared for Delivery by James B. Comey
Director, Federal Bureau of Investigation
Going Dark: Are Technology, Privacy, and Public Safety
on a Collision Course?
Brookings Institution, Washington, D.C.
October 16, 2014**

Good morning. It's an honor to be here.

I have been on the job as FBI Director for one year and one month. I like to joke that I have eight years and 11 months to go, as if I'm serving time. But the truth is, I love this job, and I wake up every day excited to be part of the FBI.

Over the past year, I have confirmed what I long believed – that the FBI is filled with amazing people, doing an amazing array of things around the world, and doing them well. I have also confirmed what I have long known: that a commitment to the rule of law and civil liberties is at the center of the FBI. It is the Bureau's organizational spine.

But we confront serious threats – threats that are changing every day. So I want to make sure we have every tool we need to keep you safe from those threats.

An Opportunity to Begin a National Conversation

I wanted to meet with you to talk about the impact of emerging technology on public safety. And within that context, I think it's important to talk about the work we do in the FBI, and what we need to do the job you have entrusted us to do.

There are a lot of misconceptions in the public eye about what we in the government collect, and the capabilities we have for collecting that information.

My job is to explain and clarify where I can with regard to the work of the FBI. But at the same time, I want to get a better handle on your thoughts, because those of us in law enforcement can't do what we need to do without your trust and your support.

My goal today isn't to tell people what to do. My goal is to urge our fellow citizens to participate in a conversation about where we are, and where we want to be, with respect to the authority of law enforcement.

The Challenge of Going Dark

Technology has forever changed the world we live in. We're online, in one way or another, all day long. Our phones and computers have become reflections of our personalities, our interests, and our identities. They hold much that is important to us.

And with that comes a desire to protect our privacy and our data – you want to share your lives with the people you choose. I sure do. But the FBI has a sworn duty to keep every American safe from crime and terrorism, and technology has become the tool of choice for some very dangerous people.

Unfortunately, the law hasn't kept pace with technology, and this disconnect has created a significant public safety problem. We call it "Going Dark," and what it means is this: Those charged with protecting our people aren't always able to access the evidence we need to prosecute crime and prevent terrorism. We have the legal authority to intercept and access communications and information pursuant to court order, but we often lack the technical ability to do so.

We face two overlapping challenges. The first concerns real-time court-ordered interception of what we call "data in motion," such as phone calls, email and text messages, and chat sessions. The second challenge concerns court-ordered access to data stored on our devices, such as email, text messages, photos, and videos – or what we call "data at rest." And both real-time communication and stored data are increasingly encrypted.

Let's talk about court-ordered interception first.

In the past, conducting electronic surveillance was more straightforward. We identified a target phone being used by a bad guy, with a single carrier. We obtained a court order for a wiretap, and, under the supervision of a judge, we collected the evidence we needed for prosecution.

Today, there are countless providers, networks, and means of communicating. We have laptops, smart phones, and tablets. We take them to work and to school, from the soccer field to Starbucks, over many networks, using any number of apps. And so do those conspiring to harm us. They use the same devices, the same networks, and the same apps to make plans, to target victims, and to concoct cover-up stories. And that makes it tough for us to keep up.

If a suspected criminal is in his car, and he switches from cellular coverage to Wi-Fi, we may be out of luck. If he switches from one app to another, or from cellular voice service to a voice or messaging app, we may lose him. What if he has a kidnapped child in the car? We may not have the capability to quickly switch lawful surveillance between devices, methods, and networks. The bad guys know this; they're taking advantage of it every day.

In the wake of the Snowden disclosures, the prevailing view is that the government is sweeping up all of our communications. Of course, that's not true. And unfortunately, the idea that the government has access to all communications at all times has extended – unfairly – to the investigations of law enforcement agencies that obtain individual warrants, approved by judges, to intercept the communications of suspected criminals.

Some believe that the FBI has these phenomenal capabilities to access any information at any time – that we can get what we want, when we want it, by flipping some sort of switch. It may be true in the movies or on TV. It is simply not the case in real life.

It frustrates me, because I want people to understand that law enforcement needs to be able to access communications and information to bring people to justice. We do so pursuant to the rule of law, with clear guidance and strict oversight. But even with lawful authority, we may not be able to access the evidence and the information we need.

Current law governing the interception of communications requires telecommunication carriers and broadband providers to build interception capabilities into their networks for court-ordered surveillance. But that law, the Communications Assistance for Law Enforcement Act, or CALEA, was enacted 20 years ago – a lifetime in the Internet age. And it doesn't cover new means of communication. Thousands of companies provide some form of communication service, and most are not required by statute to provide lawful intercept capabilities to law enforcement.

What this means is that an order from a judge to monitor a suspect's communication may amount to nothing more than a piece of paper. Some companies fail to comply with the court order. Some can't comply, because they have not developed interception capabilities. Other providers want to provide assistance, but they have to build interception capabilities, and that takes time and money.

The issue is whether companies not currently subject to the Communications Assistance for Law Enforcement Act should be required to build lawful intercept capabilities for law enforcement. We aren't seeking to expand our authority to intercept communications. We are struggling to keep up with changing technology, and to maintain our ability to actually collect the communications we are authorized to intercept.

And if the challenges of real-time interception threaten to leave us in the dark, encryption threatens to lead all of us to a very dark place.

Encryption is nothing new. But the challenge to law enforcement and national security officials is markedly worse, with recent default encryption settings and encrypted devices and networks – all designed to increase security and privacy.

With Apple's new operating system, the information stored on many iPhones and other Apple devices will be encrypted by default. Shortly after Apple's announcement, Google announced plans to follow suit with its Android operating system. This means the companies themselves won't be able to unlock phones, laptops, and tablets to reveal photos, documents, email, and recordings stored within.

Both companies are run by good people, responding to what they perceive is a market demand. But the place they are leading us is one we shouldn't go to without careful thought and debate.

At the outset, Apple says it's not that big a deal. Apple argues, for example, that its users can back-up and store much of their data in "the cloud," and that the FBI can still access that data. But uploading to the cloud doesn't include all of the stored data on a bad guy's phone, which has the potential to create a black hole for law enforcement.

And if the bad guys don't back up their phones routinely, or if they opt out of uploading to the cloud, the data will only be found on the encrypted devices themselves. And it is people most worried about what's on the phone who will be most likely to avoid the cloud, and to make sure that law enforcement can't access incriminating data.

Encryption isn't just a technical feature; it's a marketing pitch. But it will have very serious consequences for law enforcement and national security agencies at every level. Sophisticated criminals will come to count on these means of evading detection. It's the equivalent of a closet that can't be opened. A safe that can't be cracked. And my question is, at what cost?

Correcting Misconceptions

Some argue that we will still have access to metadata, which includes telephone records and location information from telecommunications carriers. That is true. But metadata doesn't provide the content of any communication. It's incomplete information, and even this is difficult to access when time is of the essence. I wish we had time in our work, especially when lives are on the line. We usually don't.

There is a misconception that building a lawful intercept solution into a system requires a so-called "back door," one that foreign adversaries and hackers may try to exploit.

But that isn't true. We aren't seeking a back-door approach. We want to use the front door, with clarity and transparency, and with clear guidance provided by law. We are completely comfortable with court orders and legal process – front doors that provide the evidence and information we need to investigate crime and prevent terrorist attacks.

Cyber adversaries will exploit any vulnerability they find. But it makes more sense to address any security risks by developing intercept solutions during the design phase, rather than resorting to a patchwork solution when law enforcement comes knocking after the fact. And with sophisticated encryption, there might be no solution, leaving the government at a dead end – all in the name of privacy and network security.

Another misperception is that we can somehow guess the password or break into the phone with a so-called “brute force” attack. Even a supercomputer would have difficulty with today's high-level encryption, and some devices have a setting whereby the encryption key is erased if someone makes too many attempts to break the password, meaning no one can access that data.

Finally, a reasonable person might also ask, “Can't you just compel the owner of the phone to produce the password?” Likely, no. And even if we could, if we had a child predator in custody, and he could choose to sit quietly through a 30-day contempt sentence for failure to provide his password, or he could risk a 30-year sentence for production and distribution of child pornography, which do you think he would choose?

Case Examples

Think about life without your smartphone, without Internet access, without texting or email or the apps you use every day. I'm guessing most of you would feel rather lost and left behind. Kids call this FOMO, or “Fear of Missing Out.”

With Going Dark, those of us in law enforcement and public safety have a major fear of missing out – missing out on predators who exploit the most vulnerable among us ... missing out on violent criminals who target our communities ... missing out on a terrorist cell using social media to recruit, plan, and execute an attack.

Criminals and terrorists would like nothing more than for us to miss out. And the more we as a society rely on these devices, the more important they are to law enforcement and public safety officials. We have seen case after case – from homicides and car crashes to drug trafficking, domestic abuse, and child exploitation – where critical evidence came from smartphones, hard drives, and online communication.

Let's just talk about cases involving the content of phones.

In Louisiana, a known sex offender posed as a teenage girl to entice a 12-year-old boy to sneak out of his house to meet the supposed young girl. This predator, posing as a taxi driver, murdered the young boy, and tried to alter and delete evidence on both his and the victim's cell phones to cover up his crime. Both phones were instrumental in showing that the suspect enticed this child into his taxi. He was sentenced to death in April of this year.

In Los Angeles, police investigated the death of a two-year-old girl from blunt force trauma to her head. There were no witnesses. Text messages from the parents' cell phones to one another, and to their family members, proved the mother caused this young girl's death, and that the father knew what was happening and failed to stop it.

Text messages also proved that the defendants failed to seek medical attention for hours while their daughter convulsed in her crib. They even went so far as to paint her tiny body with blue paint – to cover her bruises – before calling 911. Confronted with this evidence, both parents pled guilty.

In Kansas City, the DEA investigated a drug trafficking organization tied to heroin distribution, homicides, and robberies. The DEA obtained search warrants for several phones used by the group. Text messages found on the phones outlined the group's distribution chain and tied the group to a supply of lethal heroin that had caused 12 overdoses – and five deaths – including several high school students.

In Sacramento, a young couple and their four dogs were walking down the street at night when a car ran a red light and struck them – killing their four dogs, severing the young man's leg, and leaving the young woman in critical condition. The driver left the scene, and the young man died days later.

Using "red light cameras" near the scene of the accident, the California Highway Patrol identified and arrested a suspect and seized his smartphone. GPS data on his phone placed the suspect at the scene of the accident, and revealed that he had fled California shortly thereafter. He was convicted of second-degree murder and is serving a sentence of 25 years-to-life.

The evidence we find also helps exonerate innocent people. In Kansas, data from a cell phone was used to prove the innocence of several teens accused of rape. Without access to this phone, or the ability to recover a deleted video, several innocent young men could have been wrongly convicted.

These are cases in which we had access to the evidence we needed. But we're seeing more and more cases where we believe significant evidence resides on a phone or a laptop, but we can't crack the password. If this becomes the norm, homicide cases could be stalled, suspects could walk free, and child exploitation victims might not be identified or recovered. Justice may be denied, because of a locked phone, or an encrypted hard drive.

My Thoughts

I'm deeply concerned about this, as both a law enforcement officer and a citizen. I understand some of this thinking in a post-Snowden world, but I believe it is mostly based on a failure to understand why we in law enforcement do what we do, and how we do it.

I hope you know, given my history, that I'm a huge believer in the rule of law. But I also believe that no one in this country is beyond the law. I like and believe very much that we need to follow the letter of the law to examine the contents of someone's closet or someone's smart phone. But the notion that the marketplace could create something that would prevent that closet from ever being opened, even with a properly obtained court order, makes no sense to me.

It might be time to ask: Where are we, as a society? Are we no longer a country governed by the rule of law, where no one is above or beyond that law? Are we so mistrustful of government – and of law enforcement – that we are willing to let bad guys walk away ... willing to leave victims in search of justice?

There will come a day – and it comes every day in this business – where it will matter a great deal to innocent people that we in law enforcement can't access certain types of data or information, even with legal authorization. We have to have these discussions now.

I believe people should be skeptical of unchecked government power. I am. This country was founded by people who were worried about government power, so they divided it among three branches, with checks and balances for each. And they wrote a Bill of Rights to ensure that the "papers and effects" of the people are secure from unreasonable searches.

But the way I see it, the means by which we conduct surveillance through telecommunication carriers and those Internet service providers who have developed lawful intercept solutions is an example of government operating in the way the framers intended – that is, the executive, the legislative, and the judicial branches proposing, enacting, executing, and overseeing legislation, pursuant to the rule of law.

Perhaps it's time to suggest that the post-Snowden pendulum has swung too far in one direction – in a direction of fear and mistrust. It is time to have open and honest debates about liberty and security.

Some have suggested there is a conflict between liberty and security. I disagree. At our best, we in law enforcement, national security, and public safety are looking for security that enhances liberty. When a city posts police officers at a dangerous playground, security has promoted liberty – the freedom to let a child play without fear.

The people of the FBI are sworn to protect both security and liberty. It isn't a question of conflict. We must care deeply about protecting liberty through due process of law, while also safeguarding the citizens we serve – in every investigation.

Where Do We Go From Here?

These are tough issues. And finding the space and time in our busy lives to understand these issues is hard. Intelligent people can and do disagree, and that's the beauty of American life.

I've never been someone who is a scaremonger. But I'm in a dangerous business. So I want to ensure that when we discuss limiting the court-authorized law enforcement tools we use to investigate suspected criminals that we understand what society gains, and what we all stand to lose.

We in the FBI will continue to throw every tool we have at this problem, but it's costly. It's inefficient. And it takes time – time we often do not have.

We need to fix this problem. It is long past time.

We need assistance and cooperation from companies to comply with lawful court orders, so that criminals around the world cannot seek safe haven for lawless conduct. We need to find common ground. We care about the same things. And we know an adversarial posture won't take any of us very far down the road.

We understand the private sector's need to remain competitive in the global marketplace. And it isn't our intent to stifle innovation or undermine U.S. companies. But we have to find a way to help these companies understand what we need, why we need it, and how they can help, while still protecting privacy rights and providing network security and innovation. We need our private sector partners to take a step back, to change course. We need them to do the right thing.

We also need a regulatory or legislative fix to create a level playing field, so that all communication service providers are held to the same standard, and so that those of us in law enforcement, national security, and public safety can continue to do the job you have entrusted us to do, in the way you would want us to.

Perhaps most importantly, we need to make sure the American public understands the work we do, and the means by which we do it.

I really do believe we can get there, with a reasoned and practical approach. And we have to get there together. I don't have the perfect solution. But I think it's important to start the discussion. I'm happy to work with Congress, with our partners in the private sector, with my law enforcement and national security counterparts, and with the people we serve, to find the right answer – to find the balance we need.

Thank you for having me here today.

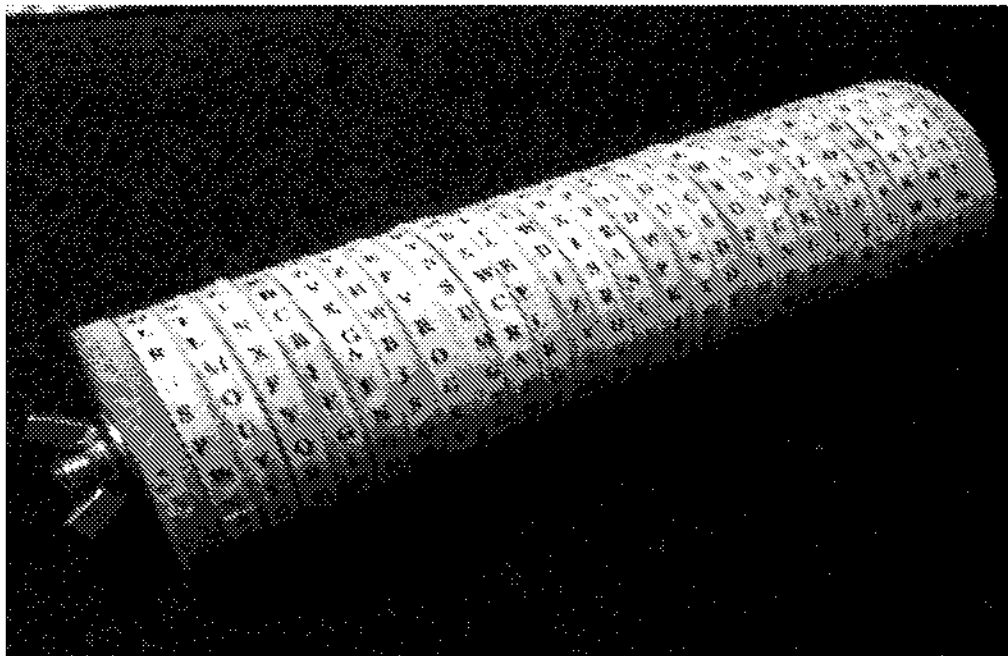
#

Encryption, Public Safety, and "Going Dark"

By James Comey

Monday, July 6, 2015, 10:38 AM

Google+
Reddit
LinkedIn



David Bruce

I am worried we are talking past each other with respect to "Going Dark," so let me try to frame it in a way that I hope is fair-minded and provides a basis for healthy discussion:

These are things I believe to be true:

1. The logic of encryption will bring us, in the not-to-distant future, to a place where devices and data in motion are protected by universal strong encryption. That is, our conversations and our "papers and effects" will be locked in such a way that permits access only by participants to a conversation or the owner of the device holding the data.
2. There are many benefits to this. Universal strong encryption will protect all of us—our innovation, our private thoughts, and so many other things of value—from thieves of all kinds. We will all have lock-boxes in our lives that only we can open and in which we can store all that is valuable to us. There are lots of good things about this.
3. There are many costs to this. Public safety in the United States has relied for a couple centuries on the ability of the government, with predication, to obtain permission from a court to access the "papers and effects" and communications of Americans. The Fourth Amendment reflects a trade-off inherent in ordered liberty: To protect the public, the government sometimes needs to be able to see an individual's stuff, but only under appropriate circumstances and with appropriate oversight.
4. These two things are in tension in many contexts. When the government's ability—with appropriate predication and court oversight—to see an individual's stuff goes away, it will affect public safety. That tension is vividly illustrated by the current ISIL threat, which involves ISIL operators in Syria recruiting and tasking dozens of troubled Americans to kill people, a process that increasingly takes part through mobile messaging apps that are end-to-end encrypted, communications that may not be intercepted, despite judicial orders under the Fourth Amendment. But the tension could as well be illustrated in criminal investigations all over the country. There is simply no doubt that bad people can communicate with impunity in a world of universal strong encryption.

5. Democracies resolve such tensions through robust debate. I really am not a maniac (or at least my family says so). But my job is to try to keep people safe. In universal strong encryption, I see something that is with us already and growing every day that will inexorably affect my ability to do that job. It may be that, as a people, we decide the benefits here outweigh the costs and that there is no sensible, technically feasible way to optimize privacy and safety in this particular context, or that public safety folks will be able to do their job well enough in the world of universal strong encryption. Those are decisions Americans should make, but I think part of my job is make sure the debate is informed by a reasonable understanding of the costs.



GOING DARK INITIATIVE AG OVERVIEW BRIEF

*An overview and discussion of the operational challenges for law enforcement
and DOJ/FBI way forward*

April 7, 2015

FBI 18-CV-1833-7721



Department of Justice

STATEMENT OF

**MICHAEL B. STEINBACH
ASSISTANT DIRECTOR
FEDERAL BUREAU OF INVESTIGATION**

BEFORE THE

**COMMITTEE ON HOMELAND SECURITY
U.S. HOUSE OF REPRESENTATIVES**

AT A HEARING ENTITLED

**“TERRORISM GONE VIRAL:
THE ATTACK IN GARLAND, TEXAS AND BEYOND”**

PRESENTED

JUNE 3, 2015



**Statement of
Michael B. Steinbach
Assistant Director
Federal Bureau of Investigation**

**Before the
Committee on Homeland Security
U.S. House of Representatives**

**At a Hearing Entitled
“Terrorism Gone Viral: The Attack in Garland, Texas and Beyond”**

**Presented
June 3, 2015**

Good morning Chairman McCaul, Ranking Member Thompson, and Members of the committee. Thank you for the opportunity to appear before you today to discuss the widespread reach of terrorists’ influence, which transcends geographic boundaries like never before. As technology advances so, too, does terrorists’ use of technology to communicate – both to inspire and recruit. The widespread use of technology propagates the persistent terrorist message to attack US interests whether in the Homeland or abroad. As the threat to harm Western interests evolves, we must adapt and confront the challenges, relying heavily on the strength of our federal, state, local, and international partnerships.

We continue to identify individuals who seek to join the ranks of foreign fighters traveling in support of the Islamic State of Iraq and the Levant, commonly known as ISIL, and also homegrown violent extremists who may aspire to attack the United States from within. These threats remain among the highest priorities for the FBI and the Intelligence Community as a whole.



Conflicts in Syria and Iraq continue to serve as the most attractive overseas theaters for Western-based extremists who want to engage in violence. We estimate upwards of 200 Americans have traveled or attempted to travel to Syria to participate in the conflict. While this number is lower in comparison to many of our international partners, we closely analyze and assess the influence groups like ISIL have on individuals located in the United States who are inspired to commit acts of violence. Whether or not the individuals are affiliated with a foreign terrorist organization and are willing to travel abroad to fight or are inspired by the call to arms to act in their communities, they potentially pose a significant threat to the safety of the United States and U.S. persons.

ISIL has proven relentless in its violent campaign to rule and has aggressively promoted its hateful message, attracting like-minded extremists to include Westerners. To an even greater degree than al-Qa'ida or other foreign terrorist organizations, ISIL has persistently used the internet to communicate. From a Homeland perspective, it is ISIL's widespread reach through the internet and social media which is most concerning as ISIL has aggressively employed this technology for its nefarious strategy. ISIL blends traditional media platforms, glossy photos, in-depth articles, and social media campaigns that can go viral in a matter of seconds. No matter the format, the message of radicalization spreads faster than we imagined just a few years ago.

Unlike other groups, ISIL has constructed a narrative that touches on all facets of life – from career opportunities, to family life, to a sense of community. The message isn't tailored solely to those who are overtly expressing symptoms of radicalization. It is seen by many who



click through the internet every day, receive social media push notifications, and participate in social networks. Ultimately, many of these individuals are seeking a sense of belonging.

As a communication medium, social media is a critical tool for terror groups to exploit. One recent example occurred last week. An individual was arrested for providing material support to ISIL by facilitating an associate's travel to Syria to join ISIL. The arrested individual had multiple connections, via a social media networking site, with other like-minded individuals.

As I've stated in previous opportunities I've had to testify before this committee, there is no set profile for the susceptible consumer of this propaganda. However, one trend continues to rise – the inspired youth. We've seen certain children and young adults drawing deeper into the ISIL narrative. These individuals are often comfortable with virtual communication platforms, specifically social media networks.

ISIL continues to disseminate their terrorist message to all social media users – regardless of age. Following other groups, ISIL has advocated for lone wolf attacks. In recent months ISIL released a video, via social media, reiterating the group's encouragement of lone offender attacks in Western countries, specifically advocating for attacks against soldiers and law enforcement, intelligence community members, and government personnel. Several incidents have occurred in the United States and Europe over the last few months that indicate this "call to arms" has resonated among ISIL supporters and sympathizers.

In one case, a Kansas-based male was arrested in April after he systematically carried out steps to attack a U.S. military institution and a local police station. The individual, who was



inspired by ISIL propaganda, expressed his support for ISIL online and took steps to carry out acts encouraged in the ISIL call to arms.

The targeting of U.S. military personnel is also evident with the release of hundreds of names of individuals serving in the U.S. military by ISIL supporters. The names were posted to the internet and quickly spread through social media, depicting ISIL's capability to produce viral messaging. Threats to U.S. military and coalition forces continue today.

Across the world, recent events commemorating ANZAC Day, a significant milestone in Australian and New Zealand military history, attracted unwanted attention that could have resulted in violence had Australian authorities not disrupted the plotting efforts underway. These arrests re-emphasize our need to remain vigilant in the Homeland against these small scale attacks.

We should also understand community and world events – as viewed through the eyes of a committed individual – may trigger action. As we've seen with recent highly publicized events, including the attack in Garland, Texas, these acts of terror will attract international media attention and may inspire "copy cat" attacks. The targeting of the Muhammad Art Exhibit and Contest exemplifies the call to arms approach encouraged by ISIL along with the power of viral messaging. In this instance, the event gained much publicity prior to it occurring and attracted negative attention that reached areas of the country – and the world – that it may not have without the widespread reach of the internet. The extensive network coupled with the magnetic messaging provides inspiration and validation that others share their outrage.



Lastly, social media has allowed groups, such as ISIL, to use the internet to spot and assess potential recruits. With the widespread horizontal distribution of social media, terrorists can identify vulnerable individuals of all ages in the United States – spot, assess, recruit and radicalize – either to travel or to conduct a Homeland attack. The foreign terrorist now has direct access into the United States like never before.

In recent arrests, a group of individuals was contacted by a known ISIL supporter who had already successfully traveled to Syria and encouraged them to do the same.

Some of these conversations occur in publicly accessed social networking sites, but others take place via private messaging platforms. As a result, it is imperative the FBI and all law enforcement organizations understand the latest communication tools and are positioned to identify and prevent terror attacks in the Homeland. We live in a technologically driven society and just as private industry has adapted to modern forms of communication so too have the terrorists. Unfortunately, changing forms of internet communication are quickly outpacing laws and technology designed to allow for the lawful intercept of communication content. This real and growing gap the FBI refers to as “Going Dark” is the source of continuing focus for the FBI, it must be urgently addressed as the risks associated with “Going Dark” are grave both in traditional criminal matters as well as in national security matters. We are striving to ensure appropriate, lawful collection remains available. Whereas traditional voice telephone companies are required by CALEA to develop and maintain capabilities to intercept communications when law enforcement has lawful authority, that requirement does not extend to most Internet communications services. As a result, such services are developed and deployed without any



ability for law enforcement to collect information critical to criminal and national security investigations and prosecutions.

The FBI, in partnership with the Department of Homeland Security, is utilizing all lawful investigative techniques and methods to combat the threat these individuals may pose to the United States. In conjunction with our domestic and foreign partners, we are rigorously collecting and analyzing intelligence information as it pertains to the ongoing threat posed by foreign terrorist organizations and homegrown violent extremists. In partnership with our many federal, state, and local agencies assigned to Joint Terrorism Task Forces around the country, we remain vigilant to ensure the safety of the American public. Be assured, the FBI continues to pursue increased efficiencies and information sharing processes as well as pursue technological and other methods to help stay ahead of threats to the Homeland.

Chairman McCaul, Ranking Member Thompson, and Committee Members, I thank you for the opportunity to testify concerning terrorists' use of the internet and social media as a platform for spreading ISIL propaganda and inspiring individuals to target the Homeland. I am happy to answer any questions you might have.



Department of Justice

STATEMENT OF

**AMY HESS
EXECUTIVE ASSISTANT DIRECTOR
FEDERAL BUREAU OF INVESTIGATION**

BEFORE THE

**SUBCOMMITTEE ON INFORMATION TECHNOLOGY
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
U.S. HOUSE OF REPRESENTATIVES**

CONCERNING

**ENCRYPTION AND CYBERSECURITY FOR
MOBILE ELECTRONIC COMMUNICATION DEVICES**

PRESENTED

APRIL 29, 2015

**Statement of
Amy Hess
Executive Assistant Director
Federal Bureau of Investigation**

**Before the
Subcommittee on Information Technology
Oversight and Government Reform
U.S. House of Representatives**

**Concerning
Encryption and Cybersecurity for
Mobile Electronic Communication Devices**

**Presented
April 29, 2015**

Good morning/afternoon, Chairman Hurd, Ranking Member Kelly, and members of the Subcommittee. Thank you for the opportunity to appear before the Committee today, and for your continued support of the men and women of the FBI.

Today's FBI

As you know, the Bureau has undergone unprecedented transformation in recent years to address and prevent threats to our national security and our public safety, from terrorism, state-sponsored espionage, and cyber security to violent gangs, transnational organized crime, and crimes against children.

As national security and criminal threats continue to evolve, so too must the FBI evolve to stay ahead of changing threats and changing technology. Today's FBI is a threat-focused, intelligence-driven organization. We must continually ask ourselves whether we are able to meet the challenges of the day, whatever they may be.

Online technology has forever changed the world we live in. We're online, in one form or another, all day long. Our phones and computers have become reflections of our personalities, our interests, and our identities. With this online presence comes the need to protect our privacy and the security of our data.

But, as with any technology, it can be used by some very dangerous people, and the FBI has a sworn duty to keep every American safe from crime and terrorism while simultaneously protecting their constitutional rights and preserving their civil liberties. Moreover, we recognize

our national interests in promoting innovation and the competitiveness of U.S. companies in the global marketplace, as well as freedom of expression around the world.

The evolution of technology is creating new challenges for law enforcement and our ability to access communications. We call it “Going Dark,” and it means that those charged with protecting the American people aren’t always able to access the information necessary to prosecute criminals and prevent terrorism even though we have lawful authority to do so. To be clear, we obtain the proper legal authority to intercept and access communications and information, but we increasingly lack the technical ability to do so. This problem is broader and more extensive than just encryption. But, for purposes of my testimony today, I will focus on the challenges we face based on the evolving use of encryption.

The issues law enforcement encounters with encryption occur in two overlapping contexts. The first concerns legally authorized real-time interception of what we call “data in motion,” such as phone calls, email, text messages and chat sessions in transit. The second challenge concerns legally authorized access to data stored on devices, such as email, text messages, photos, and videos – or what we call “data at rest.” Both data in motion and data at rest are increasingly encrypted.

Court-Ordered Interception of Encrypted Data in Motion

In the past, there were a limited number of communications carriers. As a result, conducting electronic surveillance was more straightforward. We identified a target phone being used by a suspected criminal, obtained a court order for a wiretap, and, under the supervision of a judge, collected the evidence we needed for prosecution.

Today, communications occur across countless providers, networks, and devices. We take our laptops, smart phones, and tablets to work and to school, from the soccer field to the coffee shop, traversing many networks, using any number of applications. And so, too, do those conspiring to harm us. They use the same devices, the same networks, and the same applications to make plans, to target victims, and to concoct cover-up stories.

Law enforcement and national security investigators need to be able to access communications and information to obtain the evidence necessary to prevent crime and bring criminals to justice in a court of law. We do so pursuant to the rule of law, with clear guidance and strict judicial oversight. But increasingly, even armed with a court order based on probable cause, we are too often unable to access potential evidence.

The Communications Assistance for Law Enforcement Act (CALEA) requires telecommunication carriers to be able to implement court orders for the purpose of intercepting

communications. But that law wasn't designed to cover many of the new means of communication that exist today. Currently, thousands of companies provide some form of communication service, but most do not have the ability to isolate and deliver particular information when ordered to do so by a court. Some have argued that access to metadata about these communications – which is not encrypted – should be sufficient for law enforcement. But metadata is incomplete information, and can be difficult to analyze when time is of the essence. It can take days to parse metadata into readable form, and additional time to correlate and analyze the data to obtain meaningful and actionable information.

Court-Ordered Access to Stored Encrypted Data

Encryption of stored data is not new, but it has become increasingly prevalent and sophisticated. The challenge to law enforcement and national security officials has intensified with the advent of default encryption settings and stronger encryption standards on both devices and networks.

In the past, a consumer had to decide whether to encrypt data stored on his or her device and take some action to implement that encryption. With today's new operating systems, however, a device and all of a user's information on that device can be encrypted by default – without any affirmative action by the consumer. In the past, companies had the ability to decrypt devices when the Government obtained a search warrant and a court order. Today, companies have developed encryption technology which makes it impossible for them to decrypt data on devices they manufacture and sell, even when lawfully ordered to do so. Although there are strong and appropriate cybersecurity and other reasons to support these new uses of encryption, such decisions regarding system design have a tremendous impact on law enforcement's ability to fight crime and bring perpetrators to justice.

Evidence of criminal activity used to be found in written ledgers, boxes, drawers, and file cabinets, all of which could be searched pursuant to a warrant. But like the general population, criminal actors are increasingly storing such information on electronic devices. If these devices are automatically encrypted, the information they contain may be unreadable to anyone other than the user of the device. Obtaining a search warrant for photos, videos, email, text messages, and documents can be an exercise in futility. Terrorists and other criminals know this and will increasingly count on these means of evading detection.

Additional Considerations

Some assert that although more and more devices are encrypted, users back-up and store much of their data in "the cloud," and law enforcement agencies can access this data pursuant to court order. For several reasons, however, the data may not be there. First, aside from the technical requirements and settings needed to successfully back up data to the cloud, many

companies impose fees to store information there – fees which consumers may be unwilling to pay. Second, criminals can easily avoid putting information where it may be accessible to law enforcement. Third, data backed up to the cloud typically includes only a portion of the data stored on a device, so key pieces of evidence may reside only on a criminal's or terrorist's phone, for example. And if criminals do not back up their phones routinely, or if they opt out of uploading to the cloud altogether, the data may only be found on the devices themselves – devices which are increasingly encrypted.

Facing the Challenge

The reality is that cyber adversaries will exploit any vulnerability they find. But security risks are better addressed by developing solutions during the design phase of a specific product or service, rather than resorting to a patchwork solution when law enforcement presents the company with a court order after the product or service has been deployed.

To be clear, we in the FBI support and encourage the use of secure networks and sophisticated encryption to prevent cyber threats to our critical national infrastructure, our intellectual property, and our data. We have been on the front lines of the fight against cybercrime and economic espionage and we recognize that absolute security does not exist in either the physical or digital world. Any lawful intercept or access solution should be designed to minimize its impact upon the overall security. But without a solution that enables law enforcement to access critical evidence, many investigations could be at a dead end. The same is true for cyber security investigations; if there is no way to access encrypted systems and data, we may not be able to identify those who seek to steal our technology, our state secrets, our intellectual property, and our trade secrets.

A common misperception is that we can simply break into a device using a “brute force” attack – the idea that with enough computing resources devoted to the task, we can defeat any encryption. But the reality is that even a supercomputer would have difficulty with today's high-level encryption standards. And some devices have a setting that erases the encryption key if someone makes too many attempts to break the password, effectively closing all access to that data.

Finally, a reasonable person might also ask, “Can't you just compel the owner of the device to produce the information in a readable form?” Even if we could compel an individual to provide this information, a suspected criminal would more likely choose to defy the court's order and accept a punishment for contempt rather than risk a 30-year sentence for, say, production and distribution of child pornography.

Without access to the right evidence, we fear we may not be able to identify and stop child predators hiding in the shadows of the Internet, violent criminals who are targeting our

neighborhoods, and terrorists who may be using social media to recruit, plan, and execute an attack in our country. We may not be able to recover critical information from a device that belongs to a victim who can't provide us with the password, especially when time is of the essence.

Examples

The more we as a society rely on electronic devices to communicate and store information, the more likely it is that evidence that was once found in filing cabinets, letters, and photo albums will now be available only in electronic storage. We have seen case after case – from homicides and kidnappings, to drug trafficking, financial fraud, and child exploitation – where critical evidence came from smart phones, computers, and online communications.

Each of the following examples demonstrates how important information stored on electronic devices can be to prosecuting criminals and stopping crime. As encryption solutions become increasingly inaccessible for law enforcement, it is cases like these that could go unsolved, and criminals like these that could go free.

As an example of the importance of lawful access to smart phones, consider the case involving a long-haul trucker who kidnapped his girlfriend, imprisoned her within his truck, drove her from State to State, and physically and sexually assaulted her along the way. The victim eventually leapt from the truck and escaped to nearby civilians, and later the police. The trucker refuted the charges and claimed the sexual activity was consensual. In this case, law enforcement obtained a search warrant for the trucker's smart phone, as well as a court order requiring the phone manufacturer's assistance to extract that data. Through this court-authorized process, law enforcement recovered video and images of the abuse stored on the smart phone, which were integral to corroborating the victim's testimony at trial. The trucker was convicted of kidnapping and interstate domestic violence at trial, and sentenced to life in prison.

Additionally, in a case investigated by a small Midwest police department, a woman reported that an unknown stranger forcibly raped her while she was out walking. She sought treatment at a local hospital where a sexual assault examination was performed. However, the investigator noted peculiarities in the woman's responses during the interview and requested access to her phone. She consented and, using forensic tools, the investigator uncovered evidence indicating the woman had sought out a stranger via an Internet advertisement with the intent to get pregnant. To cover her infidelity, she fabricated the story that a stranger had raped her. When confronted with the communications recovered from her phone, the woman admitted the rape report was false. Without the digital evidence, an innocent man may well have been accused of a violent sexual assault.

Another investigation in Clark County, Nevada, centered on allegations that a woman and her boyfriend conspired together to kill the woman's father who died after being stabbed

approximately 30 times. Text messages which had been deleted from the phone and recovered by investigators revealed the couple's plans in detail, clearly showing premeditation. Additionally, the communications around the time of the killing proved that both of them were involved throughout the process and during the entire event, resulting in both being charged with murder and conspiracy to commit murder.

Following a joint investigation conducted by the FBI and Indiana State Police, a pastor pleaded guilty in Federal court to transporting a minor across state lines with intent to engage in illicit sexual conduct in connection with his sexual relationship with an underage girl who was a student at the church's high school. During this investigation, information recovered from the pastor's smart phone proved to be crucial in showing the actions taken by the pastor in the commission of his crimes. Using forensic software, investigators identified Wi-Fi locations, dates, and times when the pastor traveled out of state to be with the victim. The analysis uncovered Internet searches including, "What is the legal age of consent in Indiana", "What is the legal age of consent in Michigan", and "Penalty for sexting Indiana." In addition, image files were located which depicted him in compromising positions with the victim.

These are examples of how important evidence that resides on smart phones and other devices can be to law enforcement – evidence that might not have been available to us had strong encryption been in place on those devices and the user's consent not granted.

The above examples serve to show how critical electronic evidence has become in the course of our investigations and how timely, reliable access to it is imperative to ensuring public safety. Today's encryption methods are increasingly more sophisticated, and pose an even greater challenge to law enforcement. We are seeing more and more cases where we believe significant evidence resides on a phone, a tablet, or a laptop – evidence that may be the difference between an offender being convicted or acquitted – but we cannot access it.

Previously, a company that manufactured a communications device could assist law enforcement in unlocking the device. Today, however, upon receipt of a lawful court order, the company might only be able to provide information that was backed up in the cloud – and there is no guarantee such a backup exists, that the data is current, or that it would be relevant to the investigation. If this becomes the norm, it will be increasingly difficult for us to investigate and prevent crime and terrorist threats.

Civil Liberties and the Rule of Law

Just as we have an obligation to address threats to our national security and our public safety, we also have an obligation to consider the potential impact of our investigations on civil liberties, including the right to privacy.

Intelligence and technology are key tools we use to stay ahead of those who would do us harm. Yet, as we evolve and adapt our investigative techniques and our use of technology to keep pace with today's complex threat environment, we must always act within the confines of the rule of law and the safeguards guaranteed by the Constitution.

The people of the FBI are sworn to protect both security and liberty. We care deeply about protecting liberty – including an individual's right to privacy through due process of law – while simultaneously protecting this country and safeguarding the citizens we serve.

The rule of law is our true north; it is the guiding principle for all that we do. The world around us continues to change, but within the FBI, our values must never change. Every FBI employee takes an oath promising to uphold the United States Constitution. It is not enough to catch the criminals; we must do so while upholding civil rights. It is not enough to stop the terrorists; we must do so while maintaining civil liberties. It is not enough to prevent foreign nations from stealing our secrets; we must do so while upholding the rule of law.

Following the rule of law and upholding civil liberties and civil rights are not burdens. They are what make all of us safer and stronger. In the end, we in the FBI will be judged not only by our ability to keep Americans safe from crime and terrorism, but also by whether we safeguard the liberties for which we are fighting and maintain the trust of the American people.

And with the rule of law as our guiding principle, we also believe that no one in this country should be beyond the law. We must follow the letter of the law, whether examining the contents of a suspected individual's closet or the contents of her smart phone. But the notion that the closet could never be opened – or that the phone could never be unlocked or unencrypted – even with a properly obtained court order, is troubling.

Are we as a society comfortable knowing that certain information is no longer available to law enforcement under any circumstances? Is there no way to reconcile personal privacy and public safety? It is time to have open and honest debates about these issues.

Where Do We Go From Here?

The FBI confronts serious threats to public safety every day. So in discussing developments that thwart the court-authorized tools we use to investigate suspected criminals, we must be sure to understand what society gains, and what we all stand to lose. What is law enforcement's recourse when we are not able to access stored data and real-time communications, despite having a court order? What happens when we cannot decipher the passcode? What happens if there are no other means to access the digital evidence we need to find a victim or prosecute a criminal? We will use every lawfully authorized investigative tool

we have to protect the citizens we serve, but having to rely on those other tools could delay criminal investigations, preclude us from identifying victims and co-conspirators, risk prematurely alerting suspects to our investigative interests, and potentially put lives in danger.

We will continue to work with our Federal, State, tribal, and local partners to identify a path forward. We are thankful for Congress' support in funding the National Domestic Communications Assistance Center, which will enable law enforcement to share tools, train one another in available intercept solutions, and reach out to the communications industry with one voice.

Companies must continue to provide strong encryption for their customers and make every effort to protect their privacy, but so too does law enforcement have a real need to obtain certain communications data when ordered by a court of law. We care about the same things – safety, security, and prosperity. And from the FBI's perspective, we know an adversarial posture won't help any of us in achieving those things. We must challenge both government and industry to develop innovative solutions to secure networks and devices, yet still yield information needed to protect our society against threats and ensure public safety.

Perhaps most importantly, we need to make sure the American public understands the issues and what is at stake.

I believe we can come to a consensus, through a reasoned and practical approach. And we must get there together. It is only by working together – within the law enforcement and intelligence communities, with the private sector, and with our elected officials – that we will find a long-term solution to this growing problem.

We in the FBI want to continue the discussion about how to solve these serious problems. We want to work with Congress, with our colleagues in the private sector, with our law enforcement and national security partners, and with the people we serve, to find the right balance for our country.

Conclusion

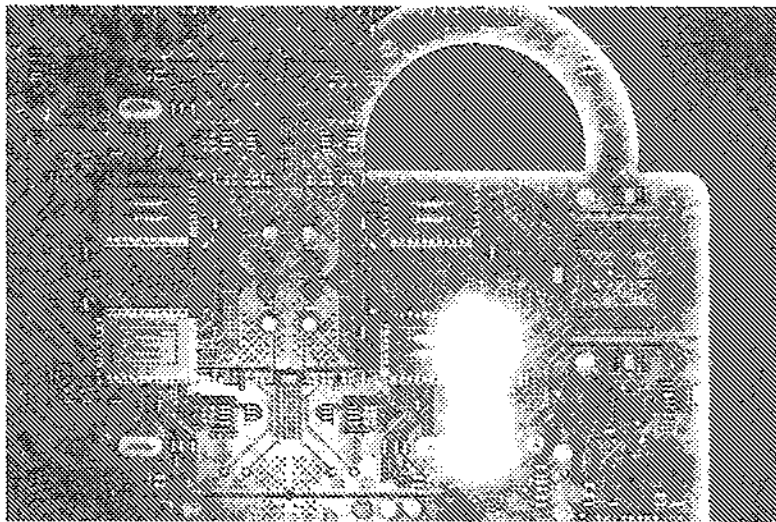
Chairman Hurd, Ranking Member Kelly, and members of the committee, I thank you for this opportunity to discuss the FBI's priorities and the challenges of Going Dark. The work we do would not be possible without the support of Congress and the American people. I would be happy to answer any questions that you may have.

#

THE WALL STREET JOURNAL
Wall Street

April 20, 2015, 3:56 AM ET

The FBI's Stance on Encrypted Communications



ISTOCK

(This post is in response to the article, [Should Law Enforcement Have the Ability to Access Encrypted Communications?](#))

AMY HESS: Imagine an America where federal, state, and municipal law enforcement agencies cannot access critical communications, even when legally authorized to do so. Imagine a time when the police cannot pursue logical leads in electronic data to rescue a missing child, identify the co-conspirators of a massive fraud scheme, or obtain relevant evidence of an elected official's public corruption. Imagine the injustice if a suspected criminal can hide incriminating communications without fear of discovery by the police, or if information that could exonerate an innocent party is inaccessible.

With the move to ubiquitous encryption, that time is closer than you think. Increasingly, law enforcement investigations require some degree of access to encrypted communications—whether stored on a computer or mobile device, or transmitted over a communication service provider's network—and that access is increasingly limited.

The FBI firmly supports the development and adoption of robust encryption as a key tool to strengthen cybersecurity, secure commerce and trade, safeguard private information, and promote free expression and association. However, absolute encryption does not mean absolute safety. Terrorists and other criminals also use encryption to conceal and facilitate their crimes.

No one in this country should be beyond the law. The notion that electronic devices and communications could never be unlocked or unencrypted – even when a judge has decided that the public interest requires accessing this data to find evidence — is troubling. It may be time to ask: Is that a cost we, as a society, are prepared to pay?

What we seek is nothing more than preserving our ability to exercise judicially-supervised access to information necessary to a continuing, authorized investigation. When law enforcement presents an order signed by a judge — who requires us to fully explain and justify why we believe someone is engaged in activity which poses a threat to public safety — the recipient must be able to quickly locate, identify, and provide the relevant data in a usable form.

Some would have you believe that privacy, security, and public safety are irreconcilable. We disagree. We believe private industry, academia, the American public, and our government can work together to strike the proper balance by putting in place the appropriate combination of laws, regulations, procedures, technology, and oversight to ensure meaningful and secure access to electronic devices and communications for law enforcement when authorized by a judge. We welcome the discussion of how to continue to ensure civil liberties while protecting the safety of the American people in this dynamic new context.

Amy Hess is the executive assistant director of the Federal Bureau of Investigation.

[redacted] (NY) (FBI)

b6 -1
b7C -1

From: [redacted] (NY) (FBI)
Sent: Monday, July 13, 2015 9:30 AM
To: RICHMAN, DANIEL C (DO)(OGA)
Subject: follow up to SCI briefing --- UNCLASSIFIED//~~FOUO~~
Attachments: SCI Initial Briefing.pptx

Classification: UNCLASSIFIED//~~FOUO~~
=====

<<SCI Initial Briefing.pptx>>

b6 -1
b7C -1
b7E -3

[redacted]
Personnel Security Specialist

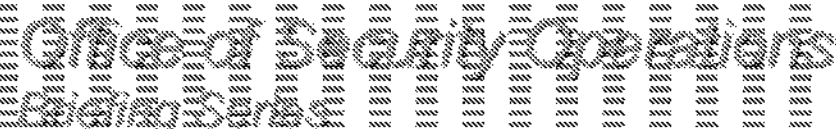
FBI New York Field Office

26 Federal Plaza, 23rd floor

New York, New York 10278

Desk: [redacted]

=====
Classification: UNCLASSIFIED//~~FOUO~~



~~Unclassified//For Official Use Only~~

Initial Briefing

1131 1380 1695 1961 2276 2542

RICHMAN, DANIEL C (DO)(OGA)

From: RICHMAN, DANIEL C (DO)(OGA)
Sent: Monday, July 13, 2015 11:45 AM
To: [REDACTED] (NY) (FBI)
Subject: RE: follow up to SCI briefing --- UNCLASSIFIED//~~FOUO~~

b6 -1
b7C -1

Classification: UNCLASSIFIED//~~FOUO~~
=====

Got it.

Thanks for all your help

Dan Richman

From: [REDACTED] (NY) (FBI)
Sent: Monday, July 13, 2015 9:30 AM
To: RICHMAN, DANIEL C (DO)(OGA)
Subject: follow up to SCI briefing --- UNCLASSIFIED//~~FOUO~~

b6 -1
b7C -1

Classification: UNCLASSIFIED//~~FOUO~~
=====

<< File: SCI Initial Briefing.pptx >>

[REDACTED]

b6 -1
b7C -1
b7E -3

Personnel Security Specialist

FBI New York Field Office

26 Federal Plaza, 23rd floor

New York, New York 10278

Desk: [REDACTED]

=====
Classification: UNCLASSIFIED//~~FOUO~~
=====

=====
Classification: UNCLASSIFIED//~~FOUO~~
=====

FBI 18-CV-1833-7775

[redacted] (NY) (FBI)

b6 -1
b7C -1

From: [redacted] (NY) (FBI)
Sent: Monday, July 13, 2015 11:45 AM
To: RICHMAN, DANIEL C (DO)(OGA)
Subject: Automatic reply: follow up to SCI briefing --- UNCLASSIFIED//~~FOUO~~

Classification: UNCLASSIFIED
=====

I will be working out of the Chelsea office 7/6 through 7/31. I will have limited phone access. I will be periodically checking my desk voice mail at 26 Federal Plaza.

Thank You,

[redacted]
Personnel Security Specialist
NYO Physical and Personnel Security Unit
26 Federal Plaza,
New York, NY 10278
Desk [redacted]

b6 -1
b7C -1
b7E -3

=====
Classification: UNCLASSIFIED

RICHMAN, DANIEL C (DO)(OGA)

From: RICHMAN, DANIEL C (DO)(OGA)
Sent: Monday, July 13, 2015 11:50 AM
To: OCONNELL, SASHA (DO) (FBI)
Subject: RE: Going Dark Documents, [REDACTED] --- UNCLASSIFIED

b7E -1

Classification: UNCLASSIFIED
=====

TRANSITORY RECORD

Got these and am reading them now. Thanks!

Dan Richman

From: OCONNELL, SASHA (DO) (FBI)
Sent: Tuesday, July 07, 2015 3:42 PM
To: RICHMAN, DANIEL C (DO)(OGA)
Cc: [REDACTED] (DO)(FBI)
Subject: Going Dark Documents, [REDACTED] --- UNCLASSIFIED

b6 -1
b7C -1
b7E -1

Classification: UNCLASSIFIED
=====

TRANSITORY RECORD

To follow up on our meeting, I have attached a snapshot of documents for your reference. Also, the following is a link to the [REDACTED] which contains additional Going Dark documents from the past year: [REDACTED]
[REDACTED] If you have any trouble with [REDACTED] access please contact [REDACTED] from my office cc'd here. Please let me know if you need any additional information or background on the included documents. We very much look forward to working with you!

b6 -1
b7C -1
b7E -1,3

Going Dark Document Appendix

- 1) Director's Brookings Institute Speech
- 2) Director's Blog Article Lawfare
- 3) Executive Assistant Director of the Science and Technology Branch Amy Hess – WSJ Article
- 4) Congressional Statement for the Record – EAD Amy Hess
- 5) Congressional Statement for the Record – AD Steinbach
- 6) DOJ Attorney General Transition PowerPoint on Going Dark

FBI 18-CV-1833-7777

<< File: 10.16.14 Director's Remarks for Brookings Institution PRESS VERSION.docx >> << File: Encryption_Public_Safety_and_Going_Dark.docx >> << File: Wall_Street_Journal_Article_4-20-2015.jpeg >> << File: SOR.Hess.4.29.15.Encryption.Cybersecurity.pdf >> << File: SFR AD Steinbach Committee on Homeland Security.pdf >> << File: Going Dark Initiative - AG Pres - Update - 0407 - 335 PM.pptx >>

=====
Classification: UNCLASSIFIED

=====
Classification: UNCLASSIFIED

=====
Classification: UNCLASSIFIED

[REDACTED]

From: [REDACTED]
Sent: Monday, July 27, 2015 12:02 PM
To: RICHMAN, DANIEL C (DO)(OGA)
Subject: New Mandatory Training Assignment: Information Security (INFOSEC) Awareness 2015
Importance: High

Dear DANIEL RICHMAN,

You are required to complete the following mandatory training assignment by 9/30/2015 11:59 PM:

Title: Information Security (INFOSEC) Awareness 2015

Type: Online

Training Sponsor: FBI - Security Division

Number of Training Hours: .5

Mandate Type: Statute or Regulation

Please log into the Virtual Academy at [REDACTED] to complete this assignment. To find your required training list, locate My Training in the blue navigation bar at the top of the page and select My Training Plan from the drop-down menu. Or you may find the Mandatory Training widget on your VA Portal Page (VA Homepage) an easy way to access your required training.

b7E -3

This assignment must be completed by 9/30/2015 11:59 PM; however, if you previously completed the course, you have satisfied the assignment and need not take it again.

Once you have satisfied the assignment, the course will disappear from your VA Training Plan. Please note, the moment you complete a WBT, it will show as complete under My Learning, My Training Progress; however, it may take a day to appear on your transcript under My Records, My Official Transcript.

Peak system usage occurs the day employees receive this email which may affect system performance. Since you have plenty of time to complete this assignment, the VA team recommends you do not try to complete this course today. Instead, schedule another date/time to take the course. Your mandates will always be listed on your training plan.

Click on the following link to access your Training Plan: [REDACTED]

b7E -3

If you have any questions, please contact the Virtual Academy for assistance via the EOC Helpdesk (202-324-1500) who will create a ticket and route it to the VA staff.

Thank you,
Virtual Academy
Training Division

Please do not reply to this email.

RICHMAN, DANIEL C (DO)(OGA)

From: RICHMAN, DANIEL C (DO)(OGA)
Sent: Thursday, September 10, 2015 6:20 PM
To: [REDACTED] (DO)(FBI)
Cc: OCONNELL, SASHA (DO) (FBI); RICHMAN, DANIEL C (DO)(OGA)
Subject: director's speech in chicago --- UNCLASSIFIED

b6 -1
b7C -1

Classification: UNCLASSIFIED

=====

Hi [REDACTED] and Sasha) – I realize I need not use High Side email to weigh in on the speech. But I can't get into the Low Side from [REDACTED]'s office because I probably am using the wrong password. And I want to write while my conversation with the Director is fresh in my mind. [REDACTED]

b5 -1
b6 -1
b7C -1

[REDACTED]

[REDACTED]

b5 -1
b6 -2
b7C -2



b5 -1
b6 -1
b7C -1

I could go into more detail on this, but figure that, at least for now (given how many people are weighing in), I should paint in broad strokes. Please don't take anything here as reflecting points that the Dir has actually decided to make. He just wanted me share my stray (and perhaps highly misguided) thoughts.

Thx

Dan richman

=====

Classification: UNCLASSIFIED

[redacted] (OGC)(FBI)

b6 -1
b7C -1

From: [redacted] (OGC)(FBI)
Sent: Monday, September 14, 2015 9:38 AM
To: RICHMAN, DANIEL C (DO)(OGA)
Subject: Travel --- UNCLASSIFIED
Attachments: Travel.pdf

Classification: UNCLASSIFIED
=====

TRANSITORY RECORD

For your records... Fingers crossed that the reimbursement is actually made to your checking account!

<<Travel.pdf>>

(U) [redacted]

b6 -1
b7C -1
b7E -3

Associate General Counsel

FBI OGC

direct: [redacted]

(U) Confidentiality Statement:

(U) This message is transmitted to you by the Office of the General Counsel of the Federal Bureau of Investigation. The message, along with any attachments, may be confidential and legally privileged. If you are not the intended recipient of this message, please destroy it promptly without further retention or dissemination (unless otherwise required by law). Please notify the sender of the error by a separate e-mail or by calling [redacted]

=====
Classification: UNCLASSIFIED

TRIP #:

Request Date: 09/08/2015

Current Stage: FO Review of Actual Expenses (Blue)

Travel Summary for Daniel Richman

b6 -1
b7C -1

Traveler Information

Who is traveling? Non-Bureau Invitational Traveler**Division/ Field Office:** DIRECTORS OFFICE**Last Name:** Richman**Cost Code:** 0010**First Name:** Daniel**Middle Name:****Please provide a short explanation for travel requested.** For meetings at HQ regarding this SGEs projects.**Is the traveler the head of an FO (ADIC or SAC)?** No**Is the travel request within the traveler's area of responsibility?** No

Itinerary

Official Travel Start Date: 09/10/2015**Official Travel End Date:** 09/12/2015**Travel Type:** Round Trip

Depart Date	Depart City	Depart State	Depart Country	Arrival Date	Dest. City	Dest. State	Dest. Country
09/10/2015	NEW YORK	NY	UNITED STATES	09/10/2015	WASHINGTON	DC	UNITED STATES
09/12/2015	WASHINGTON	DC	UNITED STATES	09/12/2015	NEW YORK	NY	UNITED STATES

☐ Traveler will be conducting personal travel outside of their official travel dates (i.e. - personal travel prior to the start or end of the official travel date, regardless of location)

☐ Traveler will be conducting personal travel to an alternate location in addition to business travel locations (indirect travel).

☐ Travel is within 50 miles of the traveler's residence or permanent duty station.

☐ Travel is part of a 60 day TDY.

GETA #:

Funding and Expenses

Total Estimated Expenses: \$843.78**Funding Division:** DIRECTORS OFFICE**Total Actual Expenses:** \$658.50**Program:** FX**Total Reimbursement Amount:** \$658.50**Subprogram:** FX**TR Type:** TR11: Division Operational Travel

Type	GSA Location	Expense Start Date	Expense End Date	Estimated Cost	Actual Cost	Receipt Required	Paid By GTA	Reimbursement Amount	Advance of Funds	Miles
Lodging	UNITED STATES, DC, DISTRICT OF COLUMBIA	09/10/2015	09/12/2015	\$444.00	\$212.44	Yes	No	\$212.44	No	0
M and IE	UNITED STATES, DC, DISTRICT OF COLUMBIA	09/10/2015	09/12/2015	\$177.50	\$177.50	No	No	\$177.50	No	0
Parking		09/10/2015	09/10/2015	\$0.00	\$17.00	No		\$17.00	No	0

TRIP #:

Request Date: 09/08/2015

Current Stage: FO Review of Actual Expenses (Blue)

Travel Summary for Daniel Richman

b6 -1
b7C -1

Type	GSA Location	Expense Start Date	Expense End Date	Estimated Cost	Actual Cost	Receipt Required	Paid By GTA	Reimbursement Amount	Advance of Funds	Miles
Train Fare		09/10/2015	09/10/2015	\$86.00	\$86.00	Yes	No	\$86.00	No	0
Tolls		09/10/2015	09/10/2015	\$0.00	\$36.18	No		\$36.18	No	0
Mileage - POV Authorized/No GOV Available		09/12/2015	09/12/2015	\$136.28	\$129.38	No	No	\$129.38	No	225

How did you book your travel?

Did not Book through Carlson

Per Federal Travel Regulation you are required to book official travel through Carlson. Please explain why you did not book through Carlson: SGE booked on his own.

Supplemental Forms Required

- ☐ Cost Comparison Form
- ☐ Foreign Air Carrier Form
- ☐ Premium Class Travel Form
- ☐ Lodging in Excess of GSA Form
- ☐ Indirect Travel Form
- ☐ 50 Mile Waiver Form

Travel Summary for Daniel Richman

Approvals

Stage	Approver Name	Date/Time	Decision
Supervisor Approval of Actual Expenses	OGC)(FBI)	09/14/2015 09:35:48	TRIP approved, no supplemental forms required.
Finance Office Review of Request	(FLSD) (CON)	09/09/2015 04:05:38	TRIP approved, no supplemental forms required.
Supervisor Review of Travel Request	OGC)(FBI)	09/09/2015 03:50:36	TRIP approved, no supplemental forms required.

[redacted] (DO) (FBI)

b6 -1
b7C -1

Subject: Going Dark Communications Strategies Conference --- UNCLASSIFIED
Location: HRD Large Conference Room 10903

Start: Friday, November 13, 2015 10:00 AM
End: Friday, November 13, 2015 4:00 PM
Show Time As: Tentative

Recurrence: {none}

Meeting Status: Not yet responded

Organizer: [redacted] (DO) (FBI)

Required Attendees: HESS, AMY S (DO)(FBI); OCONNELL, SASHA (DO) (FBI); BURRELL, JAMES (OTD)(FBI); BAKER, JAMES A (OGC)(FBI); [redacted] (OTD) (FBI); [redacted] (DO)(FBI); RICHMAN, DANIEL C (DO) (OGA); [redacted]

b6 -1,5
b7C -1,5

When: Friday, November 13, 2015 10:00 AM-4:00 PM (UTC-05:00) Eastern Time (US & Canada).

Where: HRD Large Conference Room 10903

Note: The GMT offset above does not reflect daylight saving time adjustments.

~~*~*~*~*~*~*~*~*

Classification: UNCLASSIFIED

=====
Classification: UNCLASSIFIED

[redacted] (DO) (FBI)

b6 -1
b7C -1

Subject: Prep for Columbia Law School Event --- UNCLASSIFIED
Location: OGC Conference Room 7426 - VTC

Start: Tuesday, October 06, 2015 2:15 PM
End: Tuesday, October 06, 2015 3:00 PM
Show Time As: Tentative

Recurrence: {none}

Meeting Status: Not yet responded

Organizer: [redacted] (DO) (FBI)

b6 -1
b7C -1

Required Attendees: HESS, AMY S (DO)(FBI); BAKER, JAMES A (OGC)(FBI); RICHMAN, DANIEL C (DO)(OGA); BURRELL, JAMES (OTD)(FBI); OCONNELL, SASHA (DO) (FBI); [redacted] (DO)(FBI)

When: Tuesday, October 06, 2015 2:15 PM-3:00 PM (UTC-05:00) Eastern Time (US & Canada).

Where: OGC Conference Room 7426 - VTC

Note: The GMT offset above does not reflect daylight saving time adjustments.

~~*~*~*~*~*~*~*~*

Classification: UNCLASSIFIED

=====

=====

Classification: UNCLASSIFIED

Subject: Prep for Columbia Law School Event --- UNCLASSIFIED
Location: OGC Conference Room 7426 - VTC

Start: Tuesday, October 06, 2015 2:15 PM
End: Tuesday, October 06, 2015 3:00 PM
Show Time As: Tentative

Recurrence: {none}

Meeting Status: Not yet responded

Organizer: [redacted] (DO) (FBI)

b6 -1
b7C -1

Required Attendees: HESS, AMY S (DO)(FBI); BAKER, JAMES A (OGC)(FBI); RICHMAN, DANIEL C (DO)(OGA); BURRELL, JAMES (OTD)(FBI); OCONNELL, SASHA (DO) (FBI); [redacted] (DO)(FBI)

When: Tuesday, October 06, 2015 2:15 PM-3:00 PM (UTC-05:00) Eastern Time (US & Canada).

Where: OGC Conference Room 7426 - VTC

Note: The GMT offset above does not reflect daylight saving time adjustments.

~~*~*~*~*~*~*~*~*

Classification: UNCLASSIFIED

=====

PLEASE NOTE NEW TITLE, GOING DARK INITIATIVE

ALL SITES PLEASE DIAL [redacted]

b7E -3

ALL LYNC PARTICIPANTS PLEASE CLICK LINK BELOW:

[redacted]

A Microsoft Lync session will open,

First, Click on "Video" to start the video.

You will see the Polycom RMX splash screen.

PLEASE BE SURE TO MUTE YOUR MIC

(CLICK THE MIC SYMBOL LOCATED IN THE LYNC BOX TO MUTE YOUR MIC)

POC ASAC

b6 -1
b7C -1
b7E -3

=====
Classification: UNCLASSIFIED

[redacted] (FD) (FBI)

b6 -1
b7C -1

From: [redacted] (FD) (FBI)
Sent: Tuesday, October 20, 2015 3:36 PM
To: RICHMAN, DANIEL C (DO)(OGA)
Subject: Foreign Travel --- UNCLASSIFIED

Classification: UNCLASSIFIED
=====

TRANSITORY RECORD

Daniel – per our recent discussion I’ve provided you the below link that will walk you through how to report foreign travel. Please ensure you review the entire page to ensure all the requirements are met. If you have any questions please let me know.

[redacted]

b6 -1
b7C -1
b7E -3

Respectfully,

[redacted]

Principal Deputy Chief Security Officer

Office of Security Operations

DO, FD, FLSD, INSD, IOD, OGC, OPE, RPO, WMDD

Cell: [redacted]

Fax: [redacted]

FBIHQ Suite 10270

Security questions? Visit the [OSO Website](#)

=====
Classification: UNCLASSIFIED

RICHMAN, DANIEL C (DO)(OGA)

From: RICHMAN, DANIEL C (DO)(OGA)
Sent: Monday, November 16, 2015 5:02 PM
To: [REDACTED] (FD) (FBI)
Subject: Read: Foreign Travel --- UNCLASSIFIED

b6 -1
b7C -1

Your message

To: RICHMAN, DANIEL C (DO)(OGA)
Subject: Foreign Travel --- UNCLASSIFIED
Sent: Tuesday, October 20, 2015 3:36:16 PM (UTC-05:00) Eastern Time (US & Canada)

was read on Monday, November 16, 2015 5:01:16 PM (UTC-05:00) Eastern Time (US & Canada).

RICHMAN, DANIEL C (DO)(OGA)

From: RICHMAN, DANIEL C (DO)(OGA)
Sent: Monday, November 16, 2015 5:25 PM
To: [REDACTED] (FD) (FBI)
Subject: RE: Foreign Travel --- UNCLASSIFIED

b6 -1
b7C -1

Classification: UNCLASSIFIED
=====

TRANSITORY RECORD

Hey [REDACTED] I finally made into the NYO to do my form and got stuck early on because my "supervisor" -- David Harbach -- could not be "verified." I tried Jim Rybicki and Jim Baker's names, and they didn't work either. Could you please email me on my Columbia email (as I won't be back in the NYO for a few days) to tell me what I should do.

b6 -1
b7C -1

Thx

Dan richman

From: [REDACTED] (FD) (FBI)
Sent: Tuesday, October 20, 2015 3:36 PM
To: RICHMAN, DANIEL C (DO)(OGA)
Subject: Foreign Travel --- UNCLASSIFIED

b6 -1
b7C -1

Classification: UNCLASSIFIED
=====

TRANSITORY RECORD

Daniel -- per our recent discussion I've provided you the below link that will walk you through how to report foreign travel. Please ensure you review the entire page to ensure all the requirements are met. If you have any questions please let me know.

[REDACTED]

b6 -1
b7C -1
b7E -3

Respectfully,

[REDACTED]

Principal Deputy Chief Security Officer

Office of Security Operations

FBI 18-CV-1833-7792

DO, FD, FLSD, INSD, IOD, OGC, OPE, RPO, WMDD

Cell:

b7E -3

Fax:

FBIHQ Suite 10270

Security questions? Visit the [OSO Website](#)

=====
Classification: UNCLASSIFIED

=====
Classification: UNCLASSIFIED

[redacted] (DO) (FBI)

b6 -1
b7C -1

From: [redacted] (DO) (FBI)
Sent: Thursday, December 10, 2015 11:34 AM
To: RICHMAN, DANIEL C (DO)(OGA)
Subject: Ethics Training --- UNCLASSIFIED

Classification: UNCLASSIFIED
=====

TRANSITORY RECORD

I'm sorry I didn't have you on my list.

As you know, OGE-278, OGE-450 and CIC financial disclosure filers must ensure that they have satisfied their ethics training requirement of one-hour by 12/31/15.

It is available now on Virtual Academy (VA) through the link below. You do not have to exercise this option but you must obtain ethics training by the end of the year to satisfy the Executive Branch-wide mandate. Other options include watching an ethics video available by visiting the OIC website or listening to an ethics session presented by OIC. Remember that, as you take the VA course or watch one of the available videos, you may direct related questions to OIC.

Annual Standards of Ethical Conduct Training

You can also watch "The Squad" or "The Office" on FBITV.

Required financial disclosure filers must certify completion of the training requirement to me NLT 12/31/2015. Please see link below for certification form:

[redacted]

b6 -1
b7C -1
b7E -3

[redacted]

Administrative Management and Analysis Unit

Resource Planning Office/Director's Office

Room 9798

[redacted]

Please visit the Administrative Management and Analysis Unit's webpage at [AMAU](#)

=====
Classification: UNCLASSIFIED

FBI 18-CV-1833-7794

[REDACTED] (SECD)(CON)

b6 -1
b7C -1

From: [REDACTED] (SECD)(CON)
Sent: Friday, December 18, 2015 2:14 PM
To: RICHMAN, DANIEL C (DO)(OGA)
Subject: FD-772 — UNCLASSIFIED

Classification: UNCLASSIFIED
=====

Good Afternoon,

You have been identified as logging on via OWA to the network from a non USA location.

Can you please confirm if you are is assigned to Legats, TDY, or is on Personal Travel outside the United States?

1. Real Name: Daniel C Richman

[REDACTED]

b6 -1,4
b7C -1,4

If you are not assigned to Legats, TDY, or on Personal Travel and has not submitted a FD-772, please have the user do so via SPAS.

Thanks and have a nice day!

[REDACTED]

b6 -1
b7C -1
b7E -3

Security Specialist

Office of Security Operations

DO, FD, FLSD, INSD, IOD, OGC, OPE, RPO, WMDD

Work: [REDACTED]

Fax: [REDACTED]

FBIHQ Suite 1323

=====

FBI 18-CV-1833-7795

Classification: UNCLASSIFIED

[redacted] (FD)(FBI)

b6 -1
b7C -1
b7E -11

From: [redacted] (FD)(FBI)
Sent: Friday, December 18, 2015 4:16 PM
To: RICHMAN, DANIEL C (DO)(OGA)
Subject: [redacted] -- UNCLASSIFIED
Attachments: SEC-102 Foreign Travel Briefing Acknowledgement.pdf; Foreign Travel Briefing
OSO.pdf

Classification: UNCLASSIFIED
=====

TRANSITORY RECORD

Hello Daniel,

[redacted]
[redacted] I ask that you view the attached Foreign Travel
Briefing and return via e-mail (scanned .pdf copy) the acknowledgment form also attached. If you have
any questions please feel free to contact me.

b7E -11

<<Foreign Travel Briefing OSO.pdf>>

<<SEC-102 Foreign Travel Briefing Acknowledgement.pdf>>

Thanks,

[redacted]

b6 -1
b7C -1
b7E -3

Office of Security Operations

DO, FD, FLSD, INSD, IOD, OGC, OPE, RPO, WMDD

[redacted]

Rm 10270

Visit the [OSO Website](#)

=====
Classification: UNCLASSIFIED

Foreign Travel Briefing Acknowledgement

PURPOSE OF THIS FORM

This acknowledgement serves as verification that the following individual has been afforded a foreign travel awareness briefing. The individual has been briefed on tips and tools to protect themselves, their co-travelers, and property. The individual, by affixing their signature, affirms that they will abide by all standards and requirements of the FBI's security program while traveling overseas in an official or unofficial capacity. Additionally, the individual will report to security any qualifying personal or professional security related incidents and foreign contacts as outlined in either the Standard Foreign Travel (SFT) or Hostile Intelligence Threat (HIT) briefings and as stipulated by the Security Policy Manual. Briefings are good for one year from the date conducted. Individuals should consult with security before any future foreign travel should they have any questions.

TRAVELER INFORMATION

(INCLUDES EMPLOYEE, CONTRACTOR, DETAILEE, AND TFO'S)

Full Name:	Room Number:
Assignment (Division and Unit/Office):	Work Phone Number:
Company or Agency (Contractor/Detailee/TFO only):	

BRIEFING TYPE

Select one or both as applicable:

☐ **Standard Foreign Travel (SFT) Briefing**

A complete SFT briefing was afforded in accordance with FBI policy utilizing the latest version provided by the Security Division.

☐ **Hostile Intelligence Threat (HIT) Briefing**

A HIT briefing was afforded in relation to the individual's impending foreign travel to a specific hazardous country or to a country that poses a threat to U.S. National Security.

ACKNOWLEDGEMENT

(TO BE COMPLETED BY TRAVELER)

I acknowledge that I have been afforded a SFT and/or HIT Briefing regarding my impending foreign travel. My signature below asserts that I fully comprehend my security related duties/responsibilities, and affirms my commitment to the FBI's security policies, regulations and procedures. I have been provided with resources to protect myself, my co-travelers and my property from excessive risk. I will consult with security at any time before foreign travel to ensure I have taken all reasonable and required precautions

_____	_____
Printed Name	Date

Signature	

ADMINISTRATIVE USE ONLY

(TO BE COMPLETED BY SECURITY OFFICER)

_____	_____
Security Officer Administering FTB	Date SAB Administered

RICHMAN, DANIEL C (DO)(OGA)

From: RICHMAN, DANIEL C (DO)(OGA)
Sent: Tuesday, December 22, 2015 4:13 PM
To: [REDACTED] (FD)(FBI)
Subject: RE: [REDACTED] -- UNCLASSIFIED

b6 -1
b7C -1
b7E -11

Classification: UNCLASSIFIED
=====

TRANSITORY RECORD

Dear [REDACTED] - This came in while I was in Israel and I'm back now . The entire trip was uneventful and, now that I read the materials, I see that I followed the advice. Should I do anything more? Sorry for my delay in responding, I have limited access to FBINet -- only on those rare days I go into the NYO

Thx

Dan richman

From: [REDACTED] (FD)(FBI)
Sent: Friday, December 18, 2015 4:16 PM
To: RICHMAN, DANIEL C (DO)(OGA)
Subject: [REDACTED] -- UNCLASSIFIED

b6 -1
b7C -1
b7E -11

Classification: UNCLASSIFIED
=====

TRANSITORY RECORD

Hello Daniel,

[REDACTED]
[REDACTED] I ask that you view the attached Foreign Travel Briefing and return via e-mail (scanned .pdf copy) the acknowledgment form also attached. If you have any questions please feel free to contact me.

b7E -11

<< File: Foreign Travel Briefing OSO.pdf >>

<< File: SEC-102 Foreign Travel Briefing Acknowledgement.pdf >>

Thanks,

[REDACTED]

b6 -1
b7C -1
FBI 18-CV-1833-7833

Office of Security Operations

DO, FD, FLSD, INSD, IOD, OGC, OPE, RPO, WMDD

[REDACTED]

b7E -3

Rm 10270

Visit the [OSO Website](#)

=====
Classification: UNCLASSIFIED

=====
Classification: UNCLASSIFIED

RICHMAN, DANIEL C (DO)(OGA)

From: RICHMAN, DANIEL C (DO)(OGA)
Sent: Tuesday, December 22, 2015 5:29 PM
To: [REDACTED] (FD) (FBI)
Subject: RE: Foreign Travel --- UNCLASSIFIED

b6 -1
b7C -1

Classification: UNCLASSIFIED
=====

TRANSITORY RECORD

Hey [REDACTED] - I'm (from Israel) with another problem. The system won't let me make entries on the FD772b to report my trip. Could you please respond on the low-side & tell me what magic you used to allow my entries last time?

Thanks

Dan richman

From: [REDACTED] (FD) (FBI)
Sent: Tuesday, October 20, 2015 3:36 PM
To: RICHMAN, DANIEL C (DO)(OGA)
Subject: Foreign Travel --- UNCLASSIFIED

b6 -1
b7C -1

Classification: UNCLASSIFIED
=====

TRANSITORY RECORD

Daniel – per our recent discussion I've provided you the below link that will walk you through how to report foreign travel. Please ensure you review the entire page to ensure all the requirements are met. If you have any questions please let me know.

[REDACTED]

b6 -1
b7C -1
b7E -3

Respectfully,

[REDACTED]

Principal Deputy Chief Security Officer

Office of Security Operations

FBI 18-CV-1833-7835

DO, FD, FLSD, INSD, IOD, OGC, OPE, RPO, WMDD

Cell:

b7E -3

Fax:

FBIHQ Suite 10270

Security questions? Visit the [OSO Website](#)

=====
Classification: UNCLASSIFIED

=====
Classification: UNCLASSIFIED

[REDACTED] (FD) (FBI)

b6 -1
b7C -1

From: [REDACTED] (FD) (FBI)
Sent: Tuesday, December 22, 2015 5:29 PM
To: RICHMAN, DANIEL C (DO)(OGA)
Subject: Automatic reply: Foreign Travel --- UNCLASSIFIED

I am currently out of the office and will return on Monday, December 28th.

For assistance with security matters please visit the [OSO Website](#) for a list of the OSO staff who can assist you. I will have limited access to my cell and UNET e-mail and will respond to all messages when I return.

Thanks and have a Merry Christmas!

[REDACTED]
Principle Deputy Chief Security Officer
Office of Security Operations
Federal Bureau of Investigation / Room 10270
Cell: [REDACTED]

b6 -1
b7C -1
b7E -3

[REDACTED] (FD)(FBI)

b6 -1
b7C -1
b7E -11

From: [REDACTED] (FD)(FBI)
Sent: Wednesday, December 23, 2015 8:12 AM
To: RICHMAN, DANIEL C (DO)(OGA)
Subject: RE: [REDACTED] --- UNCLASSIFIED

Classification: UNCLASSIFIED
=====

TRANSITORY RECORD

Hi Rich,

Just return the signed acknowledgement form.

Thanks,

[REDACTED]

b6 -1
b7C -1
b7E -11

From: RICHMAN, DANIEL C (DO)(OGA)
Sent: Tuesday, December 22, 2015 4:13 PM
To: [REDACTED] (FD)(FBI)
Subject: RE: [REDACTED] --- UNCLASSIFIED

Classification: UNCLASSIFIED
=====

TRANSITORY RECORD

Dear [REDACTED] This came in while I was in Israel and I'm back now . The entire trip was uneventful and, now that I read the materials, I see that I followed the advice. Should I do anything more? Sorry for my delay in responding, I have limited access to FBINet - only on those rare days I go into the NYO

Thx

Dan richman

From: [REDACTED] (FD)(FBI)
Sent: Friday, December 18, 2015 4:16 PM
To: RICHMAN, DANIEL C (DO)(OGA)
Subject: [REDACTED] --- UNCLASSIFIED

b6 -1
b7C -1
b7E -11

Classification: UNCLASSIFIED
=====

TRANSITORY RECORD

FBI 18-CV-1833-7838

Hello Daniel,

[REDACTED]

b7E -11

[REDACTED] I ask that you view the attached Foreign Travel Briefing and return via e-mail (scanned .pdf copy) the acknowledgment form also attached. If you have any questions please feel free to contact me.

<< File: Foreign Travel Briefing OSO.pdf >>

<< File: SEC-102 Foreign Travel Briefing Acknowledgement.pdf >>

Thanks,

[REDACTED]

b6 -1
b7C -1
b7E -3

Office of Security Operations

DO, FD, FLSD, INSD, IOD, OGC, OPE, RPO, WMDD

[REDACTED]

Rm 10270

Visit the [OSO Website](#)

=====
Classification: UNCLASSIFIED

=====
Classification: UNCLASSIFIED

=====
Classification: UNCLASSIFIED

To: [REDACTED] (OGC)(FBI); [REDACTED] (OGC)
[REDACTED] (FBI); [REDACTED] (OGC)(FBI); [REDACTED] (INSD)(FBI); [REDACTED]
[REDACTED] (INSD) (FBI); [REDACTED] (DO) (FBI); [REDACTED]
(OPA) (FBI); [REDACTED] (OGC) (FBI); [REDACTED] (DO)
(FBI); [REDACTED] (DO) (FBI); [REDACTED] (CK) (FBI);
[REDACTED] (OGC) (FBI); [REDACTED] (OGC) (FBI); [REDACTED]
(OGC) (FBI); [REDACTED] (OPA) (FBI); [REDACTED] (OGC)(FBI);
[REDACTED] (OGC) (FBI); [REDACTED] (OCA) (FBI); [REDACTED]
[REDACTED] (OEE) (FBI); [REDACTED] (DO) (FBI); [REDACTED]
(DO) (FBI); [REDACTED] (OGC)(FBI); [REDACTED] (OGC) (FBI);
[REDACTED] (INSD) (FBI); [REDACTED] (OPA) (FBI); [REDACTED]
[REDACTED] (DO) (FBI); [REDACTED] (DO) (FBI); [REDACTED] (DO) (FBI);
[REDACTED] (DO) (FBI); [REDACTED] (INSD)(FBI); [REDACTED]
(OGC) (FBI); [REDACTED] (OPA) (FBI); [REDACTED] (OGC)(FBI); [REDACTED]
[REDACTED] (OGC)(FBI); [REDACTED] (OGC) (FBI); [REDACTED]
[REDACTED] (OGC) (FBI); [REDACTED] (DO) (FBI); [REDACTED] (DE)
(FBI); [REDACTED] (NSD) (FBI); [REDACTED] (DO) (FBI); [REDACTED]
[REDACTED] (DO) (FBI); [REDACTED] (INSD)(FBI); [REDACTED] (DO)
(FBI); [REDACTED] (INSD)(FBI); [REDACTED] (OGC) (FBI); [REDACTED]
[REDACTED] (OGC)(FBI); [REDACTED] (OGC)(FBI); [REDACTED]
(OPA) (FBI); [REDACTED] (OPA) (FBI); [REDACTED] (DO) (FBI);
[REDACTED] (DO) (FBI); [REDACTED] (OGC)(FBI); [REDACTED]
[REDACTED] (OGC) (FBI); [REDACTED] (OGC) (FBI); [REDACTED] (DO) (FBI);
[REDACTED] (DO) (FBI); [REDACTED] (INSD) (FBI); [REDACTED] (OGC)
(FBI); RICHMAN, DANIEL C (DO) (OGA); [REDACTED] (OGC)(FBI); [REDACTED]
[REDACTED] (DO) (FBI); [REDACTED] (OGC)(FBI); [REDACTED] (OGC)
(FBI); [REDACTED] (NSD)(FBI); [REDACTED] (DO) (FBI); [REDACTED]
[REDACTED] (CYD)(FBI); [REDACTED] (INSD) (FBI); [REDACTED] (INSD)
(FBI); [REDACTED] (OGC) (FBI); [REDACTED] (DO) (FBI);
[REDACTED] (OGC) (FBI); [REDACTED] (DO) (FBI); [REDACTED]
[REDACTED] (DO) (FBI); [REDACTED] (DO) (FBI); [REDACTED]
[REDACTED] (DO) (FBI); [REDACTED] (OGC) (FBI); [REDACTED]
(OGC)(FBI); [REDACTED] (DO) (FBI); [REDACTED] (DO)(FBI)

Classification: UNCLASSIFIED

FBI 18-CV-1833-7840

Integrity and Compliance (OIC) by their deadline.

<<Annual_Reporting_Requirements_for_OGE-450_and_CIC_filers.pdf>>

All FBI OGE-450 filers are also required to complete an "Employee Certification – No Known Conflicts of Interest with Federal Duties" form ("No Conflicts" form). The No Conflicts form must be completed each year and returned with the OGE-450 form.

No Known Conflicts Certification

Please make sure you get your supervisor to sign your OGE-450 before you turn it in. If you have any questions, please let me know.

[Redacted]

Administrative Management and Analysis Unit

Resource Planning Office/Director's Office

Room 9798

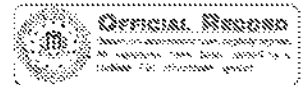
[Redacted]

Please visit the Administrative Management and Analysis Unit's webpage at AMAU

=====
Classification: UNCLASSIFIED

b6 -1
b7C -1
b7E -3

UNCLASSIFIED

**FEDERAL BUREAU OF INVESTIGATION****Electronic Communication**

Title: (U) Annual Reporting Requirements for
OGE-450 and CIC filers

Date: 01/11/2016

CC:

b6 -1
b7C -1
b7E -3

From: DIRECTOR'S OFFICE
DO-OFFICE INTEGRITY AND COMPLIANCE
Contact:

Approved By: KELLEY PATRICK W

Drafted By:

Case ID #:

(U) ETHICS FINANCIAL DISCLOSURE
REPORTING -

b6 -1
b7C -1
b7E -13

Synopsis: (U) Reminds all divisions/offices of annual filing requirements for Confidential Financial Disclosure Reports (OGE-450) and Conflict of Interest Certification (CIC) forms as well as completion of the No Known Conflicts of Interest with Federal Duties form.

Enclosure(s): Enclosed are the following items:

1. (U) OGE-450 Reviewers Aid

Details:

(U) Government-wide ethics regulations require GS-15 and below employees in certain positions to file a Confidential Financial Disclosure Report (OGE-450) or a Conflict of Interest Certification (CIC) form. Additionally, all OGE-450 filers are required to complete a "No Known Conflicts of Interest With Federal Duties Certification" form. The No Known Conflicts form must be completed each year and returned with the

UNCLASSIFIED

UNCLASSIFIED

Title: (U) Annual Reporting Requirements for OGE-450 and CIC filers
Re: [REDACTED] 01/11/2016

b7E -13

filer's OGE-450 form. CIC filers are not required to complete the No Known Conflicts form. Both the OGE-450 and No Known Conflicts forms, as well as the CIC form, can be found on the Office of Integrity & Compliance (OIC) website:

[REDACTED]

b7E -3

(U)Chief Division Counsels (CDC) and HQ Division Ethics Points of Contact are responsible for administering the confidential financial disclosure program within their divisions. CDC's and Ethics POC's should review the FBI Ethics and Integrity Program Guide, Sections 5.2.2 and 5.2.3, to identify those employees required to file an OGE-450 or CIC form.

(U)Lastly, divisions are required to track OGE-450 and CIC filers using the excel spreadsheet available on the OIC website under "Forms" labeled "Financial Disclosure Filers - Spreadsheet."

(U) FILING DEADLINES

(U)Incumbent (Annual) Filers: OGE-450 or CIC forms covering the reporting period from January 1 - December 31, 2015, must be filed by **F ebruary 16, 2016**. REPORTS MAY NOT BE DATED PRIOR TO JANUARY 1, 2016.

(Note: The due date under the regulations for these reports is February 15, 2016, but as this is President's Day, a federal holiday, the deadline for filing these reports is being extended by one business day)

(U)New Entrants: Reports must be filed within 30 days of assuming a covered position. This also applies to employees assigned to a position in an "acting" capacity. However, no report is required if the employee occupied the position for less than 60 continuous days.

(U)Special Government Employees: Special Government Employees (SGE) are required to file an OGE-450 form upon each appointment or reappointment. SGE's typically must be re-appointed on an annual basis, and should file the applicable forms each year.

UNCLASSIFIED

UNCLASSIFIED

Title: (U) Annual Reporting Requirements for OGE-450 and CIC filers
Re: [REDACTED] 01/11/2016

b7E -13

(U)REPORTING COMPLIANCE

(U)The following reports are required:

(U)No later than 2/16/2016, all annual OGE-450 forms, with corresponding No Known Conflicts forms, or CIC forms, must be filed with division CDCs or Ethics POCs.

(U)No later than 4/15/2016, each division or office must certify, via lead, that the following actions have been completed.

- a. (U)Their list of OGE-450 and CIC filers has been updated and will be retained in the appropriate files for six years, along with the completed and reviewed OGE-450 and CIC forms.
- b. (U)All employees required to file an OGE-450 or CIC form have done so in accordance with section 5.5.2 of the FBI Ethics and Integrity Program Guide.
- c. (U)All OGE-450 and CIC forms have been reviewed for completeness and potential conflicts of interest in accordance with section 5.5.2 of the FBI Ethics and Integrity Program Guide. (Also see the OGE-450 Reviewers Aid enclosed with this EC for further guidance on technical and substantive review of these forms)
- d. (U)All corrective or remedial actions indicated by the foregoing reviews have been taken.

(U)If any of the above certifications cannot be made, they must be individually noted and explained. Following review, the CDC or Ethics POC must retain the completed OGE-450 and No Known Conflicts forms, or CIC forms in one location, as provided in section 5.5.2(h) of the FBI Ethics and Integrity Program Guide. Please note that compliance with these procedures is periodically audited by OIG and the Office of Government Ethics (OGE).

(U)SECURITY FINANCIAL DISCLOSURES RELATED TO SCI ACCESS

UNCLASSIFIED

UNCLASSIFIED

Title: (J) Annual Reporting Requirements for OGE-450 and CIC filers

Re: [REDACTED] 01/11/2016

b7E -13

(J)Please note that the requirement to file an OGE-450 or CIC form is independent of the requirement (for certain FBI personnel) to file a security-based financial disclosure report. The Security Financial Disclosure Form (SFDF) is administered by the Security Division based on the employee's access to SCI. The SFDF is not a substitute for filing an OGE-450 or CIC form. Nor is filing the OGE-450, or CIC form, a substitute for filing the SFDF. Please contact the Security Division, Internal Investigations Section, Analysis and Investigations Unit for additional information on the SFDF.

(J)Questions can be directed to the OIC POC for ethics-based financial disclosure: [REDACTED]

b6 -1
b7C -1
b7E -3

◆◆

UNCLASSIFIED

[REDACTED] (DO) (FBI)

b6 -1
b7C -1

From: [REDACTED] (DO) (FBI)

Sent: Friday, January 15, 2016 12:15 PM

To: [REDACTED] (OGC) (FBI); [REDACTED] (OGC) (FBI); [REDACTED] (OGC) (FBI); [REDACTED] (OGC) (FBI); [REDACTED] (INSD) (FBI); [REDACTED] (INSD) (FBI); [REDACTED] (DO) (FBI); [REDACTED] (OPA) (FBI); [REDACTED] (OGC) (FBI); [REDACTED] (DO) (FBI); [REDACTED] (DO) (FBI); [REDACTED] (CK) (FBI); [REDACTED] (OGC) (FBI); [REDACTED] (OGC) (FBI); [REDACTED] (OGC) (FBI); [REDACTED] (OPA) (FBI); [REDACTED] (OGC) (FBI); [REDACTED] (OGC) (FBI); [REDACTED] (OCA) (FBI); [REDACTED] (OEE) (FBI); [REDACTED] (DO) (FBI); [REDACTED] (DO) (FBI); [REDACTED] (OGC) (FBI); [REDACTED] (OGC) (FBI); [REDACTED] (INSD) (FBI); [REDACTED] (OPA) (FBI); [REDACTED] (DO) (FBI); [REDACTED] (DO) (FBI); [REDACTED] (DO) (FBI); [REDACTED] (DO) (FBI); [REDACTED] (INSD) (FBI); [REDACTED] (OGC) (FBI); [REDACTED] (OPA) (FBI); [REDACTED] (OGC) (FBI); [REDACTED] (OGC) (FBI); [REDACTED] (OGC) (FBI); [REDACTED] (DO) (FBI); [REDACTED] (DE) (FBI); [REDACTED] (INSD) (FBI); [REDACTED] (DO) (FBI); [REDACTED] (DO) (FBI); [REDACTED] (INSD) (FBI); [REDACTED] (DO) (FBI); [REDACTED] (OGC) (FBI); [REDACTED] (OGC) (FBI); [REDACTED] (OGC) (FBI); [REDACTED] (OPA) (FBI); [REDACTED] (OPA) (FBI); [REDACTED] (DO) (FBI); [REDACTED] (DO) (FBI); [REDACTED] (OGC) (FBI); [REDACTED] (OGC) (FBI); [REDACTED] (DO) (FBI); [REDACTED] (DO) (FBI); [REDACTED] (INSD) (FBI); [REDACTED] (OGC) (FBI); [REDACTED] (DO) (FBI); [REDACTED] (OGC) (FBI); [REDACTED] (INSD) (FBI); [REDACTED] (DO) (FBI); [REDACTED] (CYD) (FBI); [REDACTED] (INSD) (FBI); [REDACTED] (INSD) (FBI); [REDACTED] (OGC) (FBI); [REDACTED] (DO) (FBI); [REDACTED] (OGC) (FBI); [REDACTED] (DO) (FBI); [REDACTED] (DO) (FBI); [REDACTED] (DO) (FBI); [REDACTED] (OGC) (FBI); [REDACTED] (OGC) (FBI); [REDACTED] (DO) (FBI); [REDACTED] (DO) (FBI)

Subject: RE: Annual Reporting Requirements for OGE 450 and CIC Filers --- UNCLASSIFIED

Classification: UNCLASSIFIED

=====

TRANSITORY RECORD

FBI 18-CV-1833-7846

OGE 450

b6 -1
b7C -1

TRANSITORY RECORD

<< File: Annual Reporting Requirements for OGE-450 and CIC filers.pdf >>

All FBI OGE-450 filers are also required to complete an "Employee Certification -- No Known Conflicts of Interest with Federal Duties" form ("No Conflicts" form). The No Conflicts form must be completed each year and returned with the OGE-450 form.

No Known Conflicts Certification

Please make sure you get your supervisor to sign your OGE-450 before you turn it in. If you have any questions, please let me know.

[Redacted]

Administrative Management and Analysis Unit
Resource Planning Office/Director's Office
Room 9798

[Redacted]

b6 -1
b7C -1
b7E -3

Please visit the Administrative Management and Analysis Unit's webpage at AMAU

=====
Classification: UNCLASSIFIED

=====
Classification: UNCLASSIFIED

[redacted] (INSD)(FBI)

b6 -1
b7C -1

From: [redacted] (INSD)(FBI)

Sent: Friday, February 05, 2016 7:30 AM

To: [redacted] (DO) (FBI); [redacted] OGC)(FBI); [redacted]
[redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (INSD)
(FBI); [redacted] (DO) (FBI); [redacted] (OPA) (FBI);
[redacted] (OGC) (FBI); [redacted] (CK) (FBI);
[redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted]
(OGC) (FBI); [redacted] (OGC)(FBI); [redacted] (OGC)
(FBI); [redacted] (OEE) (FBI); [redacted] (DO) (FBI);
[redacted] (OGC)(FBI); [redacted] (OGC) (FBI); [redacted]
[redacted] (INSD) (FBI); [redacted] OPA) (FBI); [redacted]
(DO) (FBI); [redacted] (DO) (FBI); [redacted] (DO) (FBI); [redacted]
[redacted] (DO) (FBI); [redacted] (INSD)(FBI); [redacted] OGC)
(FBI); [redacted] (OPA) (FBI); [redacted] (OGC)(FBI);
[redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted]
[redacted] (DE) (FBI); [redacted] (DO) (FBI); [redacted] (DO) (FBI);
[redacted] (INSD)(FBI); [redacted] (OGC) (FBI); [redacted]
[redacted] OGC)(FBI); [redacted] OGC)(FBI); [redacted] (OPA) (FBI);
[redacted] (DO) (FBI); [redacted] (OGC) (FBI);
[redacted] (OGC) (FBI); [redacted] (DO) (FBI); [redacted]
(DO) (FBI); [redacted] (OGC)(FBI); RICHMAN, DANIEL C (DO) (OGA); [redacted]
[redacted] (OGC)(FBI); [redacted] (DO) (FBI); [redacted] (OGC)
(FBI); [redacted] (OGC) (FBI); [redacted] (INSD)(FBI);
[redacted] (CYD)(FBI); [redacted] (OGC) (FBI); [redacted]
[redacted] (DO) (FBI); [redacted] (OGC) (FBI); [redacted]
(DO) (FBI); [redacted] (DO) (FBI); [redacted] (DO)
(FBI); [redacted] (DO) (FBI); [redacted] (OGC) (FBI);
[redacted] OGC)(FBI); [redacted] (DO) (FBI)

Subject: RE: Annual Reporting Requirements for OGE 450 and CIC Filers --- UNCLASSIFIED

Classification: UNCLASSIFIED

TRANSITORY RECORD

[redacted]

b6 -1
b7C -1

Attached, please find a copy of my OGE-450 along with a signed copy the No Known Conflicts Certification.

Thank you,

[redacted]

FBI 18-CV-1833-7849

[Redacted]

b6 -1
b7C -1
b7E -3

Unit Chief, INSD Analysis Unit

JEH Room 3155

Desk: [Redacted]

Cell [Redacted]

From: [Redacted] (DO) (FBI)

Sent: Friday, February 05, 2016 7:02 AM

To: [Redacted] (OGC) (FBI); [Redacted] (OGC) (FBI); [Redacted] (OGC) (FBI); [Redacted] (OGC) (FBI);
(INSD) (FBI); [Redacted] (DO) (FBI); [Redacted] (OPA) (FBI); [Redacted] (OGC) (FBI);
(FBI); [Redacted] (CK) (FBI); [Redacted] (OGC) (FBI); [Redacted] (OGC) (FBI);
[Redacted] (OGC) (FBI); [Redacted] (OGC) (FBI); [Redacted] (OGC) (FBI); [Redacted] (OGC) (FBI);
[Redacted] (OEE) (FBI); [Redacted] (DO) (FBI); [Redacted] (OGC) (FBI); [Redacted] (OGC) (FBI);
(OGC) (FBI); [Redacted] (INSD) (FBI); [Redacted] (OPA) (FBI); [Redacted] (DO) (FBI);
[Redacted] (DO) (FBI); [Redacted] (DO) (FBI); [Redacted] (DO) (FBI); [Redacted] (INSD) (FBI);
(FBI); [Redacted] (OGC) (FBI); [Redacted] (OPA) (FBI); [Redacted] (OGC) (FBI);
[Redacted] (OGC) (FBI); [Redacted] (OGC) (FBI); [Redacted] (DE) (FBI); [Redacted] (DO) (FBI);
[Redacted] (DO) (FBI); [Redacted] (INSD) (FBI); [Redacted] (DO) (FBI); [Redacted] (INSD) (FBI);
[Redacted] (OGC) (FBI); [Redacted] (OGC) (FBI); [Redacted] (OGC) (FBI); [Redacted] (OGC) (FBI);
[Redacted] (OPA) (FBI); [Redacted] (DO) (FBI); [Redacted] (OGC) (FBI); [Redacted] (OGC) (FBI);
[Redacted] (OGC) (FBI); [Redacted] (DO) (FBI); [Redacted] (DO) (FBI); [Redacted] (OGC) (FBI);
RICHMAN, DANIEL C. (DO) (OGA); [Redacted] (OGC) (FBI); [Redacted] (DO) (FBI); [Redacted] (OGC) (FBI);
(OGC) (FBI); [Redacted] (OGC) (FBI); [Redacted] (INSD) (FBI); [Redacted] (CYD) (FBI);
[Redacted] (OGC) (FBI); [Redacted] (DO) (FBI); [Redacted] (OGC) (FBI); [Redacted] (DO) (FBI);
[Redacted] (DO) (FBI); [Redacted] (DO) (FBI); [Redacted] (DO) (FBI); [Redacted] (DO) (FBI);
[Redacted] (DO) (FBI); [Redacted] (OGC) (FBI); [Redacted] (OGC) (FBI); [Redacted] (DO) (FBI);

b6 -1
b7C -1

Subject: Annual Reporting Requirements for OGE 450 and CIC Filers --- UNCLASSIFIED

Classification: UNCLASSIFIED

TRANSITORY RECORD

Just an FYI. This is due 2/11/2016.

If you are receiving this email you are an OGE 450 filer. The deadline for filing the OGE 450 is 2/16/2016. They will be due to me by **COB Thursday, 2/11/2016** so I can respond to the Office of Integrity and Compliance (OIC) by their deadline.

<< File: Annual_Reporting_Requirements_for_OGE-450_and_CIC_filers.pdf >>

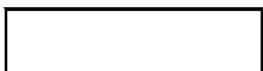
All FBI OGE-450 filers are also required to complete an "Employee Certification -- No Known Conflicts of Interest with Federal Duties" form ("No Conflicts" form). The No Conflicts form must be completed each year and returned with the OGE-450 form.

No Known Conflicts Certification

Please make sure you get your supervisor to sign your OGE-450 before you turn it in. If you have any

FBI 18-CV-1833-7850

questions, please let me know.

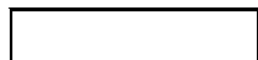


b6 -1
b7C -1
b7E -3

Administrative Management and Analysis Unit

Resource Planning Office/Director's Office

Room 9798



Please visit the Administrative Management and Analysis Unit's webpage at [AMAU](#)

=====
Classification: UNCLASSIFIED

=====
Classification: UNCLASSIFIED

(DO) (FBI)

b6 -1
b7C -1

From: (DO) (FBI)

Sent: Friday, February 05, 2016 7:02 AM

To: (OGC)(FBI); (OGC) (FBI); (DO) (FBI); (OGC) (FBI); (INSD) (FBI); (DO) (FBI); (OPA) (FBI); (OGC) (FBI); (CK) (FBI); (OGC) (FBI); (OGC) (FBI); (OGC) (FBI); (OGC) (FBI); (OEE) (FBI); (DO) (FBI); (OGC)(FBI); (OGC) (FBI); (OPA) (FBI); (DO) (FBI); (INSD) (FBI); (DO) (FBI); (DO) (FBI); (DO) (FBI); (INSD)(FBI); (OGC) (FBI); (OPA) (FBI); (OGC)(FBI); (OGC) (FBI); (OGC) (FBI); (OGC) (FBI); (DE) (FBI); (DO) (FBI); (INSD)(FBI); (DO) (FBI); (INSD)(FBI); (OGC) (FBI); (OGC) (FBI); (OGC) (FBI); (OPA) (FBI); (DO) (FBI); (OGC) (FBI); (OGC) (FBI); (DO) (FBI); (OGC) (FBI); (DO) (FBI); (OGC) (FBI); (OGC) (FBI); (INSD)(FBI); (CYD)(FBI); (OGC) (FBI); (DO) (FBI); (OGC) (FBI); (DO) (FBI); (DO) (FBI); (DO) (FBI); (DO) (FBI); (OGC) (FBI); (OGC)(FBI); (DO) (FBI)

Subject: Annual Reporting Requirements for OGE 450 and CIC Filers --- UNCLASSIFIED

Attachments: Annual_Reporting_Requirements_for_OGE-450_and_CIC_filers.pdf

Classification: UNCLASSIFIED

TRANSITORY RECORD

Just an FYI. This is due 2/11/2016.

If you are receiving this email you are an OGE 450 filer. The deadline for filing the OGE 450 is 2/16/2016. They will be due to me by **COB Thursday, 2/11/2016** so I can respond to the Office of Integrity and Compliance (OIC) by their deadline.

<<Annual_Reporting_Requirements_for_OGE-450_and_CIC_filers.pdf>>

All FBI OGE-450 filers are also required to complete an "Employee Certification - No Known Conflicts of Interest with Federal Duties" form ("No Conflicts" form). The No Conflicts form must be

FBI 18-CV-1833-7852

=====

completed each year and returned with the OGE-450 form.

No Known Conflicts Certification

Please make sure you get your supervisor to sign your OGE-450 before you turn it in. If you have any questions, please let me know.

[Redacted]

b6 -1
b7C -1
b7E -3

Administrative Management and Analysis Unit

Resource Planning Office/Director's Office

Room 9798

[Redacted]

Please visit the Administrative Management and Analysis Unit's webpage at AMAU

=====
Classification: UNCLASSIFIED

[Redacted]

b6 -1
b7C -1
b7E -3

Administrative Management and Analysis Unit

Resource Planning Office/Director's Office

Room 9798

[Redacted]

Please visit the Administrative Management and Analysis Unit's webpage at [AMAU](#)

=====
Classification: UNCLASSIFIED

[REDACTED] RMD) (FBI)

b6 -1
b7C -1
b7E -3

From: [REDACTED] (RMD) (FBI)

Sent: Thursday, February 11, 2016 3:28 PM

To: [REDACTED] (CTD) (OGA); [REDACTED] (BA) (OGA);
[REDACTED] (OGC) (OGA); [REDACTED] (CTD) (OGA); [REDACTED]
[REDACTED] (CTD) (OGA); [REDACTED] (CYD) (OGA); [REDACTED]
(RMD) (OGA); [REDACTED] (WF) (OGA); [REDACTED] (CTD) (OGA);
[REDACTED] (WF) (OGA); [REDACTED] (CTD) (OGA); [REDACTED]
[REDACTED] (CTD) (OGA); [REDACTED] (CTD) (OGA); [REDACTED]
(CTD) (OGA); [REDACTED] (DN) (OGA); [REDACTED] (OGC) (OGA); [REDACTED]
[REDACTED] (DI) (OGA); [REDACTED] (CD) (OGA); [REDACTED] (IP) (OGA);
[REDACTED] (CTD) (OGA); [REDACTED] (BA) (OGA); [REDACTED]
[REDACTED] (LR) (OGA); [REDACTED] (CTD) (OGA); [REDACTED] (CI)
(OGA); [REDACTED] (WF) (FBI); [REDACTED] (HO) (OGA); [REDACTED]
[REDACTED] (WF) (OGA); [REDACTED] (PG) (OGA); [REDACTED] (CV)
(OGA); [REDACTED] (DO) (OGA); [REDACTED] (WMD) (OGA);
[REDACTED] (AT) (OGA); [REDACTED] (FD) (OGA); [REDACTED]
[REDACTED] (CTD) (OGA); [REDACTED] (SF) (OGA); [REDACTED]
(CTD) (OGA); [REDACTED] (CTD) (OGA); [REDACTED] (SD)
(OGA); [REDACTED] (WF) (FBI); [REDACTED] (CTD) (OGA); [REDACTED]
[REDACTED] (CTD) (OGA); [REDACTED] (OGC) (OGA); [REDACTED]
(CTD) (OGA); [REDACTED] (DI) (OGA); [REDACTED] (CTD) (OGA);
[REDACTED] (CTD) (OGA); [REDACTED] (BA) (OGA); [REDACTED]
[REDACTED] (CYD) (OGA); [REDACTED] (WF) (OGA); [REDACTED]
[REDACTED] (NO) (OGA); [REDACTED] (CD) (OGA); [REDACTED] (WMD)
(OGA); [REDACTED] (OTD) (OGA); [REDACTED] (BA) (OGA);
[REDACTED] (WF) (OGA); [REDACTED] (FD) (OGA); [REDACTED]
[REDACTED] (CTD) (OGA); [REDACTED] (CYD) (OGA); [REDACTED]
[REDACTED] (AL) (OGA); [REDACTED] (WF) (OGA); [REDACTED]
(CTD) (OGA); [REDACTED] (CTD) (OGA); [REDACTED] (OGC)
(OGA); [REDACTED] (DN) (OGA); [REDACTED] (CD) (OGA); [REDACTED]
[REDACTED] (NSB) (OGA); [REDACTED] (CYD) (OGA); [REDACTED]
(CYD) (OGA); [REDACTED] (CTD) (OGA); [REDACTED] (HN) (OGA);
[REDACTED] (KC) (OGA); [REDACTED] (HIG) (OGA); [REDACTED]
[REDACTED] (CD) (OGA); [REDACTED] (CTD) (OGA); [REDACTED] (CTD) (OGA);
[REDACTED] (WF) (OGA); [REDACTED] (TSC) (OGA); [REDACTED]
[REDACTED] (KC) (OGA); [REDACTED] (WMD) (OGA); [REDACTED] (HO)
(OGA); [REDACTED] (WMD) (OGA);
RICHMAN, DANIEL C (DO) (OGA); [REDACTED] (OPE) (OGA); [REDACTED]
(OGC) (OGA); [REDACTED] (CYD) (CON); [REDACTED] (CTD) (OGA);
[REDACTED] (CTD) (OGA); [REDACTED] (WF) (OGA); [REDACTED]
[REDACTED] (OGC) (OGA); [REDACTED] (CTD) (OGA); [REDACTED]
[REDACTED] (CTD) (OGA); [REDACTED] (WF) (OGA); [REDACTED]
(CTD) (OGA); [REDACTED] (WF) (OGA); [REDACTED]
[REDACTED] (DI) (OGA); [REDACTED] (MM) (OGA);
[REDACTED] (CTD) (OGA); [REDACTED] (OGC) (CON);
[REDACTED] (NY) (OGA); [REDACTED] (BA) (OGA); [REDACTED]
[REDACTED] (CTD) (OGA); [REDACTED] (CTD) (OGA); [REDACTED]

FBI 18-CV-1833-7864

(CYD) (OGA); [REDACTED] (CTD) (OGA); [REDACTED] (CTD)
(OGA); [REDACTED] (CTD) (OGA); [REDACTED] (RMD) (OGA);
[REDACTED] (HN) (OGA); [REDACTED] (HN) (OGA); [REDACTED]
[REDACTED] (CYD) (OGA); [REDACTED] (CTD) (OGA); [REDACTED] (DI)
(OGA); [REDACTED] (CTD) (OGA); [REDACTED] (WF) (OGA);
[REDACTED] (NY) (OGA); [REDACTED] (CTD) (OGA); [REDACTED]
[REDACTED] (WF) (OGA); [REDACTED] (NSB) (OGA); [REDACTED]
(OGC) (OGA); [REDACTED] (AQ) (OGA); [REDACTED] (CTD) (OGA);
[REDACTED] (WMD) (OGA); [REDACTED] (CTD) (OGA);
[REDACTED] (CTD) (OGA); [REDACTED] (OGC) (FBI); [REDACTED]
[REDACTED] (OGC) (OGA); [REDACTED] (DI) (CON); [REDACTED]
[REDACTED] (WF) (OGA); [REDACTED] (CTD) (OGA); [REDACTED] (WF)
(OGA); [REDACTED] (CTD) (OGA); [REDACTED] (CYD) (OGA);
[REDACTED] (NY) (OGA); [REDACTED] (CTD) (OGA);
[REDACTED] (CTD) (OGA); [REDACTED] (IP) (OGA); [REDACTED]
[REDACTED] (CYD) (CON); [REDACTED] (SU) (OGA); [REDACTED]
[REDACTED] (CTD) (OGA); [REDACTED] (CTD) (CON); [REDACTED]
[REDACTED] (WMD) (OGA); [REDACTED] (ED) (CON); [REDACTED]
(WMD) (OGA); [REDACTED] (LD) (OGA); [REDACTED] (CYD) (OGA);
[REDACTED] (WF) (OGA); [REDACTED] (OGC) (OGA); [REDACTED]
[REDACTED] (TSC) (OGA); [REDACTED] (CYD) (OGA); [REDACTED] (BA)
(OGA); [REDACTED] (CE) (OGA); [REDACTED] (IR) (OGA);
[REDACTED] (DI) (OGA); [REDACTED] (OGC) (OGA); [REDACTED]
[REDACTED] (NK) (OGA); [REDACTED] (CD) (CON); [REDACTED] (CTD)
(OGA); [REDACTED] (CYD) (OGA); [REDACTED] (NY) (OGA);
[REDACTED] (CTD) (OGA); [REDACTED] (AQ) (OGA); [REDACTED]
[REDACTED] (CTD) (OGA); [REDACTED] (CID) (OGA); [REDACTED] (HIG)
(OGA); [REDACTED] (SE) (OGA); [REDACTED] (SA) (DTL); [REDACTED]
[REDACTED] (OIO) (OGA); [REDACTED] (BS) (OGA); [REDACTED] (TSC)
(OGA); [REDACTED] (CTD) (OGA); [REDACTED] (CTD) (OGA); [REDACTED]
[REDACTED] (OGC) (OGA); [REDACTED] (CTD) (OGA); [REDACTED] (IR)
(OGA); [REDACTED] (NY) (OGA); [REDACTED] (CTD) (OGA); [REDACTED]
[REDACTED] (NSB) (OGA); [REDACTED] (DL) (OGA); [REDACTED] (CD)
(OGA); [REDACTED] (CTD) (OGA); [REDACTED] (HIG) (OGA); [REDACTED]
[REDACTED] (CTD) (OGA); [REDACTED] (DI) (OGA); [REDACTED] (CTD)
(OGA); [REDACTED] (DI) (OGA); [REDACTED] (NY) (OGA); [REDACTED]
[REDACTED] (DI) (OGA); [REDACTED] (CTD) (OGA); [REDACTED] (CTD)
(OGA); [REDACTED] (CTD) (OGA); [REDACTED] (CTD) (OGA); [REDACTED]
[REDACTED] (SA) (DTL); [REDACTED] (WF) (OGA); [REDACTED]
[REDACTED] (OGC) (CON); [REDACTED] (NY) (OGA); [REDACTED] (NY)
(OGA); [REDACTED] (CYD) (OGA); [REDACTED] (CYD) (OGA);
[REDACTED] (IR) (OGA); [REDACTED] (CD) (OGA); [REDACTED]
[REDACTED] (BA) (OGA); [REDACTED] (OIO) (OGA); [REDACTED]
[REDACTED] (CTD) (OGA); [REDACTED] (CI) (OGA); [REDACTED] (IP) (OGA);
[REDACTED] (CTD) (OGA); [REDACTED] (CTD) (OGA); [REDACTED] (CTD) (OGA);
[REDACTED] (CI) (OGA); [REDACTED] (CTD) (OGA); [REDACTED]
[REDACTED] (IOD) (OGA); [REDACTED] (CD) (OGA); [REDACTED]
(CTD) (OGA); [REDACTED] (CTD) (OGA); [REDACTED] (CTD) (OGA);
[REDACTED] (CTD) (OGA); [REDACTED] (CTD) (OGA); [REDACTED]
(WF) (OGA); [REDACTED] (CTD) (OGA); [REDACTED] (TP) (OGA);

b6 -1
b7C -1
b7E -3

[REDACTED] (CTD) (OGA); [REDACTED] (NY) (OGA); [REDACTED]
[REDACTED] (KX) (OGA); [REDACTED] (LD) (CON); [REDACTED] (LD)
(OGA); [REDACTED] (WMD) (OGA); [REDACTED] (DI) (OGA);
[REDACTED] (NY) (OGA); [REDACTED] (CTD) (OGA); [REDACTED]
[REDACTED] (WMD) (OGA); [REDACTED] (CYD) (OGA); [REDACTED]
[REDACTED] (CTD) (OGA); [REDACTED] (CTD) (OGA); [REDACTED] (WF)
(OGA); [REDACTED] (WF) (OGA); [REDACTED] (PH) (OGA); [REDACTED]
[REDACTED] (OGC) (OGA); [REDACTED] (OM) (OGA); [REDACTED]
[REDACTED] (CTD) (OGA); [REDACTED] (SECD) (OGA);
[REDACTED] (CTD) (OGA); [REDACTED]
[REDACTED] (CTD) (OGA); [REDACTED] (CTD) (OGA); [REDACTED] (PH)
(OGA); [REDACTED] (OTD) (OGA); [REDACTED] (OGC) (OGA); [REDACTED]
[REDACTED] (CTD) (OGA); [REDACTED] (CTD) (OGA); [REDACTED]
[REDACTED] (RMD) (OGA); [REDACTED] (OGC) (OGA); [REDACTED]
[REDACTED] (BF) (OGA); [REDACTED] (HO) (OGA); [REDACTED]
[REDACTED] (CTD) (CON); [REDACTED] (CYD) (OGA); [REDACTED] (IR)
(OGA); [REDACTED] (CTD) (OGA); [REDACTED] (CTD) (OGA);
[REDACTED] (CTD) (OGA); [REDACTED] (CI) (OGA); [REDACTED]
[REDACTED] (CYD) (OGA); [REDACTED] (CTD) (OGA); [REDACTED] (OGC)
(OGA); [REDACTED] (NY) (OGA); [REDACTED] (OGC) (CON);
[REDACTED] (CI) (OGA); [REDACTED] (CTD) (OGA); [REDACTED]
[REDACTED] (CI) (OGA); [REDACTED] (OGC) (OGA); [REDACTED]
(CYD) (CON); [REDACTED] (SECD) (OGA); [REDACTED] (SecD) (OGA);
[REDACTED] (CTD) (OGA); [REDACTED] (CTD) (OGA); [REDACTED]
[REDACTED] (CYD) (OGA); [REDACTED] (CTD) (OGA); [REDACTED]
[REDACTED] (SA) (TFO); [REDACTED] (CTD) (OGA); [REDACTED] (CTD)
(OGA); [REDACTED] (SE) (OGA); [REDACTED] (CTD) (CON);
[REDACTED] (DI) (OGA); [REDACTED] (SL) (OGA); [REDACTED]
[REDACTED] (CTD) (OGA); [REDACTED] (CTD) (OGA); [REDACTED] (CTD) (OGA);
[REDACTED] (CTD) (OGA); [REDACTED] (CTD) (OGA); [REDACTED]
[REDACTED] (CI) (OGA); [REDACTED] (SF) (OGA); [REDACTED] (CYD)
(OGA); [REDACTED] (WF) (OGA); [REDACTED] (NSB) (OGA); [REDACTED]
[REDACTED] (NK) (OGA); [REDACTED] (WMD) (OGA); [REDACTED]
(CTD) (OGA); [REDACTED] (WF) (OGA); [REDACTED] (CTD) (OGA);
[REDACTED] (CID) (OGA); [REDACTED] (CD) (OGA); [REDACTED]
[REDACTED] (NSB) (OGA); [REDACTED] (CTD) (OGA); [REDACTED]
(CYD) (OGA); [REDACTED] (DO) (OGA); [REDACTED]
[REDACTED] (CTD) (OGA); [REDACTED] (WMD) (OGA); [REDACTED]
[REDACTED] (CTD) (OGA); [REDACTED]
(CYD) (OGA); [REDACTED] (NY) (OGA); [REDACTED] (CTD) (OGA);
[REDACTED] (MP) (OGA); [REDACTED] (CTD) (OGA); [REDACTED]
[REDACTED] (NY) (OGA); [REDACTED] (HO) (OGA); [REDACTED]
[REDACTED] (CID) (OGA); [REDACTED]
[REDACTED] (DI) (OGA); [REDACTED] (CTD) (OGA); [REDACTED] (CTD)
(OGA); [REDACTED] (BS) (OGA); [REDACTED] (WMD) (OGA); [REDACTED]
[REDACTED] (CTD) (OGA); [REDACTED] (DL) (OGA); [REDACTED]
[REDACTED] (CTD) (OGA); [REDACTED] (WMD) (OGA); [REDACTED] (CYD)
(OGA); [REDACTED] (NY) (OGA); [REDACTED] (WMD) (OGA); [REDACTED]
[REDACTED] (NK) (OGA); [REDACTED] (RMD) (OGA); [REDACTED]
[REDACTED] (OGC) (OGA); [REDACTED] (CTD) (OGA); [REDACTED] (SF)

b6 -1
b7C -1
b7E -3

(OGA); [redacted] (CTD) (OGA); [redacted] (PH) (CON); [redacted]
[redacted] (BA) (CON); [redacted] (NY) (CON); [redacted]
[redacted] (BS) (CON); [redacted] (CE) (CON); [redacted] (DI)
(CON); [redacted] (CYD) (OGA); [redacted] (HRD) (CON);
[redacted] (BS) (FBI); [redacted] (MP) (CON); [redacted]
(KX) (CON); [redacted] (DI) (CON); [redacted] (CYD) (FBI);
[redacted] (NY) (CON); [redacted] (CYD) (OGA);
[redacted] (JK) (CON); [redacted] (DI) (CON); [redacted]
(HRD) (CON); [redacted] (PX) (CON); [redacted]
(WF) (CON); [redacted] (DL) (CON); [redacted] (NY) (FBI);
[redacted] (CYD) (FBI); [redacted] (DI) (CON); [redacted]
[redacted] (DI) (CON); [redacted] (DI) (CON); [redacted] (SA)
(CON); [redacted] (SE) (CON); [redacted] (DI) (CON); [redacted]
[redacted] (NY) (CON); [redacted] (WF) (CON); [redacted] (LA) (OGA); [redacted]
[redacted] (WF) (CON); [redacted] (BS) (FBI); [redacted]
[redacted] (DI) (CON); [redacted] (NY) (FBI); [redacted]
[redacted] (NH) (CON); [redacted] (NY) (FBI); [redacted] (PX)
(CON); [redacted] (WF) (CON); [redacted] (SA) (CON)

b6 -1
b7C -1

Subject: Mandatory Training - Due 2/29/2016 --- UNCLASSIFIED

Classification: UNCLASSIFIED
=====

TRANSITORY RECORD

Please complete the mandatory FBI Records Management: Records Management for All course by 2/29/2016. This course is required for all FBI employees, contractors, task force officers and detailees.

Thank you,

[redacted]

b6 -1
b7C -1
b7E -3

[redacted]

Training Liaison & Change Management Specialist

Records Management Division

[redacted]

office

fax

blackberry

=====
Classification: UNCLASSIFIED

FBI 18-CV-1833-7867

[redacted] (OGC) (FBI)

b6 -1
b7C -1

From: [redacted] (OGC) (FBI)
Sent: Monday, November 21, 2016 8:39 AM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: FW: Dan Richman EC --- UNCLASSIFIED

Classification: UNCLASSIFIED
=====

Good morning Mr. Richman,

I work for GC Baker and recently drafted your reappointment EC. Please find below instructions from OIC to file an OGE-450.

Thank you and have a great Thanksgiving.

[redacted]

b6 -1
b7C -1
b7E -3

Management and Program Analyst

Office of the General Counsel

935 Pennsylvania Ave., N.W.

Washington, DC 20535

Desk Phone: [redacted]

Blackberry: [redacted]

Fax: [redacted]

From: KELLEY, PATRICK W. (DO) (FBI)
Sent: Monday, November 14, 2016 4:13 PM
To: [redacted] (OGC) (FBI)
Cc: [redacted] (DO) (FBI); [redacted] (DO) (FBI)
Subject: RE: Dan Richman EC --- UNCLASSIFIED

b6 -1
b7C -1

Classification: UNCLASSIFIED
=====

[redacted] I approved the EC. Please remind Mr. Richman of the requirement to file an OGE-450, Confidential Financial Disclosure Report. If you or he has any questions in this regard, please contact OIC POC [redacted] Thanks.

From: [redacted] (OGC) (FBI)
Sent: Monday, November 14, 2016 12:47 PM
To: KELLEY, PATRICK W. (DO) (FBI)
Subject: Dan Richman EC --- UNCLASSIFIED

b6 -1
b7C -1

Classification: UNCLASSIFIED
=====

Good afternoon AD Kelley,

I wanted to put on your radar an EC that is currently pending your approval in Sentinel. Dan Richman's term expired on June 30, 2016 and OGC worked on drafting his reappointment letter. Per the original EC, you were on the chain of approvals before the document was finalized. Therefore, I included you in the reappointment EC. Please let me know if you have any questions or concerns. The EC has been approved by OGC's Chief of Staff and GC Baker.

Best,

[redacted]

b6 -1
b7C -1
b7E -3

Management and Program Analyst

Office of the General Counsel

935 Pennsylvania Ave., N.W.

Washington, DC 20535

Desk Phone:

[redacted]

Blackberry:

[redacted]

Fax

[redacted]

=====
Classification: UNCLASSIFIED

=====
Classification: UNCLASSIFIED

=====
Classification: UNCLASSIFIED

RICHMAN, DANIEL C. (DO) (OGA)

From: RICHMAN, DANIEL C. (DO) (OGA)
Sent: Wednesday, January 11, 2017 12:12 PM
To: [REDACTED] (OGC) (FBI)
Subject: RE: Dan Richman EC --- UNCLASSIFIED

b6 -1
b7C -1

Classification: UNCLASSIFIED
=====

Sorry for my delay in responding. I couldn't get on to the high side, but am now on and will take care of this filing

Thx

Dan richman

From: [REDACTED] (OGC) (FBI)
Sent: Monday, November 21, 2016 8:39 AM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: FW: Dan Richman EC --- UNCLASSIFIED

b6 -1
b7C -1

Classification: UNCLASSIFIED
=====

Good morning Mr. Richman,

I work for GC Baker and recently drafted your reappointment EC. Please find below instructions from OIC to file an OGE-450.

Thank you and have a great Thanksgiving.

[REDACTED]

b6 -1
b7C -1
b7E -3

Management and Program Analyst

Office of the General Counsel

935 Pennsylvania Ave., N.W.

Washington, DC 20535

Desk Phone: [REDACTED]

Blackberry: [REDACTED]

Fax: [REDACTED]

FBI 18-CV-1833-7870

From: KELLEY, PATRICK W. (DO) (FBI)
Sent: Monday, November 14, 2016 4:13 PM
To: [REDACTED] (OGC) (FBI)
Cc: [REDACTED] (DO) (FBI); [REDACTED] (DO) (FBI)
Subject: RE: Dan Richman EC --- UNCLASSIFIED

b6 -1
b7C -1

Classification: UNCLASSIFIED
=====

[REDACTED] I approved the EC. Please remind Mr. Richman of the requirement to file an OGE-450, Confidential Financial Disclosure Report. If you or he has any questions in this regard, please contact OIC POC [REDACTED] Thanks.

From: [REDACTED] (OGC) (FBI)
Sent: Monday, November 14, 2016 12:47 PM
To: KELLEY, PATRICK W. (DO) (FBI)
Subject: Dan Richman EC --- UNCLASSIFIED

b6 -1
b7C -1

Classification: UNCLASSIFIED
=====

Good afternoon AD Kelley,

I wanted to put on your radar an EC that is currently pending your approval in Sentinel. Dan Richman's term expired on June 30, 2016 and OGC worked on drafting his reappointment letter. Per the original EC, you were on the chain of approvals before the document was finalized. Therefore, I included you in the reappointment EC. Please let me know if you have any questions or concerns. The EC has been approved by OGC's Chief of Staff and GC Baker.

Best,

[REDACTED]

b6 -1
b7C -1
b7E -3

Management and Program Analyst

Office of the General Counsel

935 Pennsylvania Ave., N.W.

Washington, DC 20535

Desk Phone: [REDACTED]

Blackberry: [REDACTED]

Fax: [REDACTED]

=====
Classification: UNCLASSIFIED

FBI 18-CV-1833-7871

=====
Classification: UNCLASSIFIED

=====
Classification: UNCLASSIFIED

=====
Classification: UNCLASSIFIED

[redacted] (OGC) (FBI)

b6 -1
b7C -1

From: [redacted] (OGC) (FBI)
Sent: Wednesday, January 11, 2017 12:29 PM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: RE: Dan Richman EC --- UNCLASSIFIED

Classification: UNCLASSIFIED
=====

Good morning,

No apologies necessary! Thank you so much for your help.

Happy New Year!

[redacted]

b6 -1
b7C -1
b7E -3

Management and Program Analyst

Office of the General Counsel

935 Pennsylvania Ave., N.W.

Washington, DC 20535

Desk Phone: [redacted]

Blackberry: [redacted]

Fax: [redacted]

From: RICHMAN, DANIEL C. (DO) (OGA)
Sent: Wednesday, January 11, 2017 12:12 PM
To: [redacted] (OGC) (FBI)
Subject: RE: Dan Richman EC --- UNCLASSIFIED

b6 -1
b7C -1

Classification: UNCLASSIFIED
=====

Sorry for my delay in responding. I couldn't get on to the high side, but am now on and will take care of this filing

Thx

Dan richman

FBI 18-CV-1833-7873

From: [REDACTED] (OGC) (FBI)
Sent: Monday, November 21, 2016 8:39 AM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: FW: Dan Richman EC --- UNCLASSIFIED

b6 -1
b7C -1

Classification: UNCLASSIFIED
=====

Good morning Mr. Richman,

I work for GC Baker and recently drafted your reappointment EC. Please find below instructions from OIC to file an OGE-450.

Thank you and have a great Thanksgiving.

[REDACTED]

b6 -1
b7C -1
b7E -3

Management and Program Analyst

Office of the General Counsel

935 Pennsylvania Ave., N.W.

Washington, DC 20535

Desk Phone: [REDACTED]

Blackberry: [REDACTED]

Fax: [REDACTED]

From: KELLEY, PATRICK W. (DO) (FBI)
Sent: Monday, November 14, 2016 4:13 PM
To: [REDACTED] (OGC) (FBI)
Cc: [REDACTED] (DO) (FBI); [REDACTED] (DO) (FBI)
Subject: RE: Dan Richman EC --- UNCLASSIFIED

b6 -1
b7C -1

Classification: UNCLASSIFIED
=====

[REDACTED] I approved the EC. Please remind Mr. Richman of the requirement to file an OGE-450, Confidential Financial Disclosure Report. If you or he has any questions in this regard, please contact OIC POC [REDACTED] Thanks.

From: [REDACTED] (OGC) (FBI)
Sent: Monday, November 14, 2016 12:47 PM
To: KELLEY, PATRICK W. (DO) (FBI)
Subject: Dan Richman EC --- UNCLASSIFIED

b6 -1
b7C -1

Classification: UNCLASSIFIED

FBI 18-CV-1833-7874

=====

Good afternoon AD Kelley,

I wanted to put on your radar an EC that is currently pending your approval in Sentinel. Dan Richman's term expired on June 30, 2016 and OGC worked on drafting his reappointment letter. Per the original EC, you were on the chain of approvals before the document was finalized. Therefore, I included you in the reappointment EC. Please let me know if you have any questions or concerns. The EC has been approved by OGC's Chief of Staff and GC Baker.

Best,

[Redacted]

Management and Program Analyst

Office of the General Counsel

935 Pennsylvania Ave., N.W.

Washington, DC 20535

Desk Phone:

[Redacted]

Blackberry

[Redacted]

Fax:

[Redacted]

=====
Classification: UNCLASSIFIED

=====
Classification: UNCLASSIFIED

=====
Classification: UNCLASSIFIED

=====
Classification: UNCLASSIFIED

=====
Classification: UNCLASSIFIED

b6 -1
b7C -1
b7E -3

RICHMAN, DANIEL C. (DO) (OGA)

From: RICHMAN, DANIEL C. (DO) (OGA)
Sent: Wednesday, January 11, 2017 12:33 PM
To: [REDACTED] (OGC) (FBI)
Subject: RE: Dan Richman EC --- UNCLASSIFIED

b6 -1
b7C -1

Classification: UNCLASSIFIED
=====

While I have you = [REDACTED] mentioned that I need to reup my OGE training. But there's no module for that in my virtual cart. Do you know where I go for that?

Thx

Dan richman

From: [REDACTED] (OGC) (FBI)
Sent: Wednesday, January 11, 2017 12:29 PM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: RE: Dan Richman EC --- UNCLASSIFIED

b6 -1
b7C -1

Classification: UNCLASSIFIED
=====

Good morning,

No apologies necessary! Thank you so much for your help.

Happy New Year!

[REDACTED]

Management and Program Analyst
Office of the General Counsel
935 Pennsylvania Ave., N.W.
Washington, DC 20535
Desk Phone: [REDACTED]
Blackberry: [REDACTED]
Fax: [REDACTED]

b6 -1
b7C -1
b7E -3

From: RICHMAN, DANIEL C. (DO) (OGA)
Sent: Wednesday, January 11, 2017 12:12 PM
To: [REDACTED] (OGC) (FBI)
Subject: RE: Dan Richman EC --- UNCLASSIFIED

b6 -1
b7C -1

Classification: UNCLASSIFIED

Sorry for my delay in responding. I couldn't get on to the high side, but am now on and will take care of this filing

Thx

Dan richman

From: [REDACTED] (OGC) (FBI)
Sent: Monday, November 21, 2016 8:39 AM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: FW: Dan Richman EC --- UNCLASSIFIED

b6 -1
b7C -1

Classification: UNCLASSIFIED

Good morning Mr. Richman,

I work for GC Baker and recently drafted your reappointment EC. Please find below instructions from OIC to file an OGE-450.

Thank you and have a great Thanksgiving,

[REDACTED]
Management and Program Analyst
Office of the General Counsel
935 Pennsylvania Ave., N.W.
Washington, DC 20535
Desk Phone: [REDACTED]
Blackberry: [REDACTED]
Fax: [REDACTED]

b6 -1
b7C -1
b7E -3

From: KELLEY, PATRICK W. (DO) (FBI)
Sent: Monday, November 14, 2016 4:13 PM
To: [REDACTED] (OGC) (FBI)
Cc: [REDACTED] (DO) (FBI); [REDACTED] (DO) (FBI)
Subject: RE: Dan Richman EC --- UNCLASSIFIED

b6 -1
b7C -1

Classification: UNCLASSIFIED

[REDACTED] I approved the EC. Please remind Mr. Richman of the requirement to file an OGE-450, Confidential Financial Disclosure Report. If you or he has any questions in this regard, please contact OIC POC [REDACTED] Thanks.

FBI 18-CV-1833-7877

From: [redacted] (OGC) (FBI)
Sent: Monday, November 14, 2016 12:47 PM
To: KELLEY, PATRICK W. (DO) (FBI)
Subject: Dan Richman EC --- UNCLASSIFIED

b6 -1
b7C -1

Classification: UNCLASSIFIED
=====

Good afternoon AD Kelley,

I wanted to put on your radar an EC that is currently pending your approval in Sentinel. Dan Richman's term expired on June 30, 2016 and OGC worked on drafting his reappointment letter. Per the original EC, you were on the chain of approvals before the document was finalized. Therefore, I included you in the reappointment EC. Please let me know if you have any questions or concerns. The EC has been approved by OGC's Chief of Staff and GC Baker.

Best,

[redacted]
Management and Program Analyst
Office of the General Counsel
935 Pennsylvania Ave., N.W.
Washington, DC 20535
Desk Phone [redacted]
Blackberry [redacted]
Fax: [redacted]

b6 -1
b7C -1
b7E -3

=====
Classification: UNCLASSIFIED

=====
Classification: UNCLASSIFIED

=====
Classification: UNCLASSIFIED

=====
Classification: UNCLASSIFIED

=====
Classification: UNCLASSIFIED

=====
Classification: UNCLASSIFIED

[redacted] (OGC) (FBI)

b6 -1
b7C -1

From: [redacted] (OGC) (FBI)
Sent: Wednesday, January 11, 2017 12:38 PM
To: RICHMAN, DANIEL C. (DO) (OGA); [redacted] (DO) (FBI)
Subject: FW: Dan Richman EC --- UNCLASSIFIED

Classification: UNCLASSIFIED
=====

Hi Dan,

I believe there is training available on OIG's website, but I have copied [redacted] from OIG's ethics office to confirm and provide any additional guidance.

b6 -1
b7C -1
b7E -3

Thank you, [redacted]

[redacted]
Management and Program Analyst
Office of the General Counsel
935 Pennsylvania Ave., N.W.
Washington, DC 20535
Desk Phone [redacted]
Blackberry [redacted]
Fax [redacted]

From: RICHMAN, DANIEL C. (DO) (OGA)
Sent: Wednesday, January 11, 2017 12:33 PM
To: [redacted] (OGC) (FBI)
Subject: RE: Dan Richman EC --- UNCLASSIFIED

b6 -1
b7C -1

Classification: UNCLASSIFIED
=====

While I have you - [redacted] mentioned that I need to reup my OGE training. But there's no module for that in my virtual cart. Do you know where I go for that?

Thx

Dan richman

From: [redacted] (OGC) (FBI)
Sent: Wednesday, January 11, 2017 12:29 PM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: RE: Dan Richman EC --- UNCLASSIFIED

b6 -1
b7C -1

Classification: UNCLASSIFIED

Good morning,

No apologies necessary! Thank you so much for your help.

Happy New Year!

[REDACTED]
Management and Program Analyst
Office of the General Counsel
935 Pennsylvania Ave., N.W.
Washington, DC 20535
Desk Phone [REDACTED]
Blackberry [REDACTED]
Fax [REDACTED]

b6 -1
b7C -1
b7E -3

From: RICHMAN, DANIEL C. (DO) (OGA)
Sent: Wednesday, January 11, 2017 12:12 PM
To: [REDACTED] (OGC) (FBI)
Subject: RE: Dan Richman EC --- UNCLASSIFIED

b6 -1
b7C -1

Classification: UNCLASSIFIED

Sorry for my delay in responding. I couldn't get on to the high side, but am now on and will take care of this filing

Thx

Dan richman

From: [REDACTED] (OGC) (FBI)
Sent: Monday, November 21, 2016 8:39 AM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: FW: Dan Richman EC --- UNCLASSIFIED

b6 -1
b7C -1

Classification: UNCLASSIFIED

Good morning Mr. Richman,

I work for GC Baker and recently drafted your reappointment EC. Please find below instructions from OIC to file an OGE-450.

Thank you and have a great Thanksgiving,

[REDACTED]
Management and Program Analyst
Office of the General Counsel
935 Pennsylvania Ave., N.W.
Washington, DC 20535
Desk Phone [REDACTED]
Blackberry [REDACTED]
Fax: [REDACTED]

b6 -1
b7C -1
b7E -3

From: KELLEY, PATRICK W. (DO) (FBI)
Sent: Monday, November 14, 2016 4:13 PM
To: [REDACTED] (OGC) (FBI)
Cc: [REDACTED] (DO) (FBI); [REDACTED] (DO) (FBI)
Subject: RE: Dan Richman EC --- UNCLASSIFIED

b6 -1
b7C -1

Classification: UNCLASSIFIED
=====

[REDACTED] I approved the EC. Please remind Mr. Richman of the requirement to file an OGE-450, Confidential Financial Disclosure Report. If you or he has any questions in this regard, please contact OIC POC [REDACTED] Thanks.

From: [REDACTED] (OGC) (FBI)
Sent: Monday, November 14, 2016 12:47 PM
To: KELLEY, PATRICK W. (DO) (FBI)
Subject: Dan Richman EC --- UNCLASSIFIED

b6 -1
b7C -1

Classification: UNCLASSIFIED
=====

Good afternoon AD Kelley,

I wanted to put on your radar an EC that is currently pending your approval in Sentinel. Dan Richman's term expired on June 30, 2016 and OGC worked on drafting his reappointment letter. Per the original EC, you were on the chain of approvals before the document was finalized. Therefore, I included you in the reappointment EC. Please let me know if you have any questions or concerns. The EC has been approved by OGC's Chief of Staff and GC Baker.

Best,

[Redacted]

Management and Program Analyst
Office of the General Counsel
935 Pennsylvania Ave., N.W.
Washington, DC 20535
Desk Phone: [Redacted]
Blackberry: [Redacted]
Fax: [Redacted]

b6 -1
b7C -1
b7E -3

=====
Classification: UNCLASSIFIED

=====
Classification: UNCLASSIFIED

=====
Classification: UNCLASSIFIED

=====
Classification: UNCLASSIFIED

=====
Classification: UNCLASSIFIED

=====
Classification: UNCLASSIFIED

=====
Classification: UNCLASSIFIED

RICHMAN, DANIEL C. (DO) (OGA)

From: RICHMAN, DANIEL C. (DO) (OGA)
Sent: Wednesday, January 11, 2017 12:46 PM
To: [REDACTED] (OGC) (FBI) [REDACTED] (DO) (FBI)
Subject: RE: Dan Richman EC --- UNCLASSIFIED

b6 -1
b7C -1

Classification: UNCLASSIFIED
=====

Thx. Since I'm leaving the NYO shortly and don't regularly check on the high side, could you please respond on the low side?

Thx
dr

From: [REDACTED] (OGC) (FBI)
Sent: Wednesday, January 11, 2017 12:38 PM
To: RICHMAN, DANIEL C. (DO) (OGA) [REDACTED] (DO) (FBI)
Subject: FW: Dan Richman EC --- UNCLASSIFIED

b6 -1
b7C -1

Classification: UNCLASSIFIED
=====

Hi Dan,

I believe there is training available on OIG's website, but I have copied [REDACTED] from OIG's ethics office to confirm and provide any additional guidance.

b6 -1
b7C -1
b7E -3

Thank you [REDACTED]

[REDACTED]
Management and Program Analyst
Office of the General Counsel
935 Pennsylvania Ave., N.W.
Washington, DC 20535
Desk Phone: [REDACTED]
Blackberry: [REDACTED]
Fax: [REDACTED]

From: RICHMAN, DANIEL C. (DO) (OGA)
Sent: Wednesday, January 11, 2017 12:33 PM
To: [REDACTED] (OGC) (FBI)
Subject: RE: Dan Richman EC --- UNCLASSIFIED

b6 -1
b7C -1

Classification: UNCLASSIFIED

While I have you = [REDACTED] mentioned that I need to reup my OGE training. But there's no module for that in my virtual cart. Do you know where I go for that?

Thx

Dan richman

b6 -1
b7C -1

From: [REDACTED] (OGC) (FBI)
Sent: Wednesday, January 11, 2017 12:29 PM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: RE: Dan Richman EC --- UNCLASSIFIED

b6 -1
b7C -1

Classification: UNCLASSIFIED

Good morning.

No apologies necessary! Thank you so much for your help.

Happy New Year!

[REDACTED]
Management and Program Analyst
Office of the General Counsel
935 Pennsylvania Ave., N.W.
Washington, DC 20535
Desk Phone: [REDACTED]
Blackberry: [REDACTED]
Fax: [REDACTED]

b6 -1
b7C -1
b7E -3

From: RICHMAN, DANIEL C. (DO) (OGA)
Sent: Wednesday, January 11, 2017 12:12 PM
To: [REDACTED] (OGC) (FBI)
Subject: RE: Dan Richman EC --- UNCLASSIFIED

b6 -1
b7C -1

Classification: UNCLASSIFIED

Sorry for my delay in responding. I couldn't get on to the high side, but am now on and will take care of this filing

Thx

Dan richman

From: [REDACTED] (OGC) (FBI)
Sent: Monday, November 21, 2016 8:39 AM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: FW: Dan Richman EC --- UNCLASSIFIED

b6 -1
b7C -1

Classification: UNCLASSIFIED
=====

Good morning Mr. Richman,

I work for GC Baker and recently drafted your reappointment EC. Please find below instructions from OIC to file an OGE-450.

Thank you and have a great Thanksgiving,

[REDACTED]
Management and Program Analyst
Office of the General Counsel
935 Pennsylvania Ave., N.W.
Washington, DC 20535
Desk Phone: [REDACTED]
Blackberry: [REDACTED]
Fax: [REDACTED]

b6 -1
b7C -1
b7E -3

From: KELLEY, PATRICK W. (DO) (FBI)
Sent: Monday, November 14, 2016 4:13 PM
To: [REDACTED] (OGC) (FBI)
Cc: [REDACTED] (DO) (FBI) [REDACTED] (DO) (FBI)
Subject: RE: Dan Richman EC --- UNCLASSIFIED

b6 -1
b7C -1

Classification: UNCLASSIFIED
=====

[REDACTED] I approved the EC. Please remind Mr. Richman of the requirement to file an OGE-450, Confidential Financial Disclosure Report. If you or he has any questions in this regard, please contact OIC POC [REDACTED] Thanks.

From: [REDACTED] (OGC) (FBI)
Sent: Monday, November 14, 2016 12:47 PM
To: KELLEY, PATRICK W. (DO) (FBI)
Subject: Dan Richman EC --- UNCLASSIFIED

b6 -1
b7C -1

Classification: UNCLASSIFIED

Good afternoon AD Kelley,

I wanted to put on your radar an EC that is currently pending your approval in Sentinel. Dan Richman's term expired on June 30, 2016 and OGC worked on drafting his reappointment letter. Per the original EC, you were on the chain of approvals before the document was finalized. Therefore, I included you in the reappointment EC. Please let me know if you have any questions or concerns. The EC has been approved by OGC's Chief of Staff and GC Baker.

Best,

[Redacted]
Management and Program Analyst
Office of the General Counsel
935 Pennsylvania Ave., N.W.
Washington, DC 20535
Desk Phone [Redacted]
Blackberry [Redacted]
Fax: [Redacted]

b6 -1
b7C -1
b7E -3

=====
Classification: UNCLASSIFIED

=====
Classification: UNCLASSIFIED

=====
Classification: UNCLASSIFIED

=====
Classification: UNCLASSIFIED

=====
Classification: UNCLASSIFIED

=====
Classification: UNCLASSIFIED

=====
Classification: UNCLASSIFIED

=====
Classification: UNCLASSIFIED

[redacted] (DO) (FBI)

b6 -1
b7C -1

From: [redacted] (DO) (FBI)
Sent: Wednesday, January 11, 2017 2:34 PM
To: [redacted] (NY) (FBI); RICHMAN, DANIEL C. (DO) (OGA)
Cc: [redacted] (OGC) (FBI)
Subject: RE: MANDATORY - ETHICS TRAINING FOR SUPERVISORS --- UNCLASSIFIED//~~FOUO~~

Classification: UNCLASSIFIED//~~FOUO~~
=====

Is Daniel coming into the NY office? Otherwise he won't get his message. [redacted] also said that he could talk to Daniel over the phone re his training.

From: [redacted] (NY) (FBI)
Sent: Wednesday, January 11, 2017 2:31 PM
To: RICHMAN, DANIEL C. (DO) (OGA) [redacted]
Cc: [redacted] (OGC) (FBI) [redacted]
(DO) (FBI) [redacted]
Subject: FW: MANDATORY - ETHICS TRAINING FOR SUPERVISORS --- UNCLASSIFIED//~~FOUO~~

b6 -1
b7C -1
b7E -3

Classification: UNCLASSIFIED//~~FOUO~~
=====

Daniel

Per the FBI Office of Integrity and Compliance (OIC), you are mandated to complete 1 hour of mandatory ethics training as a Special Government Employee. See the below email regarding the training. Please complete the certification form upon completion of the training and submit to Assistant General Counsel [redacted] Please contact OIC if you have any questions.

b6 -1
b7C -1

[redacted]

All OGE-278 Public Financial Disclosure Ethics Report filers, OGE 450 Confidential Financial Ethics Disclosure Report filers and FBI Conflict of Interest Ethics Certification Form (CIC) filers are required by regulation to receive at least one hour of training in the Standards of Ethical Conduct each calendar year. If you are in receipt of this email you must complete the training by

12/30/2016.

Compliance:

All training compliance should be documented by **completing the Certification of Annual Ethics Training form.**

<< File: Ethics Training Certification.docx >>

Web-based alternative training videos:

Filers are to watch any one of the below ethics training videos to fulfill the training requirement.

"The Squad" - FBI Annual/EOD Training



b7E -3

(NOTE: "The Squad" is the preferred alternative because it is FBI specific.)

DOJ Ethics Annual Training: "The View" on Ethics:



DOJ Ethics Annual Training: "The Office":



Filers must have the training in "verbal" form (with an instructor present or immediately available by phone or other electronic means to answer questions. *Employees who view the alternative training may ask that CDC/ADCs, as ethics counselors, be on phone standby to answer questions--or they may also call an OIC Ethics Attorneys to fill that role.*

=====
Classification: UNCLASSIFIED//~~FOUO~~

=====
Classification: UNCLASSIFIED//~~FOUO~~

[redacted] (NY) (FBI)

b6 -1
b7C -1

From: [redacted] (NY) (FBI)
Sent: Wednesday, January 11, 2017 2:43 PM
To: [redacted] (DO) (FBI); RICHMAN, DANIEL C. (DO) (OGA)
Cc: [redacted] (OGC) (FBI)
Subject: RE: MANDATORY - ETHICS TRAINING FOR SUPERVISORS ---
UNCLASSIFIED//~~FOUO~~

Classification: UNCLASSIFIED//~~FOUO~~
=====

Per your communications with him, my understanding is that he was making arrangements with [redacted] to come into the NYO. I have no further information on whether he will be coming to the NYO. He is not assigned to the NYO so he was not a part of our annual ethics data call. I was requested to send the necessary training info to Daniel to ensure his fulfillment of the ethics training required for a Special Government Employee.

b6 -1
b7C -1
b7E -3

[redacted]
SUPERVISORY SPECIAL AGENT
ASSOCIATE DIVISION COUNSEL
FBI New York
DESK [redacted]
CELL [redacted]
[redacted]

This Document May Contain Attorney Work Product and/or Attorney-Client Privileged Communications

From: [redacted] (DO) (FBI)
Sent: Wednesday, January 11, 2017 2:34 PM
To: [redacted] (NY) (FBI); RICHMAN, DANIEL C. (DO) (OGA)
Cc: [redacted] (OGC) (FBI)
Subject: RE: MANDATORY - ETHICS TRAINING FOR SUPERVISORS --- UNCLASSIFIED//~~FOUO~~

b6 -1
b7C -1

Classification: UNCLASSIFIED//~~FOUO~~
=====

Is Daniel coming into the NY office? Otherwise he won't get his message. [redacted] also said that he could talk to Daniel over the phone re his training.

From: [redacted] (NY) (FBI)

b6 -1
b7C -1

Sent: Wednesday, January 11, 2017 2:31 PM

To: RICHMAN, DANIEL C. (DO) (OGA) [REDACTED]

Cc: [REDACTED] (OGC) (FBI) [REDACTED]
(DO) (FBI) [REDACTED]

Subject: FW: MANDATORY - ETHICS TRAINING FOR SUPERVISORS --- UNCLASSIFIED//~~FOUO~~

b6 -1
b7C -1
b7E -3

Classification: UNCLASSIFIED//~~FOUO~~

=====

Daniel

Per the FBI Office of Integrity and Compliance (OIC), you are mandated to complete 1 hour of mandatory ethics training as a Special Government Employee. See the below email regarding the training. Please complete the certification form upon completion of the training and submit to Assistant General Counsel [REDACTED]. Please contact OIC if you have any questions.



All OGE-278 Public Financial Disclosure Ethics Report filers, OGE 450 Confidential Financial Ethics Disclosure Report filers and FBI Conflict of Interest Ethics Certification Form (CIC) filers are required by regulation to receive at least one hour of training in the Standards of Ethical Conduct each calendar year. If you are in receipt of this email you must complete the training by 12/30/2016.

Compliance:

All training compliance should be documented by completing the Certification of Annual Ethics Training form.

<< File: Ethics Training Certification.docx >>

Web-based alternative training videos:

Filers are to watch any one of the below ethics training videos to fulfill the training requirement.

"The Squad" - FBI Annual/EOD Training

b7E -3

(NOTE: "The Squad" is the preferred alternative because it is FBI specific.)

DOJ Ethics Annual Training: "The View" on Ethics:

DOJ Ethics Annual Training: "The Office":

Filers must have the training in "verbal" form (with an instructor present or immediately available by phone or other electronic means to answer questions. *Employees who view the alternative training may ask that CDC/ADCs, as ethics counselors, be on phone standby to answer questions--or they may also call an OIC Ethics Attorneys to fill that role.*

=====
Classification: UNCLASSIFIED//~~FOUO~~

=====
Classification: UNCLASSIFIED//~~FOUO~~

=====
Classification: UNCLASSIFIED//~~FOUO~~

[REDACTED] (DO) (FBI)

b6 -1
b7C -1

From: [REDACTED] (DO) (FBI)
Sent: Wednesday, January 11, 2017 2:55 PM
To: [REDACTED] (NY) (FBI); RICHMAN, DANIEL C. (DO) (OGA)
Cc: [REDACTED] (OGC) (FBI)
Subject: RE: MANDATORY - ETHICS TRAINING FOR SUPERVISORS ---
UNCLASSIFIED//~~FOUO~~

Classification: UNCLASSIFIED//~~FOUO~~
=====

Thank you.

From: [REDACTED] (NY) (FBI)
Sent: Wednesday, January 11, 2017 2:43 PM
To: [REDACTED] (DO) (FBI); [REDACTED] RICHMAN, DANIEL C. (DO) (OGA)
Cc: [REDACTED] (OGC) (FBI); [REDACTED]
Subject: RE: MANDATORY - ETHICS TRAINING FOR SUPERVISORS --- UNCLASSIFIED//~~FOUO~~

b6 -1
b7C -1
b7E -3

Classification: UNCLASSIFIED//~~FOUO~~
=====

Per your communications with him, my understanding is that he was making arrangements with [REDACTED] to come into the NYO. I have no further information on whether he will be coming to the NYO. He is not assigned to the NYO so he was not a part of our annual ethics data call. I was requested to send the necessary training info to Daniel to ensure his fulfillment of the ethics training required for a Special Government Employee.

b6 -1
b7C -1

[REDACTED]
SUPERVISORY SPECIAL AGENT
ASSOCIATE DIVISION COUNSEL
FBI New York
DESK [REDACTED]
CELL [REDACTED]
[REDACTED]

b6 -1
b7C -1
b7E -3

This Document May Contain Attorney Work Product and/or Attorney-Client Privileged Communications

From: [REDACTED] (DO) (FBI)
Sent: Wednesday, January 11, 2017 2:34 PM

b6 -1
b7C -1

To: [redacted] (NY) (FBI); RICHMAN, DANIEL C. (DO) (OGA)
Cc: [redacted] (OGC) (FBI)
Subject: RE: MANDATORY - ETHICS TRAINING FOR SUPERVISORS --- UNCLASSIFIED//~~FOUO~~

b6 -1
b7C -1

Classification: UNCLASSIFIED//~~FOUO~~
=====

Is Daniel coming into the NY office? Otherwise he won't get his message. [redacted] also said that he could talk to Daniel over the phone re his training.

From: [redacted] (NY) (FBI)
Sent: Wednesday, January 11, 2017 2:31 PM
To: RICHMAN, DANIEL C. (DO) (OGA) [redacted]
Cc: [redacted] (OGC) (FBI) [redacted]
(DO) (FBI) [redacted]
Subject: FW: MANDATORY - ETHICS TRAINING FOR SUPERVISORS --- UNCLASSIFIED//~~FOUO~~

b6 -1
b7C -1
b7E -3

Classification: UNCLASSIFIED//~~FOUO~~
=====

Daniel

Per the FBI Office of Integrity and Compliance (OIC), you are mandated to complete 1 hour of mandatory ethics training as a Special Government Employee. See the below email regarding the training. Please complete the certification form upon completion of the training and submit to Assistant General Counsel [redacted] Please contact OIC if you have any questions.

b6 -1
b7C -1

All OGE-278 Public Financial Disclosure Ethics Report filers, OGE 450 Confidential Financial Ethics Disclosure Report filers and FBI Conflict of Interest Ethics Certification Form (CIC) filers are required by regulation to receive at least one hour of training in the Standards of Ethical Conduct each calendar year. If you are in receipt of this email you must complete the training by 12/30/2016.

Compliance:

All training compliance should be documented by completing the **Certification of Annual Ethics Training form**.

<< File: Ethics Training Certification.docx >>

Web-based alternative training videos:

Filers are to watch any one of the below ethics training videos to fulfill the training requirement.

"The Squad" - FBI Annual/EOD Training

b7E -3

(**NOTE:** "The Squad" is the preferred alternative because it is FBI specific.)

DOJ Ethics Annual Training: "The View" on Ethics:

DOJ Ethics Annual Training: "The Office":

Filers must have the training in "verbal" form (with an instructor present or immediately available by phone or other electronic means to answer questions. *Employees who view the alternative training may ask that CDC/ADCs, as ethics counselors, be on phone standby to answer questions--or they may also call an OIC Ethics Attorneys to fill that role.*

=====
Classification: UNCLASSIFIED//~~FOUO~~

=====
Classification: UNCLASSIFIED//~~FOUO~~

=====
Classification: UNCLASSIFIED//~~FOUO~~

=====
Classification: UNCLASSIFIED//~~FOUO~~

[redacted] (NY) (FBI)

b6 -1
b7C -1

From: [redacted] (NY) (FBI)
Sent: Wednesday, January 11, 2017 2:31 PM
To: RICHMAN, DANIEL C. (DO) (OGA)
Cc: [redacted] (OGC) (FBI); [redacted] (DO) (FBI)
Subject: FW: MANDATORY - ETHICS TRAINING FOR SUPERVISORS ---
UNCLASSIFIED//~~FOUO~~
Attachments: Ethics Training Certification.docx

Classification: UNCLASSIFIED//~~FOUO~~
=====

Daniel

Per the FBI Office of Integrity and Compliance (OIC), you are mandated to complete 1 hour of mandatory ethics training as a Special Government Employee. See the below email regarding the training. Please complete the certification form upon completion of the training and submit to Assistant General Counsel [redacted] Please contact OIC if you have any questions.

b6 -1
b7C -1

[redacted]

All OGE-278 Public Financial Disclosure Ethics Report filers, OGE 450 Confidential Financial Ethics Disclosure Report filers and FBI Conflict of Interest Ethics Certification Form (CIC) filers are required by regulation to receive at least one hour of training in the Standards of Ethical Conduct each calendar year. If you are in receipt of this email you must complete the training by 12/30/2016.

Compliance:

All training compliance should be documented by **completing the Certification of Annual Ethics Training form.**

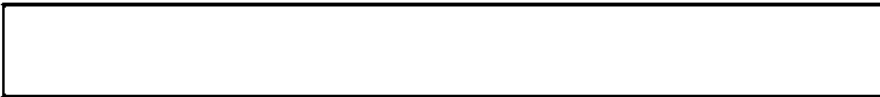
<<Ethics Training Certification.docx>>

Web-based alternative training videos:

FBI 18-CV-1833-7898

Filers are to watch any one of the below ethics training videos to fulfill the training requirement.

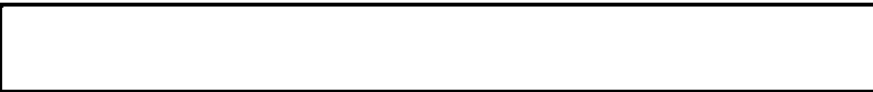
"The Squad" - FBI Annual/EOD Training



b7E -3

(**NOTE:** "The Squad" is the preferred alternative because it is FBI specific.)

DOJ Ethics Annual Training: "The View" on Ethics:



DOJ Ethics Annual Training: "The Office":



Filers must have the training in "verbal" form (with an instructor present or immediately available by phone or other electronic means to answer questions. *Employees who view the alternative training may ask that CDC/ADCs, as ethics counselors, be on phone standby to answer questions--or they may also call an OIC Ethics Attorneys to fill that role.*

=====
Classification: UNCLASSIFIED//~~FOUO~~

CERTIFICATION OF ANNUAL ETHICS TRAINING
(Rev. 7/2014)
SUBMIT TO YOUR CDC OR DIVISIONAL ETHICS POINT OF CONTACT

I certify that I have received my required **one hour** annual ethics training for calendar year _____.

Check one of the following Methods:

☐ Attended a live ethics training presentation. *[Optimal training for all filers, Completely fulfills annual requirements, but only if a qualified instructor was present or standing by to discuss the training]:*

Date: _____

Topic: _____

Presenter: _____

☐ Reviewing an ethics video or video of live ethics presentation. *[Completely fulfills annual OGE Form 278, 450 and CIC filers, but only if a qualified instructor was present or standing by to discuss the training]:*

Name of Video: _____

Date Viewed: _____

☐ Completing the following computer or qualifying web-based training offered on the Office of Govt Ethics (OGE) website at:
http://www.usoge.gov/pages/comp_web_trng/comp_web_trng.html (or one of their links to other qualifying Federal Government ethics training). *[Qualified training completely fulfills annual OGE Form 278, 450 and CIC filers, but only if a qualified instructor was present or standing by to discuss the training]:*

FBI Annual/EOD Training: "The Squad":

DOJ Ethics Annual Training: "The Office":

☐ Other (please specify): _____
[Only fulfills annual OGE Form 278, 450 and CIC filers training if a qualified instructor was present or standing by to discuss the training and if the training program was pre-qualified by your CDC or OIC Ethics Attorneys]

NAME (PLEASE PRINT)

DIVISION/SECTION/UNIT

☐ OGE-278 Filer

☐ OGE-450/CIC Filer

SIGNATURE

DATE

FEDERAL BUREAU OF INVESTIGATION
 FOI/PA
 DELETED PAGE INFORMATION SHEET
 19th Interim Release
 Civil Action# 18-cv-1833, FOIA 1404359-0

Total Withheld Page(s) = 38

Bates Page Reference	Reason for Withholding (i.e., exemptions with coded rationale, duplicate, sealed by order of court, etc.)
18-cv-1833 - 1328-1330, 1336-1338	(b)(5)-1, and b5-PER DOJ/OIP
18-cv-1833 - 4661	(b)(5)-1, (b)(6)-2, and (b)(7)(C)-2
18-cv-1833 - 4878, 4882, 4886	(b)(5)-PER NSC
18-cv-1833 - 5968-5969, 5988, 5996, 6007	(b)(5)-PER DOJ/OIP
18-cv-1833 - 5973, 5976, 5994, 5999, 6011-6012	(b)(5)-1, and (b)(5)-PER DOJ/OIP
18-cv-1833 - 5974, 5977, 5991, 5993, 5997-5998, 6000-6001	(b)(5)-1, (b)(6)-2, (b)(7)(C)-2, and (b)(5)-PER DOJ/OIP
18-cv-1833 - 5986-5987, 5989, 6010	(b)(7)(E)-3 and (b)(5)-PER DOJ/OIP
18-cv-1833 - 5990	(b)(7)(E)-3 and (b)(5) and (b)(6)-PER DOJ/OIP
18-cv-1833 - 5992	(b)(5)-1, (b)(7)(E)-3, and (b)(5)-PER DOJ/OIP,
18-cv-1833 - 5995, 6006, 6009	(b)(6)-2, (b)(7)(C)-2, (b)(7)(E)-3, and (b)(5)-PER DOJ/OIP

XXXXXXXXXXXXXXXXXXXXXXXXXXXXX
 X Deleted Page(s) X
 X No Duplication Fee X
 X For this Page X
 XXXXXXXXXXXXXXXXXXXXXXXXXXXXX

From: COMEY, JAMES B. (DO) (FBI)
Sent: Monday, January 9, 2017 6:22 PM
To: [REDACTED] (DO) (OGA)
Subject: RE: --- UNCLASSIFIED

b6 -1
b7C -1

SentinelCaseId: TRANSITORY RECORD

Classification: UNCLASSIFIED
=====

TRANSITORY RECORD

Thanks.

From: [REDACTED] (DO) (OGA)
Sent: Monday, January 09, 2017 5:16 PM
To: COMEY, JAMES B. (DO) (FBI) <JBCOMEY@fbi.sgov.gov>
Subject: RE: --- UNCLASSIFIED

b6 -1
b7C -1

Classification: UNCLASSIFIED
=====

TRANSITORY RECORD

Will do, Boss. The Cyber DPI team member who will be taking the lead on cyber personnel issues had a call with Dan Richman earlier this afternoon (at my request) and it sounds like they've identified some initial areas where Dan might contribute as this workstream progresses. I've also notified OGC and asked them to work on an amended MOU for Dan that would reflect this added area.

[REDACTED]

From: COMEY, JAMES B. (DO) (FBI)
Sent: Monday, January 09, 2017 4:32 PM
To: [REDACTED] (DO) (OGA)
Subject: --- UNCLASSIFIED

b5 -1
b6 -1
b7C -1

Classification: UNCLASSIFIED
=====

TRANSITORY RECORD

Dan Richman thinks he can add some value on the cyber personnel front. Apparently he had conversations with one of our cyber supervisors in NY and believes he may be able help us with our interest in developing things like [REDACTED]
[REDACTED] When you next speak to him, see if you agree he can add value there. Thanks.

=====
Classification: UNCLASSIFIED

=====
Classification: UNCLASSIFIED

=====
Classification: UNCLASSIFIED

Raj, Kiran (ODAG)

From: Raj, Kiran (ODAG)
Sent: Thursday, February 04, 2016 10:53 AM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: "Going Dark" question

DRAFT//DELIBERATIVE

My comments are in brackets below. (Apologies in advance for the stream-of-conscious nature of my comments below).

From: Daniel Charles Richman [mailto:]
Sent: Tuesday, February 02, 2016 11:38 AM
To: Raj, Kiran (ODAG)
Subject: Fwd: "Going Dark" question

b6 -2, 4
b7C - 2, 4

I'll use italics for [] And I'd love to hear your thoughts on his. I'm planning to see him to chat

----- Forwarded message -----

From: []
Date: Mon, Feb 1, 2016 at 5:41 PM
Subject: Re: "Going Dark" question
To: Daniel Charles Richman []

Comments inline.

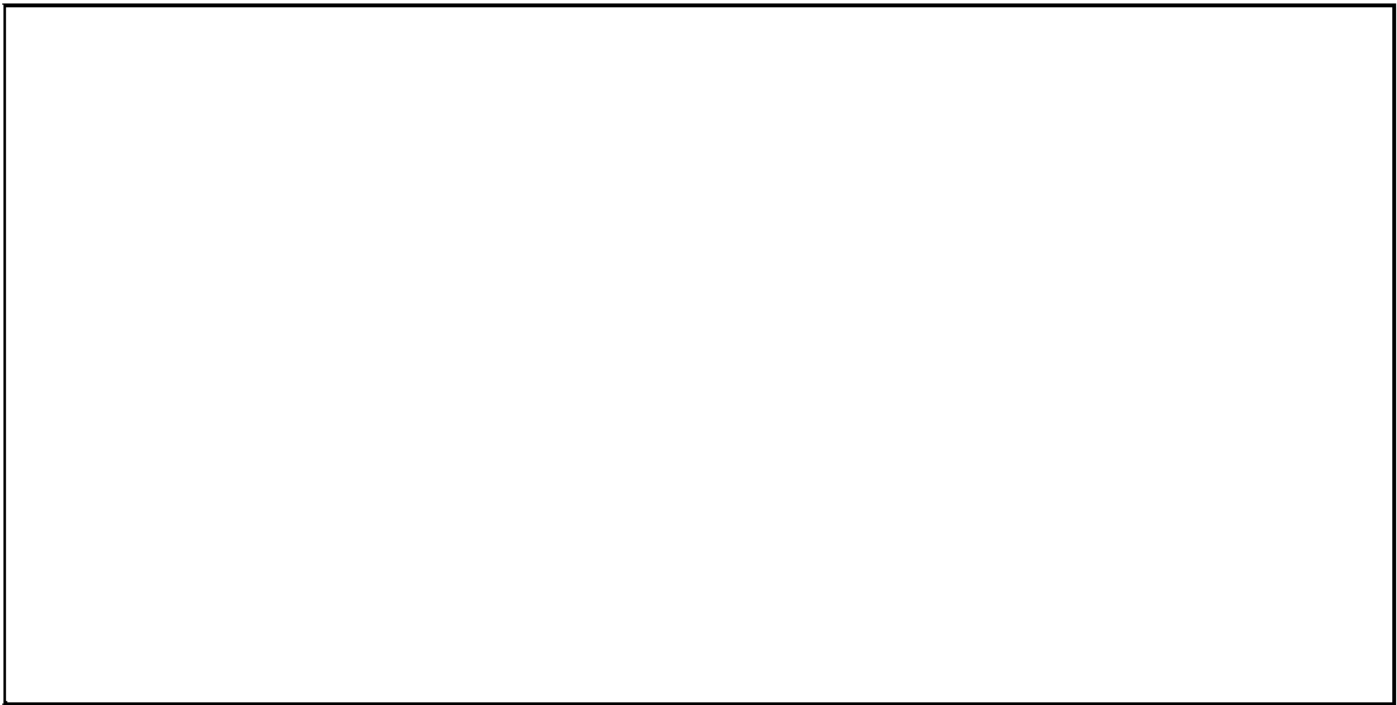
On 31 Jan 2016, at 13:48, Daniel Charles Richman wrote:

Hi [] It's been a while, and I do hope all's well. I'm still trying to get my bearings on the encryption debate (and advising the FBI Director) and would be really grateful if you gave me a reality check on the following thoughts. Would you be willing to do so? If you'd prefer to do this in person, I'm happy to come by your office when it's convenient.
thx so much
dan richman

b6 -2
b7C -2

b5 -1

FBI 18-CV-1833-1327



b5 -1 and Per DOJ/OIP

Kiran

--

Daniel Richman
Paul J. Kellner Professor of Law,
Columbia Law School
office [REDACTED]
cellphone [REDACTED]

You can download my papers at <http://ssrn.com/author=937729>

b6 -4

b7C -4

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Thursday, February 04, 2016 11:18 AM
To: Raj, Kiran (ODAG)
Subject: RE: "Going Dark" question

thanks so much. I need to think about this more tonight. But your comments will really prepare me for my chat with [REDACTED] tomorrow morning, and I'm extremely grateful d

From: Raj, Kiran (ODAG) [Kiran.Raj@usdoj.gov]
Sent: Thursday, February 04, 2016 10:52 AM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: "Going Dark" question

b6 -2
b7C -2

DRAFT//DELIBERATIVE

My comments are in brackets below. (Apologies in advance for the stream-of-conscious nature of my comments below).

From: Daniel Charles Richman [mailto:[REDACTED]]
Sent: Tuesday, February 02, 2016 11:38 AM
To: Raj, Kiran (ODAG)
Subject: Fwd: "Going Dark" question

b6 -2, 4
b7C -2, 4

I'll use italics for [REDACTED] And I'd love to hear your thoughts on his. I'm planning to see him to chat -----

-- Forwarded message ----- **From:** [REDACTED]

[REDACTED] **Date:** Mon, Feb 1, 2016 at 5:41 PM **Subject:** Re: "Going Dark" question **To:** Daniel Charles Richman [REDACTED]

Comments inline.

On 31 Jan 2016, at 13:48, Daniel Charles Richman wrote:

Hi [REDACTED] It's been a while, and I do hope all's well. I'm still trying to get my bearings on the encryption debate (and advising the FBI Director) and would be really grateful if you gave me a reality check on the following thoughts. Would you be willing to do so? If you'd prefer to do this in person, I'm happy to come by your office when it's convenient.
thx so much
dan richman

b5 -1



Kiran

b5 -1 and Per DOJ/OIP

--

Daniel Richman
Paul J. Kellner Professor of Law,
Columbia Law School
office [REDACTED]
cellphone [REDACTED]

b6 -4
b7C -4

You can download my papers at <http://ssrn.com/author=937729>

Daniel Charles Richman

From: Daniel Charles Richman
Sent: Thursday, October 29, 2015 1:12 PM
To: Stawasz, Michael (CRM); Oconnell, Sasha C. (DO) (FBI); Burrell, James C. (OTD) (FBI)
Subject: Re: Going Dark

Thanks Mick. I'll keep you posted. When it comes to just this issue, it would great to get the USG needs and asks sorted out, even as we bring in the industry folks. To that end, I'm looping in Sasha O'Connell and Jim Burrell at the Bureau.

thx
dan r

On Thu, Oct 29, 2015 at 11:40 AM, Stawasz, Michael [REDACTED]@usdoj.gov> wrote:

Professor Richman,

b6 Per DOJ/CRM
b7C Per DOJ/CRM

I will be at International CES the first week of January, but assuming the next meeting is not scheduled that week, I would very much like to continue to participate as ideas are formed into action. In particular, my team is responsible for creating the guidance and sample requests that federal prosecutors use to obtain information from providers of electronic communication services and remote computer services. So my team might be best able to help there. I look forward to seeing you again soon.

Mick

Michael J. Stawasz

Deputy Chief for Computer Crime

Head of the CCIPS Cybersecurity Unit

Computer Crime and Intellectual Property Section

United States Department of Justice

FBI 18-CV-1833-3935

From: Daniel Charles Richman [mailto:[REDACTED]]

Sent: Thursday, October 29, 2015 10:28 AM

To: [REDACTED] Eggers, Matthew J [REDACTED]

Jack Lichtenstein [REDACTED]

Benjamin Rosenberg [REDACTED]

O'Connell, Sasha C. (DO) (FBI)

Baker, James A. (OGC)

(FBI) [REDACTED] Burrell, James C. (OTD) (FBI) [REDACTED]

(ODAG) [REDACTED] (DO) (FBI)

Stawasz, Michael [REDACTED]

Subject: Going Dark

Thank you for those who followed up with me after the October 16 roundtable. To continue the momentum, I have compiled a list of takeaways from the meeting and subsequent conversations with various attendees. Please note, these themes may not be exhaustive, so please respond to the thread if you feel anything has been left off or if you have additional suggestions.

Themes

- Law enforcement has not provided sufficient data to specifically demonstrate the scope/parameters of the problem nor have they offered any prioritization of the problem. Providers frequently lack a clear picture/roadmap of the data they do have and could provide in response to lawful orders. Law enforcement, for its part, could be better at specifying what they need. There is considerable room for improvement/collaboration on all sides.
- Academia has offered to help explore technical options.
- We need to change the environment to address the perception that private sector cooperation with LE/government is a bad thing.

Potential Next Steps

I think – subject to reactions from you all – that we should plan another roundtable for early January, and perhaps even early December. The goal here would be to get more granular in the identification of common ground – something that we can best do as a group if some preliminary work can be done long before we meet. I'm in the process of reaching out to some of you who have expressed interest in preparing particular issues for discussion. But please don't wait for a special invitation if you're interested in getting actively involved. Just let [REDACTED] and me know.

b6 -2
b7C -2

You should note that, in deference to the restrictions of the Federal Advisory Committee Act, the Bureau wants to be clear that it is not expecting or looking for consensus recommendations from the group, either now or later. The goal is to get ideas on the table and a better understanding of the issues.

thanks

Dan Richman and [REDACTED]

Daniel Richman

Daniel Richman

Paul J. Kellner Professor of Law,
Columbia Law School

office [REDACTED]

cellphone [REDACTED]

You can download my papers at <http://ssrn.com/author=937729>

b6 -4
b7C -4

Spam

Not spam

Forget previous vote

—
Daniel Richman

Paul J. Kellner Professor of Law,
Columbia Law School

office [REDACTED]

cellphone [REDACTED]

You can download my papers at <http://ssrn.com/author=937729>

b6 -4
b7C -4

Oconnell, Sasha C. (DO) (FBI)

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Monday, December 05, 2016 12:47 PM
To: [REDACTED] (DO) (OGA)
Subject: RE: Cybersecurity Commission report

b6 -1
b7C -1

Oh man don't show this to Dan. He has been asking for a DARPA rep and I have not delivered!

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

From: [REDACTED] (DO) (OGA)
Sent: Monday, December 05, 2016 10:26 AM
To: Oconnell, Sasha C. (DO) (FBI); [REDACTED] Daniel Charles Richman
[REDACTED]
Subject: FW: Cybersecurity Commission report

b6 -1,4
b7C -1,4
b7E -3

Fyi.

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

b6 Per DOJ/CRM
b7C Per DOJ/CRM

Begin forwarded message:

From: "Stawasz, Michael" [REDACTED]@CRM.USDOJ.GOV<mailto:[REDACTED]@CRM.USDOJ.GOV>>
Date: December 2, 2016 at 5:21:44 PM EST
To: "Bailey, Leonard" [REDACTED]@CRM.USDOJ.GOV<mailto:[REDACTED]@CRM.USDOJ.GOV>>, "Chun, Harold (CRM)" [REDACTED]@CRM.USDOJ.GOV<mailto:[REDACTED]@CRM.USDOJ.GOV>>, "Cooper, Aaron" [REDACTED]@CRM.USDOJ.GOV<mailto:[REDACTED]@CRM.USDOJ.GOV>>, "Dantiki, Sumon (CRM)" [REDACTED]@CRM.USDOJ.GOV<mailto:[REDACTED]@CRM.USDOJ.GOV>>, "Eltringham, Scott" [REDACTED]@CRM.USDOJ.GOV<mailto:[REDACTED]@CRM.USDOJ.GOV>>, "Ervin, Kendra" [REDACTED]@CRM.USDOJ.GOV<mailto:[REDACTED]@CRM.USDOJ.GOV>>, "Fitzpatrick, Benjamin (CRM)" [REDACTED]@CRM.USDOJ.GOV<mailto:[REDACTED]@CRM.USDOJ.GOV>>, "Levine, Brian" [REDACTED]@CRM.USDOJ.GOV<mailto:[REDACTED]@CRM.USDOJ.GOV>>, "Rees, Albert" [REDACTED]@CRM.USDOJ.GOV<mailto:[REDACTED]@CRM.USDOJ.GOV>>, "Roman, Peter" [REDACTED]@CRM.USDOJ.GOV<mailto:[REDACTED]@CRM.USDOJ.GOV>>, "Zacharia, John" [REDACTED]@CRM.USDOJ.GOV<mailto:[REDACTED]@CRM.USDOJ.GOV>>
Cc: "Lynch, John" [REDACTED]@CRM.USDOJ.GOV<mailto:[REDACTED]@CRM.USDOJ.GOV>>, "Goldfoot, Josh (CRM)" [REDACTED]@CRM.USDOJ.GOV<mailto:[REDACTED]@CRM.USDOJ.GOV>>, "O'Neil, Erica (CRM)" [REDACTED]@CRM.USDOJ.GOV<mailto:[REDACTED]@CRM.USDOJ.GOV>>
Subject: Cybersecurity Commission report

Have not read yet, https://www.whitehouse.gov/sites/default/files/docs/cybersecurity_report.pdf

but only two mentions of encryption if CTRL+F is to be believed. Quantum computing could render current encryption useless and this . . .

FBI 18-CV-1833-4242

“In conducting this research, greater use should be made of challenge competitions — with money prizes — and other creative approaches that engage individuals and teams of innovators. These competitions should include development of new technologies, along with innovation in the use and systems integration of existing inherently secure technologies. The cybersecurity community has had some success with the challenge competition model, especially the Cyber Grand Challenge created recently by the Defense Advanced Research Projects Agency (DARPA). These efforts should be sustained, multiyear, and iterative. Examples of possible challenge competition topics include privacy-enhancing technologies, IoT security, defect-free software, blockchain, and pervasive encryption.”

Michael J. Stawasz

Deputy Chief for Computer Crime

Head of the Cybersecurity Unit

Computer Crime and Intellectual Property Section United States Department of Justice

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Sunday, October 11, 2015 9:40 AM
To: Ceresney, Andrew
Subject: RE: smart phones

Actually the nyt is totally wrong. Jim is truly pissed. In fact the Decision was to leave legislation on the table. The WaPo picked this up. Times will have to walk the story back and stop listening to the tech folks in the WH. Your city is moronic

From: Ceresney, Andrew [REDACTED]@SEC.GOV]
Sent: Sunday, October 11, 2015 9:13 AM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: smart phones

b6 Per SEC

Dan - Surprising article in NYT on WH position re encryption. Am sure you guys are not happy. Andrew

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

From: Richman, Daniel C. (DO) (OGA) [REDACTED]
Sent: Wednesday, October 07, 2015 08:39 PM Eastern Standard Time
To: Ceresney, Andrew
Cc: Oconnell, Sasha C. (DO) (FBI); Boujoukos, Jeffrey; [REDACTED]
Subject: RE: smart phones

b7E -3

b6 Per SEC

Thanks. More generally, even though it's always a challenge to clarify how a precluded line of investigation affected a case, and a particular challenge for an enforcement agency sensitive to disclosure risks, we'd appreciate hearing about other cases where password protection and encryption have stymied you Thx for being so quick on this Dan r

From: Ceresney, Andrew [REDACTED]@SEC.GOV]
Sent: Wednesday, October 07, 2015 7:10 PM
To: Richman, Daniel C. (DO) (OGA)
Cc: Oconnell, Sasha C. (DO) (FBI); Boujoukos, Jeffrey; [REDACTED]
Subject: RE: smart phones

b6 Per SEC

b5 Per SEC

b6 Per SEC

Sure. Good to hear from you Dan. Glad to hear you are doing Gods work. I know about the case.

[REDACTED] our sense is the case with ultimately resolve -- hopefully in our favor -- without us getting the chance to challenge it. And we are seeking other ways to try to get the info from the phone. I have cc'd Jeff Boujoukos and [REDACTED] who are in our Philly office and closest to the matter. They can provide more info. Andrew

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

From: Richman, Daniel C. (DO) (OGA) [REDACTED]

b7E -3

FBI 18-CV-1833-4522

Sent: Wednesday, October 07, 2015 07:07 PM Eastern Standard Time

To: Ceresney, Andrew

Cc: Oconnell, Sasha C. (DO) (FBI)

Subject: smart phones

Hi Andrew -- I'm working these days with Jim Comey and his crew on, among other things, the "Going Dark" problem. I don't know the extent to which the attached EDPa case -- about SEC access to a password protected smartphone -- is on your radar. But I (and Sasha O'Connell, the policy point person in the Director's office -- cc'd here) would love to get more information about the extent to which the problem is affecting your work, in this case and others.

thx

dan richman

Ceresney, Andrew

From: Ceresney, Andrew
Sent: Sunday, October 11, 2015 9:14 AM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: smart phones

Dan - Surprising article in NYT on WH position re encryption. Am sure you guys are not happy. Andrew

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

From: Richman, Daniel C. (DO) (OGA) [REDACTED]
Sent: Wednesday, October 07, 2015 08:39 PM Eastern Standard Time
To: Ceresney, Andrew
Cc: Oconnell, Sasha C. (DO) (FBI); Boujoukos, Jeffrey; [REDACTED]
Subject: RE: smart phones

b7E -3

b6 Per SEC

Thanks. More generally, even though it's always a challenge to clarify how a precluded line of investigation affected a case, and a particular challenge for an enforcement agency sensitive to disclosure risks, we'd appreciate hearing about other cases where password protection and encryption have stymied you
Thx for being so quick on this
Dan r

From: Ceresney, Andrew [REDACTED]@SEC.GOV]
Sent: Wednesday, October 07, 2015 7:10 PM
To: Richman, Daniel C. (DO) (OGA)
Cc: Oconnell, Sasha C. (DO) (FBI); Boujoukos, Jeffrey [REDACTED]
Subject: RE: smart phones

b6 Per SEC

b5 Per SEC

b6 Per SEC

Sure. Good to hear from you Dan. Glad to hear you are doing Gods work. I know about the case. [REDACTED]
[REDACTED] our sense is the case with ultimately resolve -- hopefully in our favor -- without us getting the chance to challenge it. And we are seeking other ways to try to get the info from the phone. I have cc'd Jeff Boujoukos and [REDACTED] who are in our Philly office and closest to the matter. They can provide more info. Andrew

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

From: Richman, Daniel C. (DO) (OGA) [REDACTED]
Sent: Wednesday, October 07, 2015 07:07 PM Eastern Standard Time
To: Ceresney, Andrew
Cc: Oconnell, Sasha C. (DO) (FBI)
Subject: smart phones

b7E -3

Hi Andrew -- I'm working these days with Jim Comey and his crew on, among other things, the "Going Dark" problem. I don't know the extent to which the attached EDPa case -- about SEC access to a password protected smartphone -- is on your radar. But I (and Sasha O'Connell, the policy point person in the Director's office -- cc'd here) would love to get more information about the extent to which the problem is affecting your work, in this case and others.

thx
dan richman

FBI 18-CV-1833-4525

Ceresney, Andrew

From: Ceresney, Andrew
Sent: Sunday, October 11, 2015 10:00 AM
To: Richman, Daniel C. (DO) (OGA)
Subject: Re: smart phones

Let's just say NY should not be judged by Times. Assume you are having trouble w Wh

Original Message

From: Richman, Daniel C. (DO) (OGA)
Sent: Sunday, October 11, 2015 9:42 AM
To: Ceresney, Andrew
Subject: RE: smart phones

Actually the nyt is totally wrong. Jim is truly pissed. In fact the Decision was to leave legislation on the table. The WaPo picked this up. Times will have to walk the story back and stop listening to the tech folks in the WH. Your city is moronic

From: Ceresney, Andrew [REDACTED]@SEC.GOV]
Sent: Sunday, October 11, 2015 9:13 AM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: smart phones

b6 Per SEC

Dan - Surprising article in NYT on WH position re encryption. Am sure you guys are not happy. Andrew

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

From: Richman, Daniel C. (DO) (OGA) [REDACTED]
Sent: Wednesday, October 07, 2015 08:39 PM Eastern Standard Time
To: Ceresney, Andrew
Cc: Oconnell, Sasha C. (DO) (FBI); Boujoukos, Jeffrey; [REDACTED]
Subject: RE: smart phones

b7E -3

b6 Per SEC

Thanks. More generally, even though it's always a challenge to clarify how a precluded line of investigation affected a case, and a particular challenge for an enforcement agency sensitive to disclosure risks, we'd appreciate hearing about other cases where password protection and encryption have stymied you Thx for being so quick on this Dan r

From: Ceresney, Andrew [REDACTED]@SEC.GOV]
Sent: Wednesday, October 07, 2015 7:10 PM
To: Richman, Daniel C. (DO) (OGA)
Cc: Oconnell, Sasha C. (DO) (FBI); Boujoukos, Jeffrey; [REDACTED]
Subject: RE: smart phones

b6 Per SEC

b5 Per SEC

Sure. Good to hear from you Dan. Glad to hear you are doing Gods work. I know about the case.

[REDACTED] our sense is the case with ultimately resolve -- hopefully in our favor --

FBI 18-CV-1833-4527

without us getting the chance to challenge it. And we are seeking other ways to try to get the info from the phone. I have cc'd Jeff Boujoukos and [REDACTED] who are in our Philly office and closest to the matter. They can provide more info. Andrew

b6 Per SEC

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

From: Richman, Daniel C. (DO) (OGA) [REDACTED]

b7E -3

Sent: Wednesday, October 07, 2015 07:07 PM Eastern Standard Time

To: Ceresney, Andrew

Cc: Oconnell, Sasha C. (DO) (FBI)

Subject: smart phones

Hi Andrew -- I'm working these days with Jim Comey and his crew on, among other things, the "Going Dark" problem. I don't know the extent to which the attached EDPa case -- about SEC access to a password protected smartphone -- is on your radar. But I (and Sasha O'Connell, the policy point person in the Director's office -- cc'd here) would love to get more information about the extent to which the problem is affecting your work, in this case and others.

thx

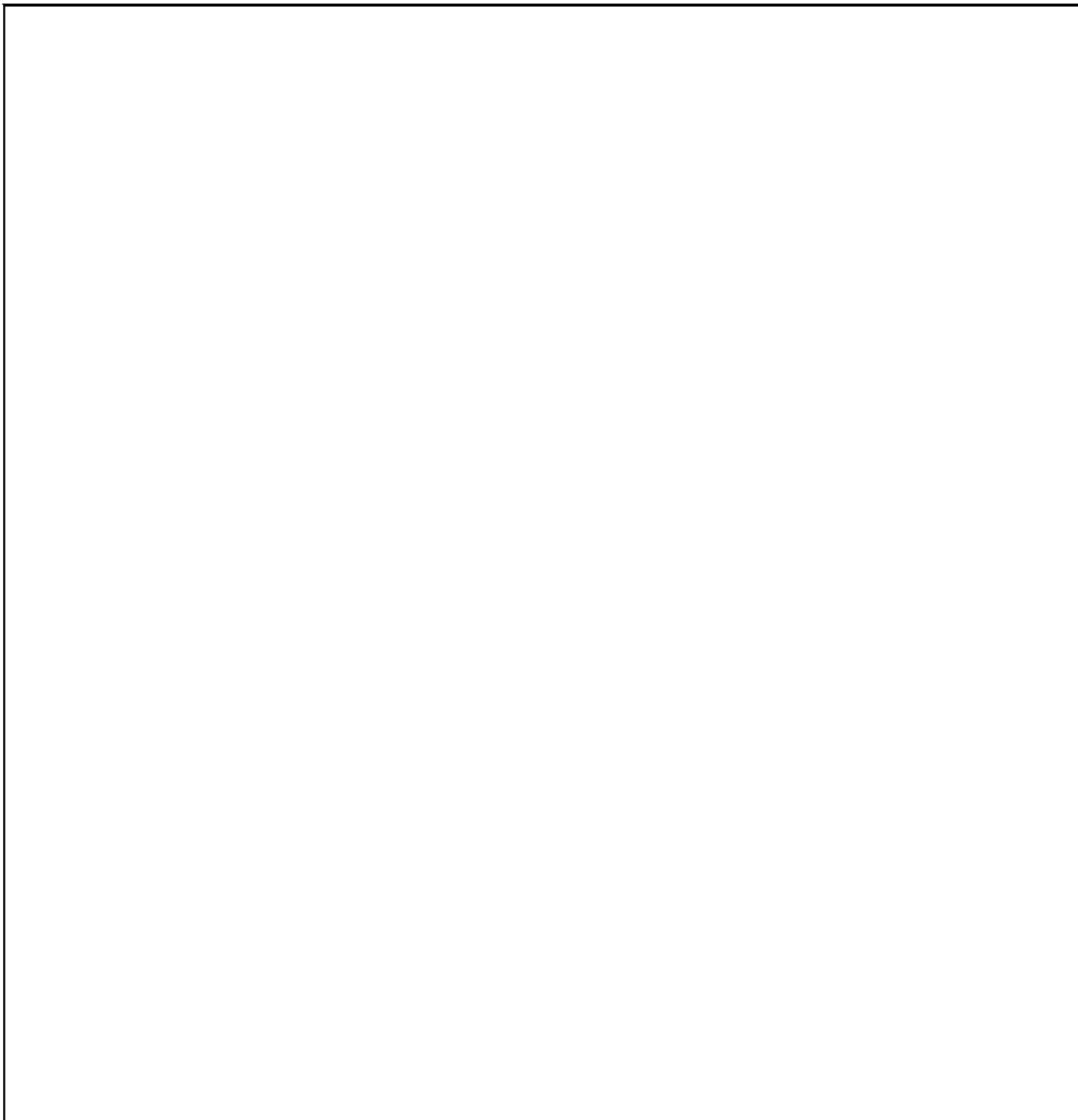
dan richman

Oconnell, Sasha C. (DO) (FBI)

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Sunday, October 11, 2015 10:01 AM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: With court order, federal judge seeks to fuel debate about data encryption from The Washington Post

Per your request, here is some background on the case.

b5 Per EOUSA



--

----- Original message -----

From: "Richman, Daniel C. (DO) (OGA)" [REDACTED]
Date: 10/11/2015 9:47 AM (GMT-05:00)
To: "Oconnell, Sasha C. (DO) (FBI)" [REDACTED]
Subject: RE: With court order, federal judge seeks to fuel debate about data encryption from The Washington Post

b6 -5
b7C -5
b7E -3

Thx. Suspect it would be useful if [REDACTED] reached out to the edny folks to coordinate

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Sunday, October 11, 2015 6:39 AM
To: Richman, Daniel C. (DO) (OGA)
Subject: Fwd: With court order, federal judge seeks to fuel debate about data encryption from The Washington Post

--

----- Original message -----

From: Sasha O'Connell [REDACTED]
Date: 10/11/2015 6:29 AM (GMT-05:00)
To: "Oconnell, Sasha C. (DO) (FBI)" [REDACTED]
Subject: With court order, federal judge seeks to fuel debate about data encryption from The Washington Post

b6 -1
b7C -1
b7E -3

<http://wpo.st/F9Cg0>

Sent from my iPhone

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Sunday, October 11, 2015 6:10 PM
To: Ceresney, Andrew
Subject: RE: smart phones

Wh ended up backing Jim as an official. But gosh that's a big building

From: Ceresney, Andrew [REDACTED]@SEC.GOV]
Sent: Sunday, October 11, 2015 10:00 AM
To: Richman, Daniel C. (DO) (OGA)
Subject: Re: smart phones

b6 Per SEC

Let's just say NY should not be judged by Times. Assume you are having trouble w Wh
Original Message

From: Richman, Daniel C. (DO) (OGA)
Sent: Sunday, October 11, 2015 9:42 AM
To: Ceresney, Andrew
Subject: RE: smart phones

Actually the nyt is totally wrong. Jim is truly pissed. In fact the Decision was to leave legislation on the table. The WaPo picked this up. Times will have to walk the story back and stop listening to the tech folks in the WH. Your city is moronic

From: Ceresney, Andrew [REDACTED]@SEC.GOV]
Sent: Sunday, October 11, 2015 9:13 AM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: smart phones

b6 Per SEC

Dan - Surprising article in NYT on WH position re encryption. Am sure you guys are not happy. Andrew

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

From: Richman, Daniel C. (DO) (OGA) [REDACTED]
Sent: Wednesday, October 07, 2015 08:39 PM Eastern Standard Time
To: Ceresney, Andrew
Cc: Oconnell, Sasha C. (DO) (FBI); Boujoukos, Jeffrey [REDACTED]
Subject: RE: smart phones

b7E -3

b6 Per SEC

Thanks. More generally, even though it's always a challenge to clarify how a precluded line of investigation affected a case, and a particular challenge for an enforcement agency sensitive to disclosure risks, we'd appreciate hearing about other cases where password protection and encryption have stymied you Thx for being so quick on this Dan r

From: Ceresney, Andrew [REDACTED]@SEC.GOV]

b6 Per SEC

FBI 18-CV-1833-4531

Sent: Wednesday, October 07, 2015 7:10 PM

To: Richman, Daniel C. (DO) (OGA)

Cc: Oconnell, Sasha C. (DO) (FBI); Boujoukos, Jeffrey; [REDACTED]

Subject: RE: smart phones

b6 Per SEC

b5 Per SEC

b6 Per SEC

Sure. Good to hear from you Dan. Glad to hear you are doing Gods work. I know about the case.

[REDACTED] our sense is the case with ultimately resolve -- hopefully in our favor -- without us getting the chance to challenge it. And we are seeking other ways to try to get the info from the phone. I have cc'd Jeff Boujoukos and [REDACTED] who are in our Philly office and closest to the matter. They can provide more info. Andrew

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

From: Richman, Daniel C. (DO) (OGA)

Sent: Wednesday, October 07, 2015 07:07 PM Eastern Standard Time

To: Ceresney, Andrew

Cc: Oconnell, Sasha C. (DO) (FBI)

Subject: smart phones

b7E -3

Hi Andrew -- I'm working these days with Jim Comey and his crew on, among other things, the "Going Dark" problem. I don't know the extent to which the attached EDPa case -- about SEC access to a password protected smartphone -- is on your radar. But I (and Sasha O'Connell, the policy point person in the Director's office -- cc'd here) would love to get more information about the extent to which the problem is affecting your work, in this case and others.

thx

dan richman

Oconnell, Sasha C. (DO) (FBI)

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Monday, October 12, 2015 9:38 AM
To: Richman, Daniel C. (DO) (OGA)
Subject: Fwd: DARPA paper on Encryption/Brandeis

----- Original message -----

From: "Launchbury, John" <john.launchbury@darpa.mil>
Date: 10/12/2015 12:19 AM (GMT-05:00)
To: "Raj, Kiran (ODAG) (JMD)" <Kiran.Raj@usdoj.gov>
Cc: "Oconnell, Sasha C. (DO) (FBI)" [REDACTED] [REDACTED]

[REDACTED]@darpa.mil> b6 Per DOD/OSD
Subject: Re: DARPA paper on Encryption/Brandeis b7E -3

Hi Kiran,

b5 Per DOD/OSD

I chatted with the DARPA director about this again on Thursday, [REDACTED]

[REDACTED]

Let me know whether this would meet your needs.

Thanks,
John

On Oct 9, 2015, at 4:28 PM, "Raj, Kiran (ODAG)" <Kiran.Raj@usdoj.gov> wrote:

Hi John -

I wanted to check in again. Apologies for pestering you on this, but we would like to review the paper as soon as possible. If it would be helpful for us to elevate the request, we are happy to do so. Please let us know what works best for your organization.

FBI 18-CV-1833-4533

Best,

Kiran

From: Raj, Kiran (ODAG)
Sent: Monday, October 05, 2015 1:56 PM
To: Oconnell, Sasha C. (DO) (FBI); Launchbury, John; [REDACTED] (US) b6 Per DOD/OSD
Cc: [REDACTED]
Subject: RE: DARPA paper on Encryption/Brandeis

Hi John –

I wanted to check back in on this to see where things stood. Let us know if there is anything you need from us.

Best,

Kiran

From: Oconnell, Sasha C. (DO) (FBI) [mailto:[REDACTED]] b6 -1 and Per DOD/OSD
Sent: Thursday, September 24, 2015 8:18 AM b7C -1
To: Launchbury, John; [REDACTED] b7E -3
Cc: Raj, Kiran (ODAG); [REDACTED]
Subject: RE: DARPA paper on Encryption/Brandeis

Thanks so much John, we look forward to connecting with you at your convenience and learning more about the program. Appreciate it!

Best,
Sasha

Sasha Cohen O'Connell
Chief, Office of National Policy
Office of the Deputy Director
FBIHQ-- [REDACTED]

From: Launchbury, John [john.launchbury@darpa.mil]
Sent: Thursday, September 24, 2015 6:38 AM
To: [REDACTED] b6 Per DOD/OSD
Cc: Oconnell, Sasha C. (DO) (FBI); Raj, Kiran (ODAG) (JMD); [REDACTED]
Subject: RE: DARPA paper on Encryption/Brandeis

Hi Harry,

b5 Per DOD/OSD

[REDACTED]

Thanks
John

John Launchbury

FBI 18-CV-1833-4534

Director, Information Innovation Office
DARPA

From: [REDACTED]
Sent: Tuesday, September 22, 2015 4:48:58 PM
To: Launchbury, John
Cc: Oconnell, Sasha C. (DO) (FBI); Raj, Kiran (ODAG) (JMD)
Subject: DARPA paper on Encryption/Brandeis

b6 Per DOD/OSD

John,

b5 Per DOD/OSD

[REDACTED]

V/r,

b6 Per DOD/OSD

[REDACTED]

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Monday, October 12, 2015 11:42 AM
To: Oconnell, Sasha C. (DO) (FBI)
Subject: RE: DARPA paper on Encryption/Brandeis

This sounds like a great idea, and I look forward to reading. Happy to pretend a large chunk of the USG doesn't exist ps - if you end up having to restrict this to the high side, please let me know and I'll to to the NYO to read _____

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Monday, October 12, 2015 9:38 AM
To: Richman, Daniel C. (DO) (OGA)
Subject: Fwd: DARPA paper on Encryption/Brandeis

--

----- Original message -----

From: "Launchbury, John" <john.launchbury@darpa.mil>
Date: 10/12/2015 12:19 AM (GMT-05:00)
To: "Raj, Kiran (ODAG) (JMD)" <Kiran.Raj@usdoj.gov>
Cc: "Oconnell, Sasha C. (DO) (FBI)" _____

b6 Per DOD/OSD
b7E -3

@darpa.mil>

Subject: Re: DARPA paper on Encryption/Brandeis

Hi Kiran,

b5 Per DOD/OSD

I chatted with the DARPA director about this again on Thursday, _____

Let me know whether this would meet your needs.

Thanks,
John

On Oct 9, 2015, at 4:28 PM, "Raj, Kiran (ODAG)" <Kiran.Raj@usdoj.gov<mailto:Kiran.Raj@usdoj.gov>>>
wrote:

FBI 18-CV-1833-4536

Hi John -

I wanted to check in again. Apologies for pestering you on this, but we would like to review the paper as soon as possible. If it would be helpful for us to elevate the request, we are happy to do so. Please let us know what works best for your organization.

Best,

Kiran

From: Raj, Kiran (ODAG)

Sent: Monday, October 05, 2015 1:56 PM

To: Oconnell, Sasha C. (DO) (FBI); Launchbury, John; Arter, [REDACTED]

b6 Per DOD/OSD

Cc: [REDACTED]

Subject: RE: DARPA paper on Encryption/Brandeis

Hi John -

I wanted to check back in on this to see where things stood. Let us know if there is anything you need from us.

Best,

Kiran

From: Oconnell, Sasha C. (DO) (FBI) [mailto:[REDACTED]]

b6 Per DOD/OSD

Sent: Thursday, September 24, 2015 8:18 AM

b7E -3

To: Launchbury, John; [REDACTED]

Cc: Raj, Kiran (ODAG); [REDACTED]

Subject: RE: DARPA paper on Encryption/Brandeis

Thanks so much John, we look forward to connecting with you at your convenience and learning more about the program. Appreciate it!

Best,

Sasha

Sasha Cohen O'Connell

Chief, Office of National Policy

Office of the Deputy Director

FBIHQ-- [REDACTED]

From: Launchbury, John [john.launchbury@darpa.mil<mailto:john.launchbury@darpa.mil>]

Sent: Thursday, September 24, 2015 6:38 AM

To: [REDACTED]

b6 Per DOD/OSD

Cc: Oconnell, Sasha C. (DO) (FBI); Raj, Kiran (ODAG) (JMD); [REDACTED]

Subject: RE: DARPA paper on Encryption/Brandeis

[REDACTED]



Thanks
John

John Launchbury
Director, Information Innovation Office
DARPA

From [REDACTED]
Sent: Tuesday, September 22, 2015 4:48:58 PM
To: Launchbury, John
Cc: Oconnell, Sasha C. (DO) (FBI); Raj, Kiran (ODAG) (JMD)
Subject: DARPA paper on Encryption/Brandeis
John,

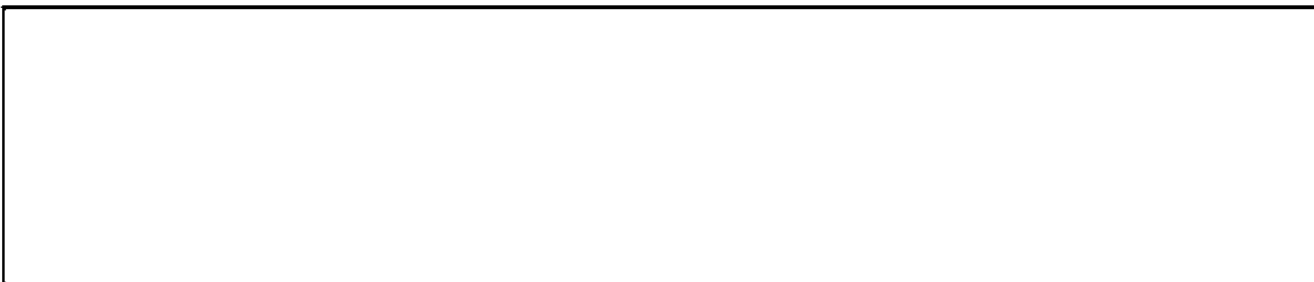
b6 Per DOD/OSD

b5 Per DOD/OSD



V/r,

b6 Per DOD/OSD



Richman, Daniel C. (DO) (OGA)

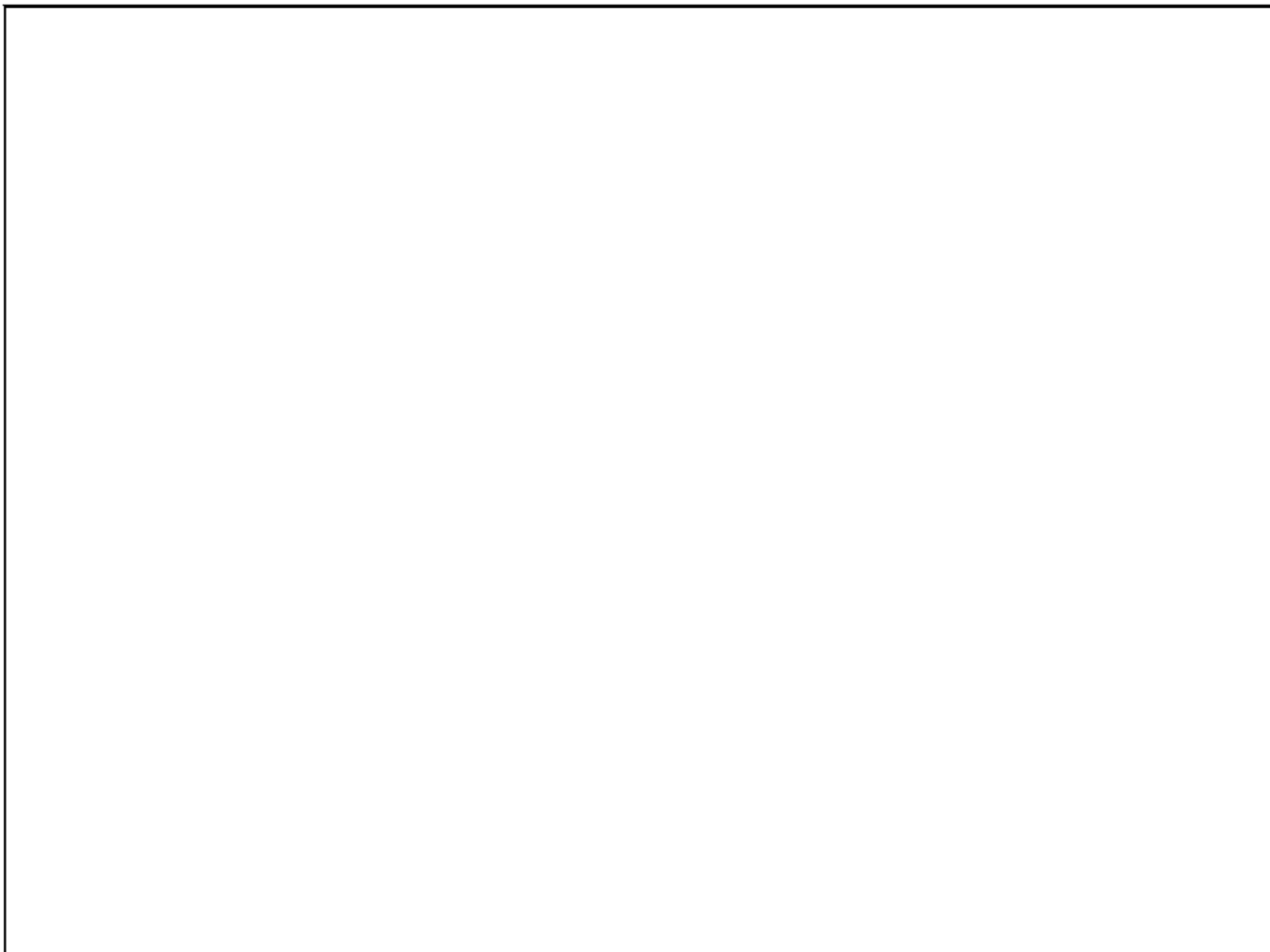
From: Richman, Daniel C. (DO) (OGA)
Sent: Monday, October 12, 2015 11:57 AM
To: Oconnell, Sasha C. (DO) (FBI)
Subject: RE: With court order, federal judge seeks to fuel debate about data encryption from The Washington Post

This case reminds me that we should include DEA in our reaching out for emerging GD problems. I'm happy to ask Chuck R (who obviously knows about the issue but may not have alerted his crew), but you might prefer to do this thru real people. Just let me know d

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Sunday, October 11, 2015 10:00 AM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: With court order, federal judge seeks to fuel debate about data encryption from The Washington Post

Per your request, here is some background on the case.

b5 Per EOUSA





--

----- Original message -----

From: "Richman, Daniel C. (DO) (OGA)" [REDACTED]
Date: 10/11/2015 9:47 AM (GMT-05:00)
To: "Oconnell, Sasha C. (DO) (FBI)" [REDACTED]
Subject: RE: With court order, federal judge seeks to fuel debate about data encryption from The Washington Post

b6 -5
b7C -5
b7E -3

Thx. Suspect it would be useful if [REDACTED] reached out to the edny folks to coordinate

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Sunday, October 11, 2015 6:39 AM
To: Richman, Daniel C. (DO) (OGA)
Subject: Fwd: With court order, federal judge seeks to fuel debate about data encryption from The Washington Post

--

----- Original message -----

From: Sasha O'Connell [REDACTED]
Date: 10/11/2015 6:29 AM (GMT-05:00)
To: "Oconnell, Sasha C. (DO) (FBI)" [REDACTED]
Subject: With court order, federal judge seeks to fuel debate about data encryption from The Washington Post

b6 -1
b7C -1
b7E -3

<http://wpo.st/F9Cg0>

Sent from my iPhone

Oconnell, Sasha C. (DO) (FBI)

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Monday, October 12, 2015 11:45 AM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: DARPA paper on Encryption/Brandeis

Will do thanks! :)

----- Original message -----

From: "Richman, Daniel C. (DO) (OGA)" [REDACTED]
Date: 10/12/2015 11:44 AM (GMT-05:00)
To: "Oconnell, Sasha C. (DO) (FBI)" [REDACTED]
Subject: RE: DARPA paper on Encryption/Brandeis

b7E -3

This sounds like a great idea, and I look forward to reading. Happy to pretend a large chunk of the USG doesn't exist ps - if you end up having to restrict this to the high side, please let me know and I'll to to the NYO to read

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Monday, October 12, 2015 9:38 AM
To: Richman, Daniel C. (DO) (OGA)
Subject: Fwd: DARPA paper on Encryption/Brandeis

--

----- Original message -----

From: "Launchbury, John" <john.launchbury@darpa.mil>
Date: 10/12/2015 12:19 AM (GMT-05:00)
To: "Raj, Kiran (ODAG) (JMD)" <Kiran.Raj@usdoj.gov>
Cc: "Oconnell, Sasha C. (DO) (FBI)" [REDACTED]

[REDACTED]@darpa.mil>
Subject: Re: DARPA paper on Encryption/Brandeis

b6 Per DOD/OSD
b7E -3

Hi Kiran,

b5 Per DOD/OSD

I chatted with the DARPA director about this again on Thursday, [REDACTED]

[REDACTED]

Let me know whether this would meet your needs.

Thanks,
John

FBI 18-CV-1833-4541

On Oct 9, 2015, at 4:28 PM, "Raj, Kiran (ODAG)" <Kiran.Raj@usdoj.gov<mailto:Kiran.Raj@usdoj.gov>> wrote:

Hi John –

I wanted to check in again. Apologies for pestering you on this, but we would like to review the paper as soon as possible. If it would be helpful for us to elevate the request, we are happy to do so. Please let us know what works best for your organization.

Best,

Kiran

From: Raj, Kiran (ODAG)

Sent: Monday, October 05, 2015 1:56 PM

To: Oconnell, Sasha C. (DO) (FBI); Launchbury, John; Arter, [REDACTED]

b6 Per DOD/OSD

Cc: [REDACTED]

Subject: RE: DARPA paper on Encryption/Brandeis

Hi John –

I wanted to check back in on this to see where things stood. Let us know if there is anything you need from us.

Best,

Kiran

From: Oconnell, Sasha C. (DO) (FBI) [mailto:[REDACTED]]

b6 Per DOD/OSD

Sent: Thursday, September 24, 2015 8:18 AM

b7E -3

To: Launchbury, John [REDACTED]

Cc: Raj, Kiran (ODAG) [REDACTED]

Subject: RE: DARPA paper on Encryption/Brandeis

Thanks so much John, we look forward to connecting with you at your convenience and learning more about the program. Appreciate it!

Best,

Sasha

Sasha Cohen O'Connell

Chief, Office of National Policy

Office of the Deputy Director

FBIHQ-[REDACTED]

From: Launchbury, John [john.launchbury@darpa.mil<mailto:john.launchbury@darpa.mil>]

Sent: Thursday, September 24, 2015 6:38 AM

To: [REDACTED]

b6 Per DOD/OSD

Cc: Oconnell, Sasha C. (DO) (FBI); Raj, Kiran (ODAG) (JMD); [REDACTED]

Subject: RE: DARPA paper on Encryption/Brandeis

b5 Per DOD/OSD

Thanks
John

John Launchbury

FBI 18-CV-1833-4542

Director, Information Innovation Office
DARPA

From: [REDACTED]
Sent: Tuesday, September 22, 2015 4:48:58 PM
To: Launchbury, John
Cc: Oconnell, Sasha C. (DO) (FBI); Raj, Kiran (ODAG) (JMD)
Subject: DARPA paper on Encryption/Brandeis
John,

b6 Per DOD/OSD

b5 Per DOD/OSD

V/r,

b6 Per DOD/OSD

Oconnell, Sasha C. (DO) (FBI)

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Monday, October 12, 2015 1:12 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: With court order, federal judge seeks to fuel debate about data encryption from The Washington Post

Oh yes we are working with Chuck. We did a note and presentation for him. He sent it out to his whole workforce.

--

----- Original message -----

From: "Richman, Daniel C. (DO) (OGA)" [REDACTED]
Date: 10/12/2015 11:59 AM (GMT-05:00)
To: "Oconnell, Sasha C. (DO) (FBI)" [REDACTED]
Subject: RE: With court order, federal judge seeks to fuel debate about data encryption from The Washington Post

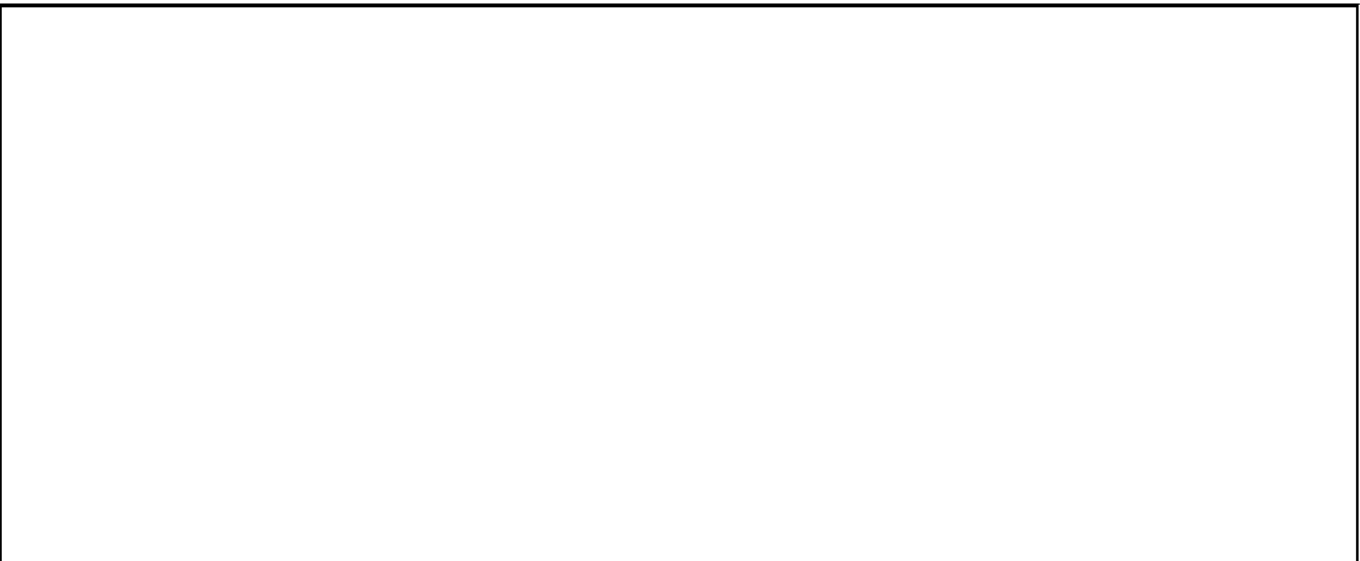
b7E -3

This case reminds me that we should include DEA in our reaching out for emerging GD problems. I'm happy to ask Chuck R (who obviously knows about the issue but may not have alerted his crew), but you might prefer to do this thru real people. Just let me know
d

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Sunday, October 11, 2015 10:00 AM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: With court order, federal judge seeks to fuel debate about data encryption from The Washington Post

Per your request, here is some background on the case.

b5 Per EOUSA





--

----- Original message -----

From: "Richman, Daniel C. (DO) (OGA)" [REDACTED]
Date: 10/11/2015 9:47 AM (GMT-05:00)
To: "Oconnell, Sasha C. (DO) (FBI)" [REDACTED]
Subject: RE: With court order, federal judge seeks to fuel debate about data encryption from The Washington Post

b6 -5
b7C -5
b7E -3

Thx. Suspect it would be useful if [REDACTED] reached out to the edny folks to coordinate

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Sunday, October 11, 2015 6:39 AM
To: Richman, Daniel C. (DO) (OGA)
Subject: Fwd: With court order, federal judge seeks to fuel debate about data encryption from The Washington Post

--

----- Original message -----

From: Sasha O'Connell [REDACTED]
Date: 10/11/2015 6:29 AM (GMT-05:00)
To: "Oconnell, Sasha C. (DO) (FBI)" [REDACTED]
Subject: With court order, federal judge seeks to fuel debate about data encryption from The Washington Post

b6 -1
b7C -1
b7E -3

<http://wpo.st/F9Cg0>

Sent from my iPhone

Oconnell, Sasha C. (DO) (FBI)

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Monday, October 12, 2015 2:22 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: Fwd: Correcting the Record

FYSA...

----- Original message -----

From: "Raj, Kiran (ODAG)" <Kiran.Raj@usdoj.gov>
Date: 10/12/2015 1:57 PM (GMT-05:00)
To: "Oconnell, Sasha C. (DO) (FBI)" [REDACTED]
Subject: Fwd: Correcting the Record

b7E -3

Sent from my iPhone

Begin forwarded message:

From: "Raj, Kiran (ODAG)" <kraj@jmd.usdoj.gov<mailto:kraj@jmd.usdoj.gov>>
Date: October 12, 2015 at 1:56:36 PM EDT
To: "Joe M. EOP Daniel" [REDACTED]

Mark Stroh

b6 Per NSC

Cc: "Pierce, Emily (OPA)" <enierce@jmd.usdoj.gov<mailto:enierce@jmd.usdoj.gov>> "Andrew [REDACTED]
[REDACTED] Scott" [REDACTED] "Newman, Melanie (OPA)"
<mnewman@jmd.usdoj.gov<mailto:mnewman@jmd.usdoj.gov>>
Subject: Correcting the Record

Michael & Mark -

b5 Per DOJ/OIP and NSC

As you have probably seen, [REDACTED]

FBI 18-CV-1833-4548



I am happy to chat further if you would like.

Best,

Kiran

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Monday, October 12, 2015 2:29 PM
To: Oconnell, Sasha C. (DO) (FBI)
Subject: RE: Correcting the Record

nice. Maybe Kiran should have added -- And beyond this, pls tell your people to shut the hell up

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Monday, October 12, 2015 2:21 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: Fwd: Correcting the Record

FYSA...

--

----- Original message -----

From: "Raj, Kiran (ODAG)" <Kiran.Raj@usdoj.gov>
Date: 10/12/2015 1:57 PM (GMT-05:00)
To: "Oconnell, Sasha C. (DO) (FBI)" [REDACTED]
Subject: Fwd: Correcting the Record

b7E -3

Sent from my iPhone

Begin forwarded message:

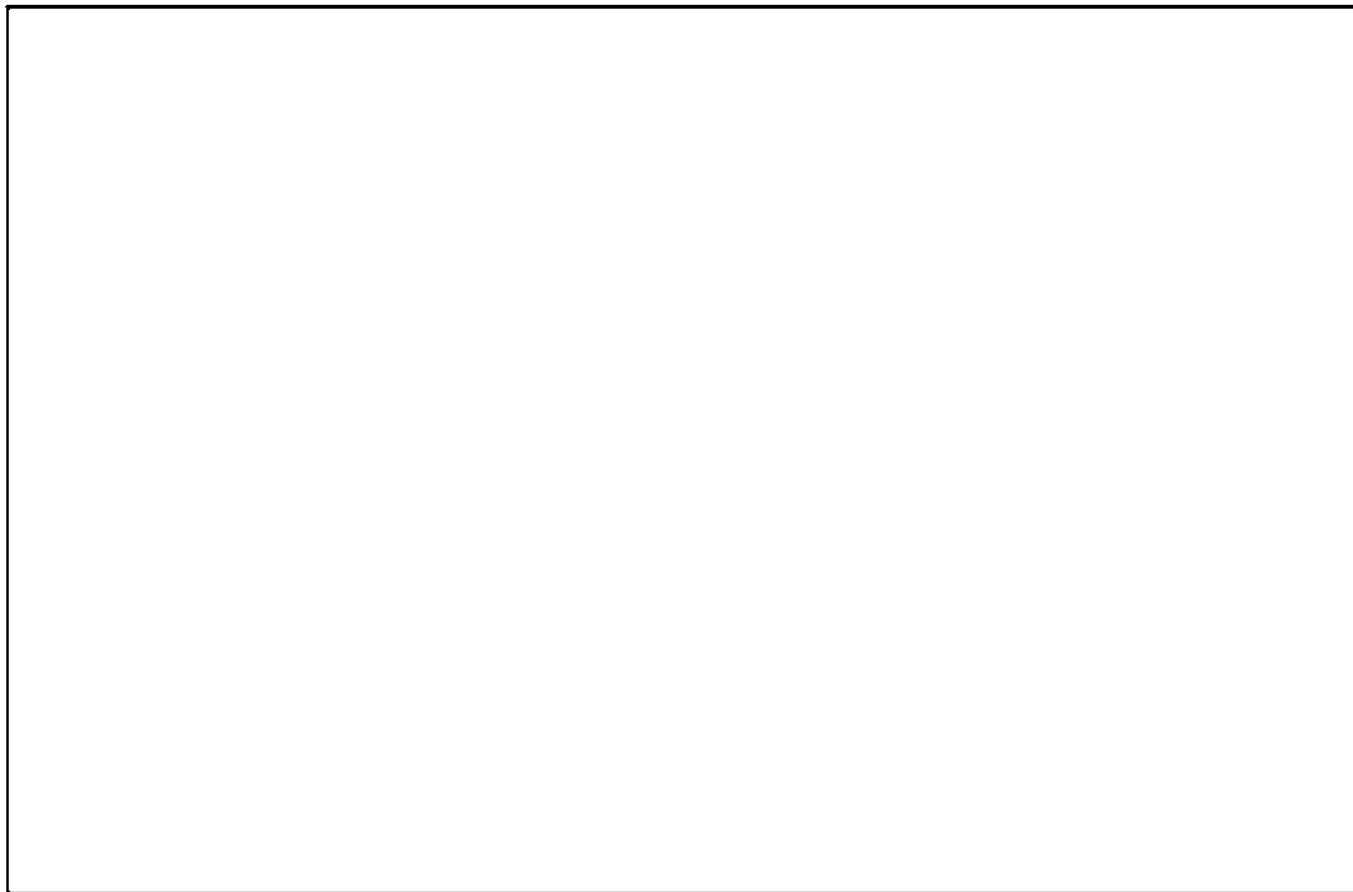
From: "Raj, Kiran (ODAG)" <kraj@jmd.usdoj.gov<mailto:kraj@jmd.usdoj.gov>>
Date: October 12, 2015 at 1:56:36 PM EDT
To: "Joe M. EOP Daniel" [REDACTED] Mark b6 Per NSC
Stroh [REDACTED]
Cc: "Pierce, Emily (OPA)" <epierce@jmd.usdoj.gov<mailto:epierce@jmd.usdoj.gov>>, "Andrew [REDACTED] Scott" [REDACTED]
[REDACTED] "Newman, Melanie (OPA)" <mnewman@jmd.usdoj.gov<mailto:mnewman@jmd.usdoj.gov>>
Subject: Correcting the Record

Michael & Mark -

b5 Per DOJ/OIP

As you have probably seen, [REDACTED]
[REDACTED]

FBI 18-CV-1833-4550



I am happy to chat further if you would like.

Best,

Kiran

Oconnell, Sasha C. (DO) (FBI)

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Monday, October 12, 2015 2:31 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: Correcting the Record

OK you made me laugh out loud ;)

----- Original message -----

From: "Richman, Daniel C. (DO) (OGA)" [REDACTED]
Date: 10/12/2015 2:30 PM (GMT-05:00)
To: "Oconnell, Sasha C. (DO) (FBI)" [REDACTED]
Subject: RE: Correcting the Record

b7E -3

nice. Maybe Kiran should have added -- And beyond this, pls tell your people to shut the hell up

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Monday, October 12, 2015 2:21 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: Fwd: Correcting the Record

FYSA...

--

----- Original message -----

From: "Raj, Kiran (ODAG)" <Kiran.Raj@usdoj.gov>
Date: 10/12/2015 1:57 PM (GMT-05:00)
To: "Oconnell, Sasha C. (DO) (FBI)" [REDACTED]
Subject: Fwd: Correcting the Record

b7E -3

Sent from my iPhone

Begin forwarded message:

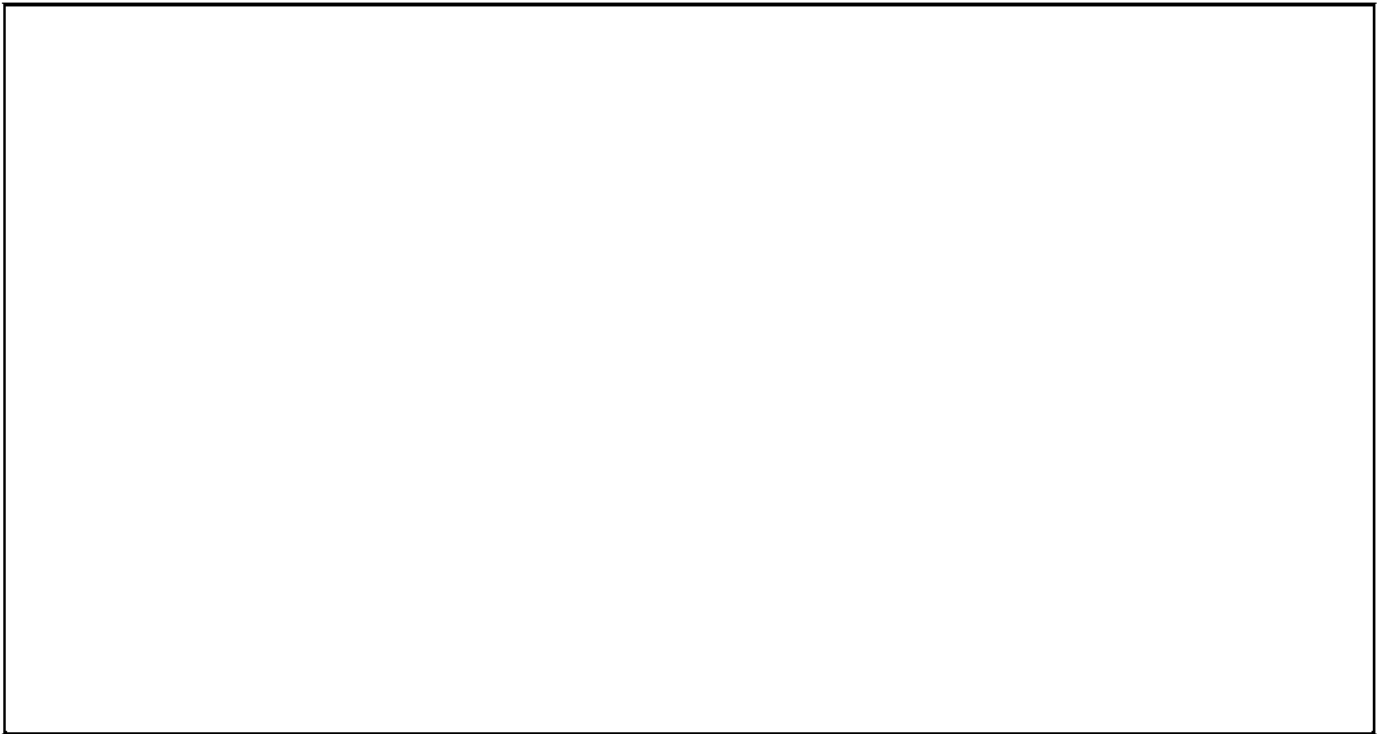
From: "Raj, Kiran (ODAG)" <kraj@jmd.usdoj.gov<mailto:kraj@jmd.usdoj.gov>>
Date: October 12, 2015 at 1:56:36 PM EDT
To: "Joe M. EOP Daniel" [REDACTED]

Mark Stroh

b6 Per NSC

Cc: "Pierce, Emily (OPA)" <epierce@jmd.usdoj.gov<mailto:epierce@jmd.usdoj.gov>>, "Andrew [REDACTED]
[REDACTED] Scott" [REDACTED] "Newman, Melanie (OPA)"
<mnewman@jmd.usdoj.gov<mailto:mnewman@jmd.usdoj.gov>>
Subject: Correcting the Record

FBI 18-CV-1833-4552



I am happy to chat further if you would like.

Best,

Kiran

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Monday, October 12, 2015 4:16 PM
To: Oconnell, Sasha C. (DO) (FBI)
Subject: RE: Correcting the Record

good tea leaf reading at
<https://www.lawfareblog.com/administration-decision-encryption-policy>

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Monday, October 12, 2015 2:31 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: Correcting the Record

OK you made me laugh out loud ;)

--

----- Original message -----

From: "Richman, Daniel C. (DO) (OGA)" [redacted]
Date: 10/12/2015 2:30 PM (GMT-05:00)
To: "Oconnell, Sasha C. (DO) (FBI)" [redacted]
Subject: RE: Correcting the Record

b7E -3

nice. Maybe Kiran should have added -- And beyond this, pls tell your people to shut the hell up

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Monday, October 12, 2015 2:21 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: Fwd: Correcting the Record

FYSA...

--

----- Original message -----

From: "Raj, Kiran (ODAG)" <Kiran.Raj@usdoj.gov>
Date: 10/12/2015 1:57 PM (GMT-05:00)
To: "Oconnell, Sasha C. (DO) (FBI)" [redacted]

b7E -3

FBI 18-CV-1833-4554

Subject: Fwd: Correcting the Record

Sent from my iPhone

Begin forwarded message:

From: "Raj, Kiran (ODAG)" <kraj@jmd.usdoj.gov<mailto:kraj@jmd.usdoj.gov>>

b6 Per NSC

Date: October 12, 2015 at 1:56:36 PM EDT

To: "Joe M. EOP Daniel" [REDACTED], Mark

Stroh [REDACTED]

Cc: "Pierce, Emily (OPA)" <epierce@jmd.usdoj.gov<mailto:epierce@jmd.usdoj.gov>>, "Andrew

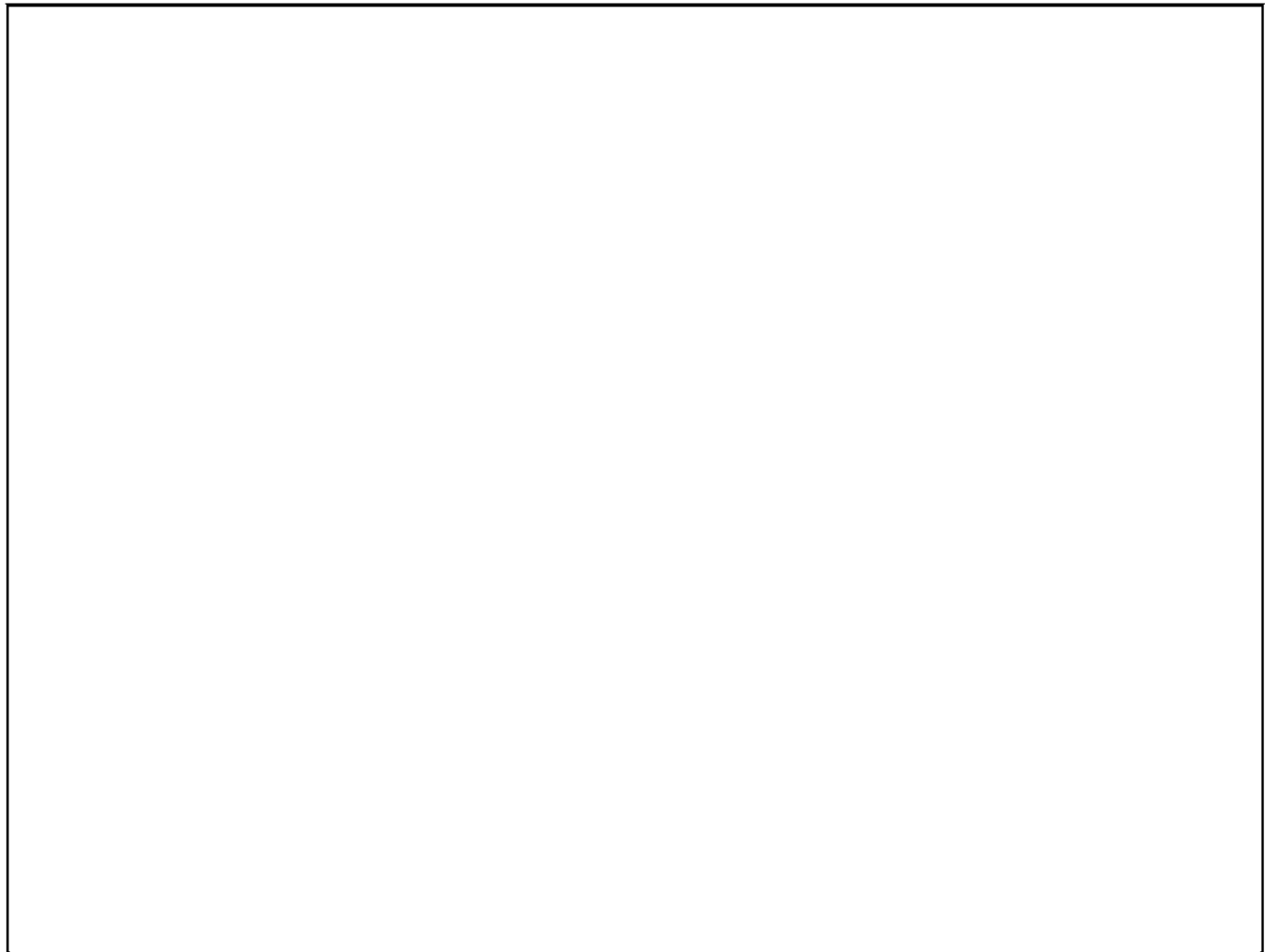
[REDACTED] Scott" [REDACTED]

[REDACTED] "Newman, Melanie (OPA)" <mnewman@jmd.usdoj.gov<mailto:mnewman@jmd.usdoj.gov>>

Subject: Correcting the Record

Michael & Mark -

b5 Per DOJ/OIP and NSC



I am happy to chat further if you would like.

Best,

Kiran

Oconnell, Sasha C. (DO) (FBI)

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Monday, October 12, 2015 10:42 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: Fwd:

...

----- Original message -----

From: "Raj, Kiran (ODAG)" <Kiran.Raj@usdoj.gov>
Date: 10/12/2015 9:09 PM (GMT-05:00)
To: "Oconnell, Sasha C. (DO) (FBI)" [REDACTED]
Subject:

b7E -3

<http://www.digitaltrends.com/apple/apple-deactivates-its-news-app-in-china-to-appease-censorship-requirements/>

Sent from my iPhone

Oconnell, Sasha C. (DO) (FBI)

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Monday, October 12, 2015 4:43 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: Correcting the Record

indeed!

From: Richman, Daniel C. (DO) (OGA)
Sent: Monday, October 12, 2015 4:16 PM
To: Oconnell, Sasha C. (DO) (FBI)
Subject: RE: Correcting the Record

good tea leaf reading at
<https://www.lawfareblog.com/administration-decision-encryption-policy>

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Monday, October 12, 2015 2:31 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: Correcting the Record

OK you made me laugh out loud ;)

--

----- Original message -----

From: "Richman, Daniel C. (DO) (OGA)" [REDACTED]
Date: 10/12/2015 2:30 PM (GMT-05:00)
To: "Oconnell, Sasha C. (DO) (FBI)" [REDACTED]
Subject: RE: Correcting the Record

b7E -3

nice. Maybe Kiran should have added -- And beyond this, pls tell your people to shut the hell up

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Monday, October 12, 2015 2:21 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: Fwd: Correcting the Record

FYSA...

FBI 18-CV-1833-4558

----- Original message -----

From: "Raj, Kiran (ODAG)" <Kiran.Raj@usdoj.gov>

Date: 10/12/2015 1:57 PM (GMT-05:00)

To: "Oconnell, Sasha C. (DO) (FBI)" [REDACTED]

Subject: Fwd: Correcting the Record

b7E -3

Sent from my iPhone

Begin forwarded message:

From: "Raj, Kiran (ODAG)" <kraj@jmd.usdoj.gov<mailto:kraj@jmd.usdoj.gov>>

Date: October 12, 2015 at 1:56:36 PM EDT

To: "Joe M. EOP Daniel" [REDACTED]

Mark b6 Per NSC

Stroh [REDACTED]

Cc: "Pierce, Emily (OPA)" <epierce@jmd.usdoj.gov<mailto:epierce@jmd.usdoj.gov>>, "Andrew

[REDACTED] Scott" [REDACTED]

[REDACTED] "Newman, Melanie (OPA)" <mnewman@jmd.usdoj.gov<mailto:mnewman@jmd.usdoj.gov>>

Subject: Correcting the Record

Michael & Mark -

b5 Per DOJ/OIP and Per NSC

I am happy to chat further if you would like.

Best,

Kiran

Oconnell, Sasha C. (DO) (FBI)

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Wednesday, October 14, 2015 8:48 AM
To: Richman, Daniel C. (DO) (OGA)
Subject: Fwd: DARPA Paper on Encryption
Attachments: Law-Enforcement_Access_Paper_(Sept_2015).docx

Please do not distribute further; not for attribution as discussed. Thanks!

----- Original message -----

From: [REDACTED]
Date: 10/14/2015 8:43 AM (GMT-05:00)
To: [REDACTED]
[REDACTED]
Subject: DARPA Paper on Encryption

b6 Per DOD/OSD

b7E -3

b5 Per DOD/OSD

b6 Per DOD/OSD

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Wednesday, October 14, 2015 11:31 AM
To: Oconnell, Sasha C. (DO) (FBI)
Subject: RE: DARPA Paper on Encryption



b5 -1
b6 -2
b7C -2

(It would be useful if Jim Burrell could see the DARPA paper but I won't distribute without your OK)

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Wednesday, October 14, 2015 8:47 AM
To: Richman, Daniel C. (DO) (OGA)
Subject: Fwd: DARPA Paper on Encryption

Please do not distribute further; not for attribution as discussed. Thanks!

--

----- Original message -----

From: [REDACTED]
Date: 10/14/2015 8:43 AM (GMT-05:00)
To: [REDACTED]
[REDACTED]

b6 Per DOD/OSD
b7E -3

Subject: DARPA Paper on Encryption



b5 Per DOD/OSD

FBI 18-CV-1833-4586

V/r,



b6 Per DOD/OSD

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Wednesday, October 14, 2015 12:05 PM
To: Oconnell, Sasha C. (DO) (FBI); Burrell, James C. (OTD) (FBI)
Subject: RE: DARPA Paper on Encryption

Just to add, Jim --

b5 -1

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Wednesday, October 14, 2015 12:00 PM
To: Burrell, James C. (OTD) (FBI)
Cc: Richman, Daniel C. (DO) (OGA)
Subject: FW: DARPA Paper on Encryption

Jim,

We have received the attached from DOD with the caveat we will not distribute or raise ideas included here with attribution. That being said it is good background going into the Friday discussion--I don't think there is anything terribly new here

b5 -1

but it would be helpful if you could take a look before Friday and let me and Dan know what you think and if there is anything here worth kind of raising in general terms?

Thank you!!

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

From: [REDACTED]
Sent: Wednesday, October 14, 2015 8:43 AM
To: [REDACTED]
Subject: DARPA Paper on Encryption

b6 Per DOD/OSD

b5 Per DOD/OSD

b6 Per DOD/OSD



b6 Per DOD/OSD

Oconnell, Sasha C. (DO) (FBI)

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Wednesday, October 14, 2015 12:01 PM
To: Burrell, James C. (OTD) (FBI)
Cc: Richman, Daniel C. (DO) (OGA)
Subject: FW: DARPA Paper on Encryption
Attachments: Law-Enforcement_Access_Paper_(Sept_2015).docx

Jim,

We have received the attached from DOD with the caveat we will not distribute or raise ideas included here with attribution. That being said it is good background going into the Friday discussion--I don't think there is anything terribly new here [REDACTED]

b5 -1

[REDACTED] but it would be helpful if you could take a look before Friday and let me and Dan know what you think and if there is anything here worth kind of raising in general terms?
Thank you!!

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

From: [REDACTED]
Sent: Wednesday, October 14, 2015 8:43 AM
To: [REDACTED]
Subject: DARPA Paper on Encryption

b6 Per DOD/OSD

b5 Per DOD/OSD

b6 Per DOD/OSD

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Thursday, October 15, 2015 3:05 PM
To: Oconnell, Sasha C. (DO) (FBI)
Subject: DARPA

Yes, it's last minute, but I wonder if it's worth putting a pitch in to DARPA to send someone to lurk. That outfit might be a pivotal contributor down the road, and the paper -- altho it was written in May -- suggests that they would benefit from plugging into the policy debate.

Oconnell, Sasha C. (DO) (FBI)

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Thursday, October 15, 2015 3:14 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: DARPA

I think based on their emails that they have been instructed to stay out of the formal policy discuss and thus would decline (and my guess is it might make them nervous to be invited). I would say for sure DOD in the next round but they may be hesitant too. I know DHS would love to come :)
On the train now working our way to you!

--

----- Original message -----

From: "Richman, Daniel C. (DO) (OGA)" [REDACTED]
Date: 10/15/2015 3:08 PM (GMT-05:00)
To: "Oconnell, Sasha C. (DO) (FBI)" [REDACTED]
Subject: DARPA

b7E -3

Yes, it's last minute, but I wonder if it's worth putting a pitch in to DARPA to send someone to lurk. That outfit might be a pivotal contributor down the road, and the paper -- altho it was written in May -- suggests that they would benefit from plugging into the policy debate.

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Thursday, October 15, 2015 3:17 PM
To: Oconnell, Sasha C. (DO) (FBI)
Subject: RE: DARPA

Makes sense on DARPA

When it comes to DHS, I feel like a "Mean Girl" have a lovely trip. City is beautiful today

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Thursday, October 15, 2015 3:13 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: DARPA

I think based on their emails that they have been instructed to stay out of the formal policy discuss and thus would decline (and my guess is it might make them nervous to be invited). I would say for sure DOD in the next round but they may be hesitant too. I know DHS would love to come :) On the train now working our way to you!

--

----- Original message -----

From: "Richman, Daniel C. (DO) (OGA)" [redacted]
Date: 10/15/2015 3:08 PM (GMT-05:00)
To: "Oconnell, Sasha C. (DO) (FBI)" [redacted]
Subject: DARPA

b7E -3

Yes, it's last minute, but I wonder if it's worth putting a pitch in to DARPA to send someone to lurk. That outfit might be a pivotal contributor down the road, and the paper -- altho it was written in May -- suggests that they would benefit from plugging into the policy debate.

Oconnell, Sasha C. (DO) (FBI)

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Thursday, October 15, 2015 3:27 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: DARPA

You completely crack me up :) see you soon!!

----- Original message -----

From: "Richman, Daniel C. (DO) (OGA)" [REDACTED]
Date: 10/15/2015 3:18 PM (GMT-05:00)
To: "Oconnell, Sasha C. (DO) (FBI)" [REDACTED]
Subject: RE: DARPA

b7E -3

Makes sense on DARPA
When it comes to DHS, I feel like a "Mean Girl"
have a lovely trip. City is beautiful today

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Thursday, October 15, 2015 3:13 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: DARPA

I think based on their emails that they have been instructed to stay out of the formal policy discuss and thus would decline (and my guess is it might make them nervous to be invited). I would say for sure DOD in the next round but they may be hesitant too. I know DHS would love to come :)
On the train now working our way to you!

--

----- Original message -----

From: "Richman, Daniel C. (DO) (OGA)" [REDACTED]
Date: 10/15/2015 3:08 PM (GMT-05:00)
To: "Oconnell, Sasha C. (DO) (FBI)" [REDACTED]
Subject: DARPA

b7E -3

Yes, it's last minute, but I wonder if it's worth putting a pitch in to DARPA to send someone to lurk. That outfit might be a pivotal contributor down the road, and the paper -- altho it was written in May -- suggests that they would benefit from plugging into the policy debate.

Krieger, Paul (USANYS)

From: Krieger, Paul (USANYS)
Sent: Thursday, October 15, 2015 6:41 PM
To: Richman, Daniel C. (DO) (OGA)
Cc: Loughnane, Joan (USANYS)
Subject: Roundtable at Columbia

Dan -

Hope all is well. We just wanted to touch base on the roundtable tomorrow. When we spoke about it at last week's meeting at FBI NY, my impression was that the roundtable wasn't going to be open to the public. Is that right? [REDACTED]

[REDACTED] If your thinking on that has changed, let us know.

b5 Per EOUSA

Thanks Dan. Speak to you soon.

Best,
Paul

b6 -1,2,5
b7C -1,2,5
b7D -1
b7E -3

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

From: Richman, Daniel C. (DO) (OGA) [mailto:[REDACTED]]
Sent: Friday, October 09, 2015 11:01 AM
To: Burrell, James C. (OTD) (FBI); [REDACTED] (DO) (FBI); Oconnell, Sasha C. (DO) (FBI); Baker, James A. (OGC) (FBI); [REDACTED] (DO) (FBI); [REDACTED] (ODAG) (JMD); [REDACTED] (CRM); Krieger, Paul (USANYS); Loughnane, Joan (USANYS)
Subject: DANY going dark white paper

Dear All -- Attached, courtesy of Ben Rosenberg at DANY, is [REDACTED]

[REDACTED] Ben has authorized me to share it within the DOJ family but on condition that it be kept "confidential." I'm confident that Ben would welcome constructive criticism, either before or after the 10/16 roundtable (which he'll be attending).
thx
dan richman

Krieger, Paul (USANYS)

From: Krieger, Paul (USANYS)
Sent: Thursday, October 15, 2015 10:21 PM
To: Richman, Daniel C. (DO) (OGA)
Cc: Loughnane, Joan (USANYS)
Subject: Re: Roundtable at Columbia

b6 Per EOUSA

Thanks a lot Dan. Makes sense. I also touched base with Sasha tonight on these issues. That case is interesting.

b5 Per EOUSA
b6 -1 and Per EOUSA
b7C -1
b7E -3

> On Oct 15, 2015, at 8:24 PM, Richman, Daniel C. (DO) (OGA) wrote:

>

> Right on both counts.

If this is productive there will be more such conversations that I'd love you to join. In the meantime from the NYO will be reaching to you to make sure we capture problems that occur in your nonbureau cases.

> Meanwhile, we are watching what Apple will do in the case with SDNY law may be different but I suspect that Apple will be rethinking its position across districts. Which will make it more adversarial or not.

> _____ > From: Krieger, Paul (USANYS)

[Paul.Krieger@usdoj.gov] > Sent: Thursday, October 15, 2015 6:41 PM > To: Richman, Daniel C. (DO) (OGA) > Cc: Loughnane, Joan (USANYS) > Subject: Roundtable at Columbia

>

> Dan -

> Hope all is well. We just wanted to touch base on the roundtable tomorrow. When we spoke about it at last week's meeting at FBI NY, my impression was that the roundtable wasn't going to be open to the public. Is that right?

If your thinking on that has changed, let us know.

b5 Per EOUSA

> Thanks Dan. Speak to you soon.

> Best,

> Paul

>

> -----Original Message-----

b6 -1,2,5
b7C -1,2,5
b7D -1
b7E -3

> From: Richman, Daniel C. (DO) (OGA) [mailto:]

> Sent: Friday, October 09, 2015 11:01 AM

> To: Burrell, James C. (OTD) (FBI); (DO) (FBI); Oconnell, Sasha C. (DO) (FBI); Baker, James A. (OGC) (FBI); (DO) (FBI); (ODAG) (JMD); (CRM); Krieger, Paul (USANYS); Loughnane, Joan (USANYS)

> Subject: DANY going dark white paper

>

> Dear All -- Attached, courtesy of Ben Rosenberg at DANY

Ben has authorized me to share it within the DOJ family but on condition that it be kept "confidential." I'm confident that Ben would welcome constructive criticism, either before or after the 10/16 roundtable (which he'll be attending).

FBI 18-CV-1833-4609

> thx
> dan richman

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Thursday, October 15, 2015 8:24 PM
To: Krieger, Paul (USANYS)
Cc: Loughnane, Joan (USANYS)
Subject: RE: Roundtable at Columbia

b5 Per EOUSA
b6 -1 and Per EOUSA
b7C -1

Right on both counts. [REDACTED]

[REDACTED] If this is productive there will be more such conversations that I'd love you to join. In the meantime, [REDACTED] from the NYO will be reaching to you to make sure we capture problems that occur in your nonbureau cases.

Meanwhile, we are watching what Apple will do in the case with [REDACTED]

From: Krieger, Paul (USANYS) [Paul.Krieger@usdoj.gov]
Sent: Thursday, October 15, 2015 6:41 PM
To: Richman, Daniel C. (DO) (OGA)
Cc: Loughnane, Joan (USANYS)
Subject: Roundtable at Columbia

Dan -

Hope all is well. We just wanted to touch base on the roundtable tomorrow. When we spoke about it at last week's meeting at FBI NY, my impression was that the roundtable wasn't going to be open to the public. Is that right? [REDACTED]

[REDACTED] If your thinking on that has changed, let us know.

b5 Per EOUSA

Thanks Dan. Speak to you soon.

Best,
Paul

b6 -1,2,5
b7C -1,2,5
b7D -1
b7E -3

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

From: Richman, Daniel C. (DO) (OGA) [mailto:[REDACTED]]
Sent: Friday, October 09, 2015 11:01 AM
To: Burrell, James C. (OTD) (FBI) [REDACTED] (DO) (FBI); Oconnell, Sasha C. (DO) (FBI); Baker, James A. (OGC) (FBI) [REDACTED] (DO) (FBI) [REDACTED] (ODAG) (JMD); [REDACTED] (CRM); Krieger, Paul (USANYS); Loughnane, Joan (USANYS)
Subject: DANY going dark white paper

Dear All -- Attached, courtesy of Ben Rosenberg at DANY, [REDACTED]

[REDACTED] Ben has authorized me to share it within the DOJ family but on condition that it be kept "confidential." I'm confident that Ben would welcome constructive criticism, either before or after the 10/16 roundtable (which he'll be attending).
thx

dan richman

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Monday, October 19, 2015 1:47 PM
To: Oconnell, Sasha C. (DO) (FBI)
Subject: RE: EDNY

Makes sense. As long as Kiran is coordinating from the DOJ end. Want to make sure that EDNY treats this as an important test case, because I'll bet Apple is _____

—
From: Oconnell, Sasha C. (DO) (FBI)
Sent: Monday, October 19, 2015 1:35 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: EDNY

Well and we are kind of out of it now. DEA case and all. Should make for interesting testimony this week though!

--

----- Original message -----

From: "Richman, Daniel C. (DO) (OGA)" [REDACTED]
Date: 10/19/2015 1:33 PM (GMT-05:00)
To: "Oconnell, Sasha C. (DO) (FBI)" [REDACTED]
Subject: RE: EDNY

b7E -3

excellent. I'm happy to help, but suspect there are 100 cooks already at work

—
From: Oconnell, Sasha C. (DO) (FBI)
Sent: Monday, October 19, 2015 1:21 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: EDNY

DOJ has decided to litigate. Should be public later today....

--

Oconnell, Sasha C. (DO) (FBI)

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Monday, October 19, 2015 1:53 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: EDNY

10 4 absolutely. They are all over it, DAG personally involved, Kiran heavily involved etc. Should be interesting.

--

----- Original message -----

From: "Richman, Daniel C. (DO) (OGA)" [REDACTED]
Date: 10/19/2015 1:48 PM (GMT-05:00)
To: "Oconnell, Sasha C. (DO) (FBI)" [REDACTED]
Subject: RE: EDNY

b7E -3

Makes sense. As long as Kiran is coordinating from the DOJ end. Want to make sure that EDNY treats this as an important test case, because I'll bet Apple is

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Monday, October 19, 2015 1:35 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: EDNY

Well and we are kind of out of it now. DEA case and all. Should make for interesting testimony this week though!

--

----- Original message -----

From: "Richman, Daniel C. (DO) (OGA)" [REDACTED]
Date: 10/19/2015 1:33 PM (GMT-05:00)
To: "Oconnell, Sasha C. (DO) (FBI)" [REDACTED]
Subject: RE: EDNY

b7E -3

excellent. I'm happy to help, but suspect there are 100 cooks already at work

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Monday, October 19, 2015 1:21 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: EDNY

DOJ has decided to litigate. Should be public later today....

--

Raj, Kiran (ODAG)

From: Raj, Kiran (ODAG)
Sent: Wednesday, October 21, 2015 4:05 PM
To: Richman, Daniel C. (DO) (OGA); Oconnell, Sasha C. (DO) (FBI)
Cc: Burrell, James C. (OTD) (FBI); [REDACTED] (DO) (FBI)
Subject: RE:

b6 -1
b7C -1

Quick question for the group: Is it our normal practice to review and provide edits to state & local whitepapers? I assume it is, but wanted to double check with folks who know more about how we deal with state & local LE. Thanks!

Kiran

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

From: Richman, Daniel C. (DO) (OGA) [mailto:[REDACTED]]
Sent: Tuesday, October 20, 2015 12:06 PM
To: Oconnell, Sasha C. (DO) (FBI)
Cc: Burrell, James C. (OTD) (FBI); Raj, Kiran (ODAG); [REDACTED] (DO) (FBI)
Subject: RE:

b6 -1
b7C -1

In the short-term, could all of you -- and particularly Jim B, since my personal tech expert -- look at the DANY white paper? Tho there's no need to coordinate policy moves with them, I think we owe them help correcting tech/law mistakes if we find them. Their law seems fine to me, but my systems ignorance prevents me from saying more authoratatively thx d _____

From: Oconnell, Sasha C. (DO) (FBI) Sent: Tuesday, October 20, 2015 9:42 AM To:

Richman, Daniel C. (DO) (OGA) Cc: Burrell, James C. (OTD) (FBI); Raj, Kiran (ODAG) (JMD); [REDACTED]
[REDACTED] (DO) (FBI) Subject: RE:

b6 -1,2
b7C -1,2

Thanks Dan, sorry for the delay. Responses below. In re-reading this/writing this I think we should follow up with Dean and [REDACTED] in short order to see if we can help get the data organization/transparency piece off the ground...

From: Richman, Daniel C. (DO) (OGA)
Sent: Friday, October 16, 2015 4:19 PM

To: Baker, James A. (OGC) (FBI); Burrell, James C. (OTD) (FBI); Oconnell, Sasha C. (DO) (FBI); Raj, Kiran (ODAG) (JMD); [REDACTED] (DO) (FBI)
Subject:

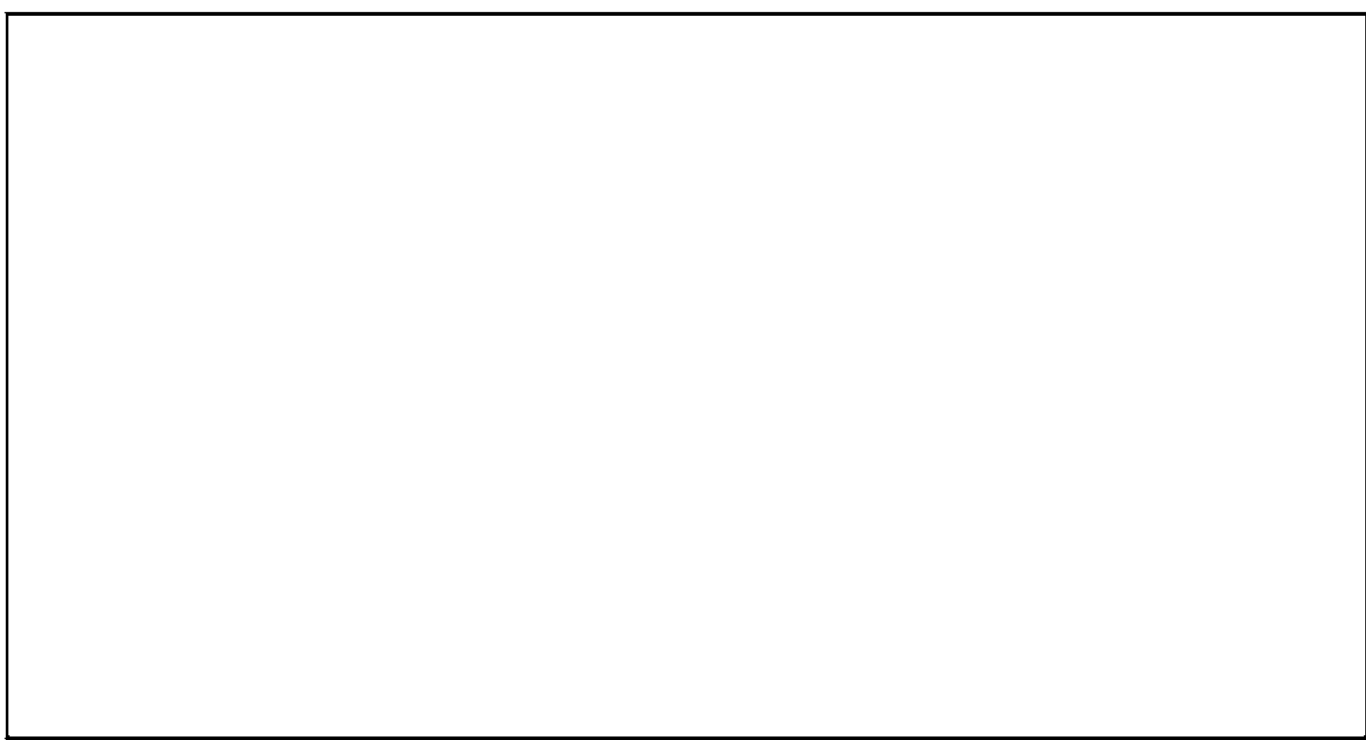
b6 -1
b7C -1

Thank you all for making the roundtable a big step forward in improved discourse on the GD issue. Here are a few initial reflections that I have in my Bureau capacity:

[REDACTED]

b5 -1

FBI 18-CV-1833-4660



I will keep thinking about today. In the meantime, it was lovely to see you all. And my Columbia colleagues look forward to hosting more such events.

dan r

From: Richman, Daniel C. (DO) (OGA)
Sent: Wednesday, October 21, 2015 4:14 PM
To: Raj, Kiran (ODAG); Oconnell, Sasha C. (DO) (FBI)
Cc: Burrell, James C. (OTD) (FBI); [REDACTED] (DO) (FBI)
Subject: RE:

I differ to you on political and bureaucratic sensitivities. But, just to clarify, I think it serves neither DANY's purpose nor our own to seek true harmonization of views on the policy or even the legal issues. What I suspect DANY is looking for, at least at this point, is that we help them catch factual misstatements, particularly on the tech side.

b6 -1
b7C -1

Quick question for the group: Is it our normal practice to review and provide edits to state & local whitepapers? I assume it is, but wanted to double check with folks who know more about how we deal with state & local LE. Thanks!

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

b6 -1
b7C -1
b7E -3

In the short-term, could all of you -- and particularly Jim B, since my personal tech expert -- look at the DANY white paper? Tho there's no need to coordinate policy moves with them, I think we owe them help correcting tech/law mistakes if we find them. Their law seems fine to me, but my systems ignorance prevents me from saying more authoratatively thx d

b6 -1,2
b7C -1,2

Thanks Dan, sorry for the delay. Responses below. In re-reading this/writing this I think we should follow up with Dean and [REDACTED] in short order to see if we can help get the data organization/transparency piece off the ground...

From: Richman, Daniel C. (DO) (OGA)

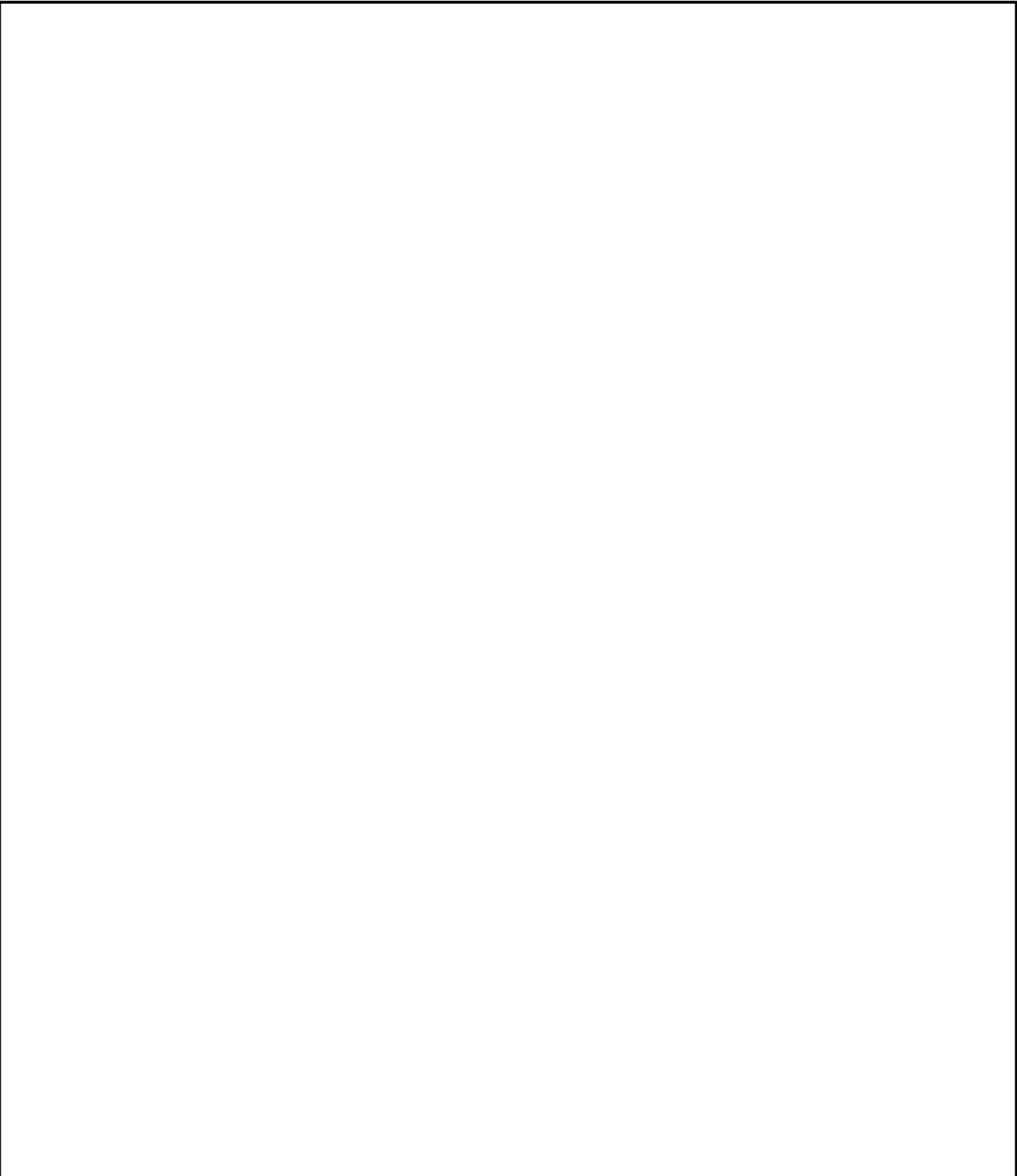
Sent: Friday, October 16, 2015 4:19 PM

To: Baker, James A. (OGC) (FBI); Burrell, James C. (OTD) (FBI); Oconnell, Sasha C. (DO) (FBI); Raj, Kiran (ODAG) (JMD); [REDACTED] (DO) (FBI)

Subject:

b6 -1
b7C -1

Thank you all for making the roundtable a big step forward in improved discourse on the GD issue. Here are a few initial reflections that I have in my Bureau capacity:



b5 -1
b6 -2
b7C -2

I will keep thinking about today. In the meantime, it was lovely to see you all. And my Columbia colleagues look forward to hosting more such events.
dan r

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Monday, October 26, 2015 4:40 PM
To: Loughnane, Joan (USANYS)
Subject: RE:

b5 Per EOUSA
b6 -1
b7C -1

Hi again - Lovely to see you. I'm glad to hear Diego has been asking you about GD problems. But just to be clear, we'd love to hear about those problems in non-Bu cases as well as Bu cases. [REDACTED] from the NYO may well have already made this ask.) The Bu machine (i've been promised) is prodding its offices for data. And I know [REDACTED]

[REDACTED] Luckily you're in the center of everything thanks so much for your help dan richman [REDACTED]

From: Loughnane, Joan (USANYS) [Joan.Loughnane@usdoj.gov]
Sent: Tuesday, October 06, 2015 10:46 PM
To: Krieger, Paul (USANYS)
Cc: Richman, Daniel C. (DO) (OGA); Oconnell, Sasha C. (DO) (FBI)
Subject: Re:

Thanks, Paul. And hi, Dan. Great to see you in your new capacity at FBI. Looking forward to hearing more about your round table. Hope you're well, Joan

> On Oct 6, 2015, at 9:50 PM, Krieger, Paul (USANYS) <PKrieger@usa.doj.gov> wrote:

>
> Dan - It was great seeing you as well. And Sasha, it was nice meeting you. Please do keep me/SDNY in the loop going forward. We'd like to help/participate in these important efforts. I'm also looping in Joan Loughnane, who is chief counsel to Preet.

> Best,
> Paul

>
>
>
>
>

>> On Oct 6, 2015, at 8:49 PM, Richman, Daniel C. (DO) (OGA) [REDACTED] wrote:

b7E -3

>>
>> Hi Paul - great seeing you again. And let's definitely keep in touch on the GDark issue. Certainly if this "roundtable" idea I'm beta testing works out, I want to make sure the SDNY gets a piece of the action (to explain how its work is/maybe affected). Sasha O'C (cc'd here) is of course the point person.
>> say hi to Preet et al
>> best
>> dan richman

Raj, Kiran (ODAG)

From: Raj, Kiran (ODAG)
Sent: Wednesday, November 18, 2015 7:39 PM
To: Richman, Daniel C. (DO) (OGA); Oconnell, Sasha C. (DO) (FBI)
Subject: RE: GD EDNY and Apple

Hi Dan -

I spoke with Sasha today, and our current plan is to get together to talk through next steps on Friday morning. Are you available at 10 a.m.? It would be great to get your input.

Kiran

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

From: Richman, Daniel C. (DO) (OGA) [mailto:]
Sent: Tuesday, November 17, 2015 3:42 PM
To: Raj, Kiran (ODAG); Oconnell, Sasha C. (DO) (FBI)
Subject: GD EDNY and Apple

b6 -5
b7C -5
b7E -3

Hi Kiran - Sasha (cc'd here) says you're [] So I'm sorry about that. For when you return: I just wanted to make sure that DOJ takes full advantage of the coincidence of the Apple EDNY papers saying "We can open iOS7 but don't want to" and the emerging story in Paris (which may involve an iPhone). Even before the EDNY litigation plays out and regardless of the precise facts that will emerge from Paris, Apple's tone-deafness can really be used to our advantage in public statements. And I'm hoping you and your peeps are focusing on that.

thx

dan richman

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Wednesday, November 18, 2015 9:51 PM
To: Raj, Kiran (ODAG); Oconnell, Sasha C. (DO) (FBI)
Subject: RE: GD EDNY and Apple

b6 -4
b7C -4

I have [REDACTED] at 10 on Friday but can talk or email chat most of the day thereafter.

From: Raj, Kiran (ODAG) [Kiran.Raj@usdoj.gov]
Sent: Wednesday, November 18, 2015 7:38 PM
To: Richman, Daniel C. (DO) (OGA); Oconnell, Sasha C. (DO) (FBI)
Subject: RE: GD EDNY and Apple

Hi Dan -

I spoke with Sasha today, and our current plan is to get together to talk through next steps on Friday morning. Are you available at 10 a.m.? It would be great to get your input.

Kiran

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

From: Richman, Daniel C. (DO) (OGA) [mailto:[REDACTED]]
Sent: Tuesday, November 17, 2015 3:42 PM
To: Raj, Kiran (ODAG); Oconnell, Sasha C. (DO) (FBI)
Subject: GD EDNY and Apple

b6 -5
b7C -5

Hi Kiran - Sasha (cc'd here) says you're [REDACTED] So I'm sorry about that. For when you return: I just wanted to make sure that DOJ takes full advantage of the coincidence of the Apple EDNY papers saying "We can open iOS7 but don't want to" and the emerging story in Paris (which may involve an iPhone). Even before the EDNY litigation plays out and regardless of the precise facts that will emerge from Paris, Apple's tone-deafness can really be used to our advantage in public statements. And I'm hoping you and your peeps are focusing on that.

thx

dan richman

Raj, Kiran (ODAG)

From: Raj, Kiran (ODAG)
Sent: Wednesday, November 18, 2015 7:42 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE:

Thanks, Dan -

I think I may have mentioned this to you before, but going to trial with [REDACTED] was a treat and just plain fun.

b6 -2
b7C -2

Kiran

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

From: Richman, Daniel C. (DO) (OGA) [mailto:[REDACTED]]
Sent: Wednesday, November 18, 2015 7:20 PM
To: Raj, Kiran (ODAG)
Subject:

b6 -2
b7C -2
b7E -3

I saw [REDACTED] at my General Crimes unit reunion last night. He remembers you fondly & sends his best d

Oconnell, Sasha C. (DO) (FBI)

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Friday, November 20, 2015 3:59 PM
To: Richman, Daniel C. (DO) (OGA); Raj, Kiran (ODAG) (JMD)
Subject: RE: David Sanger & willful misunderstanding

Unfortunately I don't think we are going to get help there. Below please find

b5 Per NSC

b5 Per NSC



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

From: Richman, Daniel C. (DO) (OGA)

Sent: Friday, November 20, 2015 3:57 PM

To: Oconnell, Sasha C. (DO) (FBI); Raj, Kiran (ODAG) (JMD)

Subject: David Sanger & willful misunderstanding

b5 Per NSC

Sorry I missed your powwow. Even as I like the news of real engagement from the tech folks, David Sanger's constant incorrect statement about what the PC may itself be a impediment and likely reflects an incorrect understanding on the part of some industry people and "experts" that needs correcting. What about resurrecting Kiran's idea [REDACTED] and -- for extra points -- coming write out and saying that Sanger's reporting is wrong??

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Friday, November 20, 2015 4:10 PM
To: Oconnell, Sasha C. (DO) (FBI); Raj, Kiran (ODAG) (JMD)
Subject: RE: David Sanger & willful misunderstanding

of course tech firms are also hearing the growing political noise.

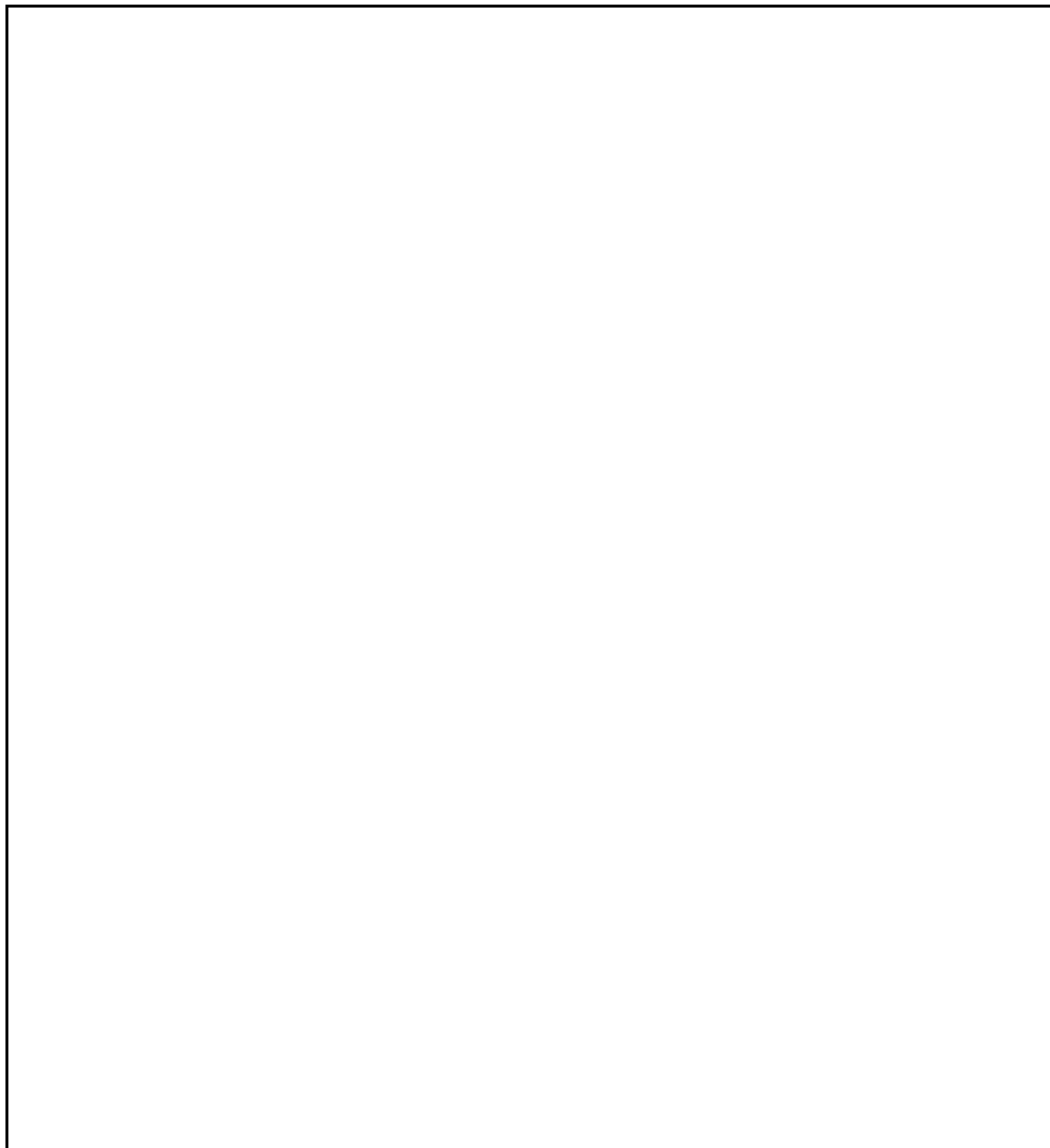
<http://www.wired.com/2015/11/after-paris-encryption-will-be-a-key-issue-in-the-2016-race/>

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Friday, November 20, 2015 3:58 PM
To: Richman, Daniel C. (DO) (OGA); Raj, Kiran (ODAG) (JMD)
Subject: RE: David Sanger & willful misunderstanding

Unfortunately I don't think we are going to get help there. Below please find

b5 Per NSC

b5 Per NSC



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

From: Richman, Daniel C. (DO) (OGA)

Sent: Friday, November 20, 2015 3:57 PM

To: Oconnell, Sasha C. (DO) (FBI); Raj, Kiran (ODAG) (JMD)

Subject: David Sanger & willful misunderstanding

Sorry I missed your powwow. Even as I like the news of real engagement from the tech folks, David

Sanger's constant incorrect statement about what the PC may itself be a impediment and likely reflects an incorrect understanding on the part of some industry people and "experts" that needs correcting.

What about resurrecting Kiran's idea [REDACTED] and --

for extra points -- coming write out and saying that Sanger's reporting is wrong??

b5 Per NSC

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Friday, November 20, 2015 4:07 PM
To: Oconnell, Sasha C. (DO) (FBI); Raj, Kiran (ODAG) (JMD)
Subject: RE: David Sanger & willful misunderstanding

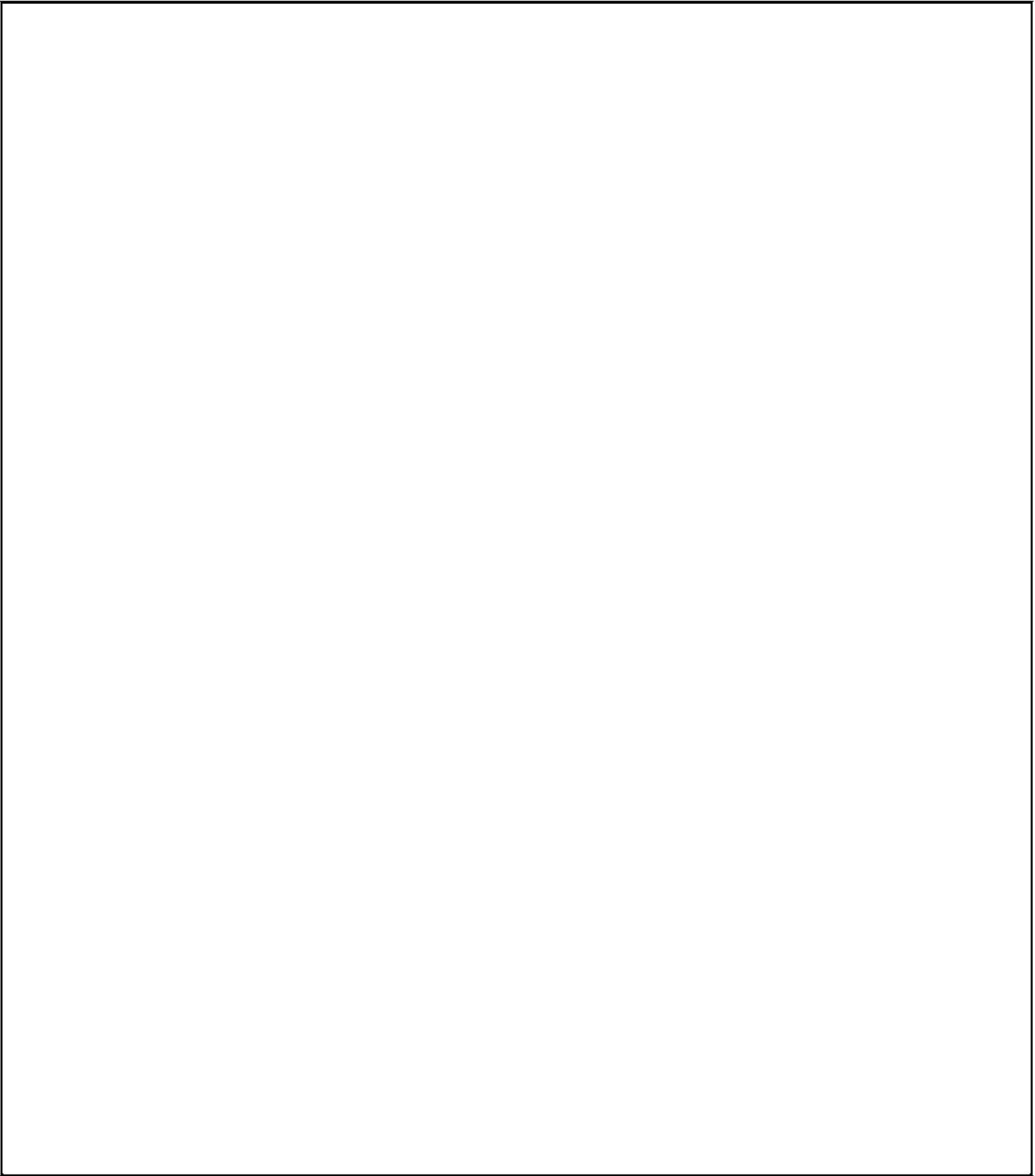
none at all! And I'm going to assume all the refs to "working with companies" are to us -- and not to any other parts of the USG, all of which will sit by acting bemused at the bu's temerity. Such is life in the Big City i guess

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Friday, November 20, 2015 3:58 PM
To: Richman, Daniel C. (DO) (OGA); Raj, Kiran (ODAG) (JMD)
Subject: RE: David Sanger & willful misunderstanding

Unfortunately I don't think we are going to get help there. Below please find

b5 Per NSC

b5 Per NSC



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

From: Richman, Daniel C. (DO) (OGA)

Sent: Friday, November 20, 2015 3:57 PM

To: Oconnell, Sasha C. (DO) (FBI); Raj, Kiran (ODAG) (JMD)

Subject: David Sanger & willful misunderstanding

Sorry I missed your powwow. Even as I like the news of real engagement from the tech folks, David Sanger's constant incorrect statement about what the PC may itself be a impediment and likely reflects an incorrect understanding on the part of some industry people and "experts" that needs correcting. What about resurrecting Kiran's idea [REDACTED] and -- for extra points -- coming write out and saying that Sanger's reporting is wrong??

b5 Per NSC

Oconnell, Sasha C. (DO) (FBI)

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Monday, November 30, 2015 12:30 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: Input requested: Encryption Policy Dinner this Thurs (ITI & Facebook GC)

Awesome! Let me just confirm with Amy and Jim. Obviously some complexities given the AT case... will have a status on that later today. Stand by for confirmation then I will loop you in with Dean. I think this could be perfect!

----- Original message -----

From: "Richman, Daniel C. (DO) (OGA)" [REDACTED]
Date: 11/30/2015 12:03 PM (GMT-05:00)
To: "Oconnell, Sasha C. (DO) (FBI)" [REDACTED] "Hess, Amy S. (DO) (FBI)" [REDACTED] "Baker, James A. (OGC) (FBI)" [REDACTED]
Cc: "Raj, Kiran (ODAG) (JMD)" <Kiran.Raj@usdoj.gov>, [REDACTED] (DO) (FBI)" [REDACTED]
Subject: RE: Input requested: Encryption Policy Dinner this Thurs (ITI & Facebook GC)

b6 -1
b7C -1
b7E -3

I could do this. Mike C & I go way back, and tho I never met Dempsey, he reached out to me on a CALEA project in the early 90s (a million years ago).
dan r

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Monday, November 30, 2015 10:27 AM
To: Hess, Amy S. (DO) (FBI); Baker, James A. (OGC) (FBI)
Cc: Richman, Daniel C. (DO) (OGA); Raj, Kiran (ODAG) (JMD); [REDACTED] (DO) (FBI)
Subject: Input requested: Encryption Policy Dinner this Thurs (ITI & Facebook GC)

b6 -1
b7C -1

Amy/Jim,
I just spoke with Dean Garfield from ITI. At the request of the Facebook GC he is putting together a dinner this Thursday night here in DC to have a "constructive discussion" about encryption. Dean asked if we have attendee suggestions to include DOJ/FBI. Sample of invitees include:

Stu Baker
Mike Chertoff (confirmed)
Alan Davidson (formerly Google now commerce)

[REDACTED]
Jim Dempsey
Etc.

b6 -2
b7C -2

In talking with Kiran (who is not available Thursday to go) our thinking is on the one hand we want to continue discussions and open lines of communication while on the other there are pending complexities and the Director's position at our last mtg to consider.

To that end I would like to propose we ask Dan (cc'd here but I have not yet spoken with him!) If it would be possible for him to be in DC this Thursday to attend on our behalf. I throw that out there and look forward to your input/suggestions, I did tell Dean I would get back with him this afternoon. To that end I am off today but could call to discuss if that would be easier.

Thank you!!

FBI 18-CV-1833-4938

Sasha

--

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Monday, November 30, 2015 4:06 PM
To: Raj, Kiran (ODAG) (JMD); Oconnell, Sasha C. (DO) (FBI)
Subject: atlanta litigation

Hi Kiran - Hope you had a lovely Thanksgiving. Would it be possible for you to send me stuff -- public filings and/or non-public on the comm access litigation in Atlanta (was it involving WhatsApp?) so I can act a bit informed in your absence on Thurs? If my question sounds vague (it is), it's because I'm not sure what I'm talking about.

thx
dan r

Raj, Kiran (ODAG)

From: Raj, Kiran (ODAG)
Sent: Monday, November 30, 2015 4:13 PM
To: Richman, Daniel C. (DO) (OGA); Oconnell, Sasha C. (DO) (FBI)
Subject: RE: atlanta litigation

Dan -

Let's chat when you have a moment. What is the best number to use to reach you?

Kiran

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

From: Richman, Daniel C. (DO) (OGA) [mailto:]
Sent: Monday, November 30, 2015 4:06 PM
To: Raj, Kiran (ODAG); Oconnell, Sasha C. (DO) (FBI)
Subject: atlanta litigation

b7E -3

Hi Kiran - Hope you had a lovely Thanksgiving. Would it be possible for you to send me stuff -- public filings and/or non-public on the comm access litigation in Atlanta (was it involving WhatsApp?) so I can act a bit informed in your absence on Thurs? If my question sounds vague (it is), it's because I'm not sure what I'm talking about.

thx

dan r

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Monday, November 30, 2015 4:52 PM
To: Raj, Kiran (ODAG)
Subject: RE: atlanta litigation

i have to leave early today -- around 5:30. I'll be in my office til then & will be available by cell [REDACTED]
[REDACTED] - most of tomorrow thx
d

b6 -4
b7C -4

From: Raj, Kiran (ODAG) [Kiran.Raj@usdoj.gov]
Sent: Monday, November 30, 2015 4:12 PM
To: Richman, Daniel C. (DO) (OGA); Oconnell, Sasha C. (DO) (FBI)
Subject: RE: atlanta litigation

Dan -

Let's chat when you have a moment. What is the best number to use to reach you?

Kiran

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

From: Richman, Daniel C. (DO) (OGA) [mailto:[REDACTED]]
Sent: Monday, November 30, 2015 4:06 PM
To: Raj, Kiran (ODAG); Oconnell, Sasha C. (DO) (FBI)
Subject: atlanta litigation

b7E -3

Hi Kiran - Hope you had a lovely Thanksgiving. Would it be possible for you to send me stuff -- public filings and/or non-public on the comm access litigation in Atlanta (was it involving WhatsApp?) so I can act a bit informed in your absence on Thurs? If my question sounds vague (it is), it's because I'm not sure what I'm talking about.

thx
dan r

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Monday, November 30, 2015 4:25 PM
To: Raj, Kiran (ODAG); Oconnell, Sasha C. (DO) (FBI)
Subject: RE: atlanta litigation

office [REDACTED]

b6 -4
b7C -4

From: Raj, Kiran (ODAG) [Kiran.Raj@usdoj.gov]
Sent: Monday, November 30, 2015 4:12 PM
To: Richman, Daniel C. (DO) (OGA); Oconnell, Sasha C. (DO) (FBI)
Subject: RE: atlanta litigation

Dan -

Let's chat when you have a moment. What is the best number to use to reach you?

Kiran

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

From: Richman, Daniel C. (DO) (OGA) [mailto:[REDACTED]]
Sent: Monday, November 30, 2015 4:06 PM
To: Raj, Kiran (ODAG); Oconnell, Sasha C. (DO) (FBI)
Subject: atlanta litigation

b7E -3

Hi Kiran - Hope you had a lovely Thanksgiving. Would it be possible for you to send me stuff -- public filings and/or non-public on the comm access litigation in Atlanta (was it involving WhatsApp?) so I can act a bit informed in your absence on Thurs? If my question sounds vague (it is), it's because I'm not sure what I'm talking about.

thx

dan r

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Monday, November 30, 2015 5:10 PM
To: Raj, Kiran (ODAG)
Subject: RE: atlanta litigation

sounds good (on cell)
d

From: Raj, Kiran (ODAG) [Kiran.Raj@usdoj.gov]
Sent: Monday, November 30, 2015 5:08 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: Re: atlanta litigation

I am in meetings until 630 today. Let's catch up tomorrow. Does 10 am work for you?

Kiran

Sent from my iPhone

> On Nov 30, 2015, at 4:53 PM, Richman, Daniel C. (DO) (OGA) [REDACTED] wrote:

>

> i have to leave early today -- around 5:30. I'll be in my office til then & will be available by cell - [REDACTED]
[REDACTED] - most of tomorrow > thx > d > [REDACTED] > From: Raj,
Kiran (ODAG) [Kiran.Raj@usdoj.gov] > Sent: Monday, November 30, 2015 4:12 PM > To: Richman,
Daniel C. (DO) (OGA); Oconnell, Sasha C. (DO) (FBI) > Subject: RE: atlanta litigation

>

> Dan -

>

> Let's chat when you have a moment. What is the best number to use to reach you?

>

> Kiran

>

> -----Original Message-----

> From: Richman, Daniel C. (DO) (OGA) [mailto:[REDACTED]]

> Sent: Monday, November 30, 2015 4:06 PM

> To: Raj, Kiran (ODAG); Oconnell, Sasha C. (DO) (FBI)

> Subject: atlanta litigation

>

> Hi Kiran - Hope you had a lovely Thanksgiving. Would it be possible for you to send me stuff -- public filings and/or non-public on the comm access litigation in Atlanta (was it involving WhatsApp?) so I can act a bit informed in your absence on Thurs? If my question sounds vague (it is), it's because I'm not sure what I'm talking about.

> thx

> dan r

b6 -4
b7C -4
b7E -3

b7E -3

Raj, Kiran (ODAG)

From: Raj, Kiran (ODAG)
Sent: Monday, November 30, 2015 5:09 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: Re: atlanta litigation

I am in meetings until 630 today. Let's catch up tomorrow. Does 10 am work for you?

Kiran

Sent from my iPhone

> On Nov 30, 2015, at 4:53 PM, Richman, Daniel C. (DO) (OGA) [redacted] wrote:

>

> i have to leave early today -- around 5:30. I'll be in my office til then & will be available by cell - [redacted]

[redacted] - most of tomorrow > thx > d > _____ > From: Raj,

Kiran (ODAG) [Kiran.Raj@usdoj.gov] > Sent: Monday, November 30, 2015 4:12 PM > To: Richman, Daniel C. (DO) (OGA); Oconnell, Sasha C. (DO) (FBI) > Subject: RE: atlanta litigation

>

> Dan -

>

> Let's chat when you have a moment. What is the best number to use to reach you?

>

> Kiran

>

> -----Original Message-----

> From: Richman, Daniel C. (DO) (OGA) [mailto:[redacted]]

> Sent: Monday, November 30, 2015 4:06 PM

> To: Raj, Kiran (ODAG); Oconnell, Sasha C. (DO) (FBI)

> Subject: atlanta litigation

>

> Hi Kiran - Hope you had a lovely Thanksgiving. Would it be possible for you to send me stuff -- public filings and/or non-public on the comm access litigation in Atlanta (was it involving WhatsApp?) so I can act a bit informed in your absence on Thurs? If my question sounds vague (it is), it's because I'm not sure what I'm talking about.

> thx

> dan r

b6 -4
b7C -4
b7E -3

b7E -3

Oconnell, Sasha C. (DO) (FBI)

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Wednesday, December 02, 2015 3:05 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE:

And I think an unemployed PhD student. Not that there is anything wrong with that!

[REDACTED] Will let you know!!

b5 Per DOJ/OIP

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

From: Richman, Daniel C. (DO) (OGA)
Sent: Wednesday, December 02, 2015 2:41 PM
To: Oconnell, Sasha C. (DO) (FBI)
Subject: RE:

wow - actually thoughtful. But he's Canadian :) _____ **From:**
Oconnell, Sasha C. (DO) (FBI) **Sent:** Wednesday, December 02, 2015 1:54 PM **To:** Richman, Daniel C.
(DO) (OGA) **Subject:**

<http://www.csmonitor.com/World/Passcode/Passcode-Voices/2015/1202/Opinion-It-s-time-to-rethink-polarizing-encryption-debate>

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Wednesday, December 02, 2015 3:22 PM
To: Oconnell, Sasha C. (DO) (FBI)
Subject: RE:

Kiran told me he'd give me something prepared for that mtg with the status of current efforts, platform by platform. But anything I could read from this coordination mtg would be really helpful.
thx

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Wednesday, December 02, 2015 3:04 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE:

And I think an unemployed PhD student. Not that there is anything wrong with that!

[REDACTED] Will let you know!!

b5 Per DOJ/OIP

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

From: Richman, Daniel C. (DO) (OGA)
Sent: Wednesday, December 02, 2015 2:41 PM
To: Oconnell, Sasha C. (DO) (FBI)
Subject: RE:

wow - actually thoughtful. But he's Canadian :) _____ **From:**
Oconnell, Sasha C. (DO) (FBI) **Sent:** Wednesday, December 02, 2015 1:54 PM **To:** Richman, Daniel C.
(DO) (OGA) **Subject:**

<http://www.csmonitor.com/World/Passcode/Passcode-Voices/2015/1202/Opinion-It-s-time-to-rethink-polarizing-encryption-debate>

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Wednesday, December 02, 2015 4:06 PM
To: Oconnell, Sasha C. (DO) (FBI)
Subject: RE: AG Brief

thanks -- look forward to hearing fall-out from this

Also reminds me of something else on my Dir testimony wishlist: Unless the litigation maneuvering you discuss at this meeting counsels otherwise, I suggest [REDACTED]

b5 -1

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Wednesday, December 02, 2015 3:43 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: Fwd: AG Brief

--

----- Original message -----

From: "Raj, Kiran (ODAG)" <Kiran.Raj@usdoj.gov>

Date: 12/02/2015 1:28 PM (GMT-05:00)

b6 Per DOJ/CRM

b7C Per DOJ/CRM

To: "McCord, Mary (NSD) (JMD)" <Mary.McCord@usdoj.gov>, "Bitkower, David (CRM)"

[REDACTED]@usdoj.gov>, "OBrien, Paul (CRM)" [REDACTED]@usdoj.gov>, "Downing, Richard

(CRM)" [REDACTED]@usdoj.gov>, "Lan, Iris (ODAG) (JMD)" <Iris.Lan3@usdoj.gov>, "Gauhar,

Tashina (ODAG) (JMD)" <Tashina.Gauhar2@usdoj.gov>, "Evans, Stuart (NSD) (JMD)"

<Stuart.Evans@usdoj.gov>, "Wiegmann, Brad (NSD) (JMD)" <Brad.Wiegmann@usdoj.gov>, "Swartz,

Bruce (CRM)" [REDACTED]@usdoj.gov>, "Carlin, John (NSD) (JMD)"

<John.Carlin@usdoj.gov>, "Caldwell, Leslie R (CRM)" [REDACTED]@usdoj.gov>, "Cheung, Denise

(OAG) (JMD)" <Denise.Cheung2@usdoj.gov>, "Oconnell, Sasha C. (DO) (FBI)" [REDACTED]

[REDACTED] (DO) (FBI)" [REDACTED]

Cc: "Axelrod, Matthew (ODAG) (JMD)" <Matthew.Axelrod@usdoj.gov>

Subject: RE: AG Brief

b6 -1

b7C -1

b7E -3

All,

Here is an updated version of the slide based on my conversation with Mary and David. Please let me know if you have any comments or edits.

Best,

Kiran

FBI 18-CV-1833-5052

From: McCord, Mary (NSD)
Sent: Wednesday, December 02, 2015 1:00 PM
To: Raj, Kiran (ODAG); Bitkower, David; OBrien, Paul; Downing, Richard; Lan, Iris (ODAG); Gauhar, Tashina (ODAG); Evans, Stuart (NSD); Wiegmann, Brad (NSD); Swartz, Bruce; Carlin, John (NSD); Caldwell, Leslie R; Cheung, Denise (OAG); Oconnell, Sasha C. (DO) (FBI); [REDACTED] (DO) (FBI)
Cc: Axelrod, Matthew (ODAG)
Subject: RE: AG Brief

b6 -1
b7C -1

Kiran,
Just tried to reach you and got voicemail. Please give me a call. 4-6346.
Thanks,
Mary

From: Raj, Kiran (ODAG)
Sent: Wednesday, December 02, 2015 12:20 PM
To: Bitkower, David; OBrien, Paul; Downing, Richard; Lan, Iris (ODAG); Gauhar, Tashina (ODAG); Evans, Stuart (NSD); Wiegmann, Brad (NSD); Swartz, Bruce; Carlin, John (NSD); Caldwell, Leslie R; Cheung, Denise (OAG); Oconnell, Sasha C. (DO) (FBI); McCord, Mary (NSD); [REDACTED] (DO) (FBI)
Cc: Axelrod, Matthew (ODAG)
Subject: AG Brief

b6 -1
b7C -1

DRAFT//PRE-DECISIONAL

All,

Per our discussion, here is the current draft PPT that we plan to provide to the AG for the meeting today. (Note: The company name is specifically excluded from the slide). Please let me know if you have any edits or comments.

Thanks very much,

Kiran

<< File: GD 2 0 Draft Options Slide 12-2-15.pptx >> Kiran Raj Senior Counsel to the Deputy Attorney General 950 Pennsylvania Avenue, NW Washington, D.C. 20530 Tel: (202) 305-9886

Oconnell, Sasha C. (DO) (FBI)

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Wednesday, December 02, 2015 3:43 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: Fwd: AG Brief
Attachments: GD 2 0 Draft Options Slide 12-2-15.pptx

----- Original message -----

From: "Raj, Kiran (ODAG)" <Kiran.Raj@usdoj.gov>

Date: 12/02/2015 1:28 PM (GMT-05:00)

To: "McCord, Mary (NSD) (JMD)" <Mary.McCord@usdoj.gov>, "Bitkower, David (CRM)"

[REDACTED]@usdoj.gov>, "OBrien, Paul (CRM)" [REDACTED]@usdoj.gov>, "Downing, Richard (CRM)" [REDACTED]@usdoj.gov>, "Lan, Iris (ODAG) (JMD)" <Iris.Lan3@usdoj.gov>, "Gauhar, Tashina (ODAG) (JMD)" <Tashina.Gauhar2@usdoj.gov>, "Evans, Stuart (NSD) (JMD)"

<Stuart.Evans@usdoj.gov>, "Wiegmann, Brad (NSD) (JMD)" <Brad.Wiegmann@usdoj.gov>, "Swartz, Bruce (CRM)" [REDACTED]@usdoj.gov>, "Carlin, John (NSD) (JMD)"

<John.Carlin@usdoj.gov>, "Caldwell, Leslie R (CRM)" [REDACTED]@usdoj.gov>, "Cheung, Denise (OAG) (JMD)" <Denise.Cheung2@usdoj.gov>, "Oconnell, Sasha C. (DO) (FBI)"

[REDACTED] (DO) (FBI)" [REDACTED]

Cc: "Axelrod, Matthew (ODAG) (JMD)" <Matthew.Axelrod@usdoj.gov>

Subject: RE: AG Brief

All,

Here is an updated version of the slide based on my conversation with Mary and David. Please let me know if you have any comments or edits.

Best,

Kiran

From: McCord, Mary (NSD)

Sent: Wednesday, December 02, 2015 1:00 PM

To: Raj, Kiran (ODAG); Bitkower, David; OBrien, Paul; Downing, Richard; Lan, Iris (ODAG); Gauhar, Tashina (ODAG); Evans, Stuart (NSD); Wiegmann, Brad (NSD); Swartz, Bruce; Carlin, John (NSD); Caldwell, Leslie R; Cheung, Denise (OAG); Oconnell, Sasha C. (DO) (FBI); [REDACTED] (DO) (FBI)

Cc: Axelrod, Matthew (ODAG)

Subject: RE: AG Brief

b6 -1
b7C -1

Kiran,

Just tried to reach you and got voicemail. Please give me a call. 4-6346.

FBI 18-CV-1833-5054

Thanks,
Mary

From: Raj, Kiran (ODAG)
Sent: Wednesday, December 02, 2015 12:20 PM
To: Bitkower, David; OBrien, Paul; Downing, Richard; Lan, Iris (ODAG); Gauhar, Tashina (ODAG); Evans, Stuart (NSD); Wiegmann, Brad (NSD); Swartz, Bruce; Carlin, John (NSD); Caldwell, Leslie R; Cheung, Denise (OAG); Oconnell, Sasha C. (DO) (FBI); McCord, Mary (NSD); [REDACTED] (DO) (FBI)
Cc: Axelrod, Matthew (ODAG)
Subject: AG Brief

b6 -1
b7C -1

DRAFT//PRE-DECISIONAL

All,

Per our discussion, here is the current draft PPT that we plan to provide to the AG for the meeting today. (Note: The company name is specifically excluded from the slide). Please let me know if you have any edits or comments.

Thanks very much,

Kiran
<< File: GD 2 0 Draft Options Slide 12-2-15.pptx >>
Kiran Raj
Senior Counsel to the Deputy Attorney General
950 Pennsylvania Avenue, NW
Washington, D.C. 20530
Tel: (202) 305-9886

Oconnell, Sasha C. (DO) (FBI)

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Tuesday, December 08, 2015 12:24 PM
To: Raj, Kiran (ODAG) (JMD); Richman, Daniel C. (DO) (OGA); [REDACTED] (DO) b6 -1
(FBI) b7C -1
Subject: RE:

Director just sent a note out with what he would "like" to say. Stand by will get it around for thoughts

----- Original message -----

From: "Raj, Kiran (ODAG)" <Kiran.Raj@usdoj.gov>
Date: 12/08/2015 12:16 PM (GMT-05:00)
To: "Richman, Daniel C. (DO) (OGA)" [REDACTED] (DO) (FBI)"
[REDACTED] "Oconnell, Sasha C. (DO) (FBI)" [REDACTED]
Subject: RE:

b6 -1
b7C -1
b7E -3

A few thoughts/comments in the attached for your consideration.

Kiran

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

From: Richman, Daniel C. (DO) (OGA) [mailto:[REDACTED]]
Sent: Tuesday, December 08, 2015 12:13 PM
To: [REDACTED] (DO) (FBI); Raj, Kiran (ODAG); Oconnell, Sasha C. (DO) (FBI)
Subject: RE:

b6 -1
b7C -1
b7E -3

I like it. [REDACTED]
[REDACTED]

b5 -1

[REDACTED]
From: [REDACTED] (DO) (FBI)
Sent: Tuesday, December 08, 2015 11:28 AM
To: Raj, Kiran (ODAG) (JMD); Richman, Daniel C. (DO) (OGA)
Subject:

b6 -1
b7C -1

Kiran, Dan-

Attached are Sasha's discussion points for her prep with the Director this afternoon in re: SJC hearing tomorrow. To ensure I can incorporate any feedback, please have any comments back to me by 1:30pm today.

Thanks,
[REDACTED]

FBI 18-CV-1833-5135

[Redacted]

Federal Bureau of Investigation
Office of National Policy

[Redacted]

b6 -1

b7C -1

b7E -3

Raj, Kiran (ODAG)

From: Raj, Kiran (ODAG)
Sent: Tuesday, December 08, 2015 12:16 PM
To: Richman, Daniel C. (DO) (OGA); [REDACTED] (DO) (FBI); Oconnell, Sasha C. (DO) (FBI)
Subject: RE:
Attachments: SJC_Sasha TPs_12082015 KSR Edits.docx

b6 -1
b7C -1

A few thoughts/comments in the attached for your consideration.

Kiran

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

From: Richman, Daniel C. (DO) (OGA) [mailto:[REDACTED]]
Sent: Tuesday, December 08, 2015 12:13 PM
To: [REDACTED] (DO) (FBI); Raj, Kiran (ODAG); Oconnell, Sasha C. (DO) (FBI)
Subject: RE:

b6 -1
b7C -1
b7E -3

I like it, [REDACTED]
[REDACTED]

b5 -1

From: [REDACTED] (DO) (FBI)
Sent: Tuesday, December 08, 2015 11:28 AM
To: Raj, Kiran (ODAG) (JMD); Richman, Daniel C. (DO) (OGA)
Subject:

b6 -1
b7C -1

Kiran, Dan-

Attached are Sasha's discussion points for her prep with the Director this afternoon in re: SJC hearing tomorrow. To ensure I can incorporate any feedback, please have any comments back to me by 1:30pm today.

Thanks,

[REDACTED]

[REDACTED]

Federal Bureau of Investigation

FBI 18-CV-1833-5137

Office of National Policy



b7E -3

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Tuesday, December 29, 2015 3:29 PM
To: Raj, Kiran (ODAG)
Cc: Oconnell, Sasha C. (DO) (FBI); [REDACTED] (DO) (FBI); Burrell, James C. (OTD) (FBI)
Subject: RE: Apple UK submission

b6 -1,2
b7C -1,2

interesting. I guess Apple's vision of privacy extends to its legislative submissions Just for kicks, I suggested to [REDACTED] that she query David O'Neil at Debevoise.

d

From: Raj, Kiran (ODAG) [Kiran.Raj@usdoj.gov]
Sent: Tuesday, December 29, 2015 3:22 PM
To: Richman, Daniel C. (DO) (OGA)
Cc: Oconnell, Sasha C. (DO) (FBI); [REDACTED] (DO) (FBI); Burrell, James C. (OTD) (FBI)
Subject: Re: Apple UK submission

b6 -1
b7C -1

I believe we are going to ask the UK Embassy for a copy. Our folks (main DOJ) have not been able to find an online copy either.

Kiran

Sent from my iPhone

> On Dec 29, 2015, at 1:44 PM, Richman, Daniel C. (DO) (OGA) [REDACTED] wrote:
>
> Do any of you have a copy of the Apple's submission to Parliament in connection with the Investigatory Powers Bill? Based on the press coverage, I suggested to [REDACTED] who blogs at Lawfare, that she might want to critique it. But neither she nor I can find it -- which is kinda interesting. Wonder whether Apple likes just using the Guardian as its mouthpiece (at least until Parliament posts the submission online).
> dan r

b6 -1,2
b7C -1,2
b7E -3

Raj, Kiran (ODAG)

From: Raj, Kiran (ODAG)
Sent: Tuesday, December 29, 2015 3:22 PM
To: Richman, Daniel C. (DO) (OGA)
Cc: Oconnell, Sasha C. (DO) (FBI); [REDACTED] (DO) (FBI); Burrell, James C. (OTD) (FBI)
Subject: Re: Apple UK submission

b6 -1
b7C -1

I believe we are going to ask the UK Embassy for a copy. Our folks (main DOJ) have not been able to find an online copy either.

Kiran

Sent from my iPhone

> On Dec 29, 2015, at 1:44 PM, Richman, Daniel C. (DO) (OGA) [REDACTED] wrote:
>
> Do any of you have a copy of the Apple's submission to Parliament in connection with the Investigatory Powers Bill? Based on the press coverage, I suggested to [REDACTED] who blogs at Lawfare, that she might want to critique it. But neither she nor I can find it -- which is kinda interesting. Wonder whether Apple likes just using the Guardian as its mouthpiece (at least until Parliament posts the submission online).
> dan r

b6 -1,2
b7C -1,2
b7E -3

Oconnell, Sasha C. (DO) (FBI)

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Tuesday, December 29, 2015 8:19 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: Fwd: WSJ on encryption ...

----- Original message -----

From: "Raj, Kiran (ODAG)" <Kiran.Raj@usdoj.gov>
Date: 12/29/2015 7:59 PM (GMT-05:00)
To: "Oconnell, Sasha C. (DO) (FBI)" [REDACTED]
Subject: Fwd: WSJ on encryption ...

b7E -3

Sent from my iPhone

Begin forwarded message:

From: "Pierce, Emily (OPA)" <epierce@jmd.usdoj.gov<mailto:epierce@jmd.usdoj.gov>>
Date: December 29, 2015 at 5:44:35 PM EST
To: "Raj, Kiran (ODAG)" <kraj@jmd.usdoj.gov<mailto:kraj@jmd.usdoj.gov>>, "Axelrod, Matthew (ODAG)" <maaxelrod@jmd.usdoj.gov<mailto:maaxelrod@jmd.usdoj.gov>>
Cc: "Newman, Melanie (OPA)" <mnewman@jmd.usdoj.gov<mailto:mnewman@jmd.usdoj.gov>>
Subject: WSJ on encryption ...

FBI Seeks to Reframe Encryption Debate

Print<javascript:void(0)> Share<javascript:void(0)> Font-size<javascript:void(0)>
12/29/15 02:42 PM EST

By Devlin Barrett

WASHINGTON--The Federal Bureau of Investigation is issuing a more direct challenge to technology companies in the wake of terror attacks in Paris and California, urging them in blunter terms to allow investigators to decrypt private communications during terror probes.

Hoping to escape a continuing debate over the technical feasibility of decryption, which they fear plays into Silicon Valley's hands, FBI Director James Comey and others are pushing executives to move away from a policy they say values customers' privacy over public safety.

"It is a business-model question," Mr. Comey said at a recent congressional hearing, adding that executives "have designed their systems and their devices so that judges' orders cannot be complied with...Should they change their business model? That is a very, very hard question."

Challenging tech CEOs like Apple Inc.'s Tim Cook directly suggests that Mr. Comey could be laying the groundwork for a push in Congress for legislation that would force the companies to change their products.

So far, however, there is no indication the tech industry is retreating from its argument that strong encryption is necessary to protect users' information, and that providing a technological "key" or "backdoor" for law enforcement would simply make the information more vulnerable to hackers of all kinds.

Apple, in response to questions for this article, said this isn't a new issue, since the company has used encryption for well over a decade as a vital way to protect customers' personal information.

"As hacking schemes and cybercrimes against individuals, companies and governments have become daily occurrences, we have worked hard to keep pace," Apple said in a statement. "We know that criminals will seek out encryption

FBI 18-CV-1833-5226

techniques or develop their own, so weakening encryption in consumer devices will only hurt law-abiding citizens who rely on it to protect their data."

Still, not all tech companies are equally firm. John Chen, CEO of cellphone maker BlackBerry Ltd., has declared the company will work with the government to be responsive to court orders, saying, "Our privacy commitment does not extend to criminals."

In the wake of the recent mass killings, advocates on both sides are watching closely for a shift in public sentiment that might put more pressure on tech companies to allow law enforcement access to encrypted information if they have a court order.

Some members of Congress are highlighting the terror attacks and threatening legislation in an attempt to pressure companies to make changes. Others have urged the creation of a blue-ribbon panel to study the issue and offer recommendations.

The FBI's current reframing of the issue is a shift from past appeals for software designers to find technical solutions. At the same time, law-enforcement officials are citing the menace of terror attacks rather than emphasizing crimes like child abductions, as they've done previously.

Cindy Cohn, executive director of the Electronic Frontier Foundation, a privacy group, said the FBI's shift "means they realize their first strategy wasn't working." She added, "By shifting the conversation to a 'business model,' they may think they have more leverage against those people."

When the U.K. recently proposed giving officials more power to monitor communications, Apple fired back with a lengthy response saying the plan would threaten the security of millions of people's data.

Mr. Comey isn't the only law enforcement leader seeking to re-energize the effort to allow investigators pierce encryption in the wake of the terror attacks in Paris and San Bernardino, Calif.

In a lengthy report on the issue in November, Manhattan District Attorney Cyrus R. Vance Jr. argued, "Apple and Google are not responsible for keeping the public safe. That is the job of law enforcement. But the consequences of these companies' actions on the public safety are severe."

Officials at Google didn't immediately respond to a request for comment.

A year ago, senior Justice Department officials met with Apple lawyers and laid out concerns about "end-to-end" encryption, which makes it impossible for authorities to scrutinize the content of encrypted exchanges.

The meeting followed a decision by Apple to make end-to-end encryption a default setting for some features on its new iPhones. Google announced a similar move around the same time for its Android cellphone operating system, with both companies saying they were focused on protecting their customers' privacy.

At the meeting, government officials raised the specter of a child's murder going unsolved because a suspect's or victim's phone couldn't be accessed. That infuriated the Apple lawyers and widened the gulf between the two sides, according to people familiar with the discussions. Tempers have cooled since then, but the policy differences remain.

Government officials acknowledge it may be hard to find a case where encryption indisputably prevented the thwarting of a deadly attack. Even where terrorists have used encrypted communications, they say, they generally also have engaged in unencrypted exchanges that law enforcement could monitor.

The problem of suspects "going dark" isn't that investigators see nothing of what an individual does, but that they see far less of it, making it harder to know if an attack may be in the offing and try to prevent it beforehand, officials said.

Terrorism has made encryption a hotter issue, but police have long complained that it can interfere with investigations of an array of crimes. Some officials cite a 2012 federal appeals court ruling related to a child-pornography case as an example of how encryption can enable dangerous criminals to remain free.

In that case, investigators noticed an individual was using Internet connections at California hotels to access and share videos of child molestation. When they cross-checked the hotels' registries for those dates, a single name came up.

Authorities seized the man's computers and hard drives, but all the data was encrypted. He was ordered to enter the password to the devices but he refused and was jailed for contempt of court.

An appeals court eventually ruled the man couldn't be forced to provide a password, because to do so would have infringed his Fifth Amendment rights against self-incrimination. That forced prosecutors to drop the case and the man wasn't charged.

Write to Devlin Barrett at devlin.barrett@wsj.com <<mailto:devlin.barrett@wsj.com>>

(END) Dow Jones Newswires

December 29, 2015 14:42 ET (19:42 GMT)

Copyright (c) 2015 Dow Jones & Company, Inc.

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Tuesday, December 29, 2015 9:38 PM
To: Oconnell, Sasha C. (DO) (FBI)
Subject: RE: WSJ on encryption ...

Am I the only person who thinks this reads like the product of a random paragraph generator?

At least now we know what hurt apple's feelings

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Tuesday, December 29, 2015 8:18 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: Fwd: WSJ on encryption ...

--

----- Original message -----

From: "Raj, Kiran (ODAG)" <Kiran.Raj@usdoj.gov>
Date: 12/29/2015 7:59 PM (GMT-05:00)
To: "Oconnell, Sasha C. (DO) (FBI)" [REDACTED]
Subject: Fwd: WSJ on encryption ...

b7E -3

Sent from my iPhone

Begin forwarded message:

From: "Pierce, Emily (OPA)" <epierce@jmd.usdoj.gov<mailto:epierce@jmd.usdoj.gov>>
Date: December 29, 2015 at 5:44:35 PM EST
To: "Raj, Kiran (ODAG)" <kraj@jmd.usdoj.gov<mailto:kraj@jmd.usdoj.gov>>, "Axelrod, Matthew (ODAG)" <maaxelrod@jmd.usdoj.gov<mailto:maaxelrod@jmd.usdoj.gov>>
Cc: "Newman, Melanie (OPA)" <mnewman@jmd.usdoj.gov<mailto:mnewman@jmd.usdoj.gov>>
Subject: WSJ on encryption ...

FBI Seeks to Reframe Encryption Debate

Print<javascript:void(0)> Share<javascript:void(0)> Font-size<javascript:void(0)> 12/29/15 02:42 PM
EST By Devlin Barrett WASHINGTON--The Federal Bureau of Investigation is issuing a more direct

challenge to technology companies in the wake of terror attacks in Paris and California, urging them in blunter terms to allow investigators to decrypt private communications during terror probes.

Hoping to escape a continuing debate over the technical feasibility of decryption, which they fear plays into Silicon Valley's hands, FBI Director James Comey and others are pushing executives to move away from a policy they say values customers' privacy over public safety.

"It is a business-model question," Mr. Comey said at a recent congressional hearing, adding that

FBI 18-CV-1833-5228

executives "have designed their systems and their devices so that judges' orders cannot be complied with...Should they change their business model? That is a very, very hard question." Challenging tech CEOs like Apple Inc.'s Tim Cook directly suggests that Mr. Comey could be laying the groundwork for a push in Congress for legislation that would force the companies to change their products.

So far, however, there is no indication the tech industry is retreating from its argument that strong encryption is necessary to protect users' information, and that providing a technological "key" or "backdoor" for law enforcement would simply make the information more vulnerable to hackers of all kinds.

Apple, in response to questions for this article, said this isn't a new issue, since the company has used encryption for well over a decade as a vital way to protect customers' personal information.

"As hacking schemes and cybercrimes against individuals, companies and governments have become daily occurrences, we have worked hard to keep pace," Apple said in a statement. "We know that criminals will seek out encryption techniques or develop their own, so weakening encryption in consumer devices will only hurt law-abiding citizens who rely on it to protect their data." Still, not all tech companies are equally firm. John Chen, CEO of cellphone maker BlackBerry Ltd., has declared the company will work with the government to be responsive to court orders, saying, "Our privacy commitment does not extend to criminals." In the wake of the recent mass killings, advocates on both sides are watching closely for a shift in public sentiment that might put more pressure on tech companies to allow law enforcement access to encrypted information if they have a court order. Some members of Congress are highlighting the terror attacks and threatening legislation in an attempt to pressure companies to make changes. Others have urged the creation of a blue-ribbon panel to study the issue and offer recommendations.

The FBI's current reframing of the issue is a shift from past appeals for software designers to find technical solutions. At the same time, law-enforcement officials are citing the menace of terror attacks rather than emphasizing crimes like child abductions, as they've done previously.

Cindy Cohn, executive director of the Electronic Frontier Foundation, a privacy group, said the FBI's shift "means they realize their first strategy wasn't working." She added, "By shifting the conversation to a 'business model,' they may think they have more leverage against those people." When the U.K. recently proposed giving officials more power to monitor communications, Apple fired back with a lengthy response saying the plan would threaten the security of millions of people's data.

Mr. Comey isn't the only law enforcement leader seeking to re-energize the effort to allow investigators pierce encryption in the wake of the terror attacks in Paris and San Bernardino, Calif. In a lengthy report on the issue in November, Manhattan District Attorney Cyrus R. Vance Jr. argued, "Apple and Google are not responsible for keeping the public safe. That is the job of law enforcement. But the consequences of these companies' actions on the public safety are severe."

Officials at Google didn't immediately respond to a request for comment.

A year ago, senior Justice Department officials met with Apple lawyers and laid out concerns about "end-to-end" encryption, which makes it impossible for authorities to scrutinize the content of encrypted exchanges.

The meeting followed a decision by Apple to make end-to-end encryption a default setting for some features on its new iPhones. Google announced a similar move around the same time for its Android cellphone operating system, with both companies saying they were focused on protecting their customers' privacy.

At the meeting, government officials raised the specter of a child's murder going unsolved because a suspect's or victim's phone couldn't be accessed. That infuriated the Apple lawyers and widened the gulf between the two sides, according to people familiar with the discussions. Tempers have cooled since then, but the policy differences remain.

Government officials acknowledge it may be hard to find a case where encryption indisputably prevented the thwarting of a deadly attack. Even where terrorists have used encrypted communications, they say, they generally also have engaged in unencrypted exchanges that law

enforcement could monitor.

The problem of suspects "going dark" isn't that investigators see nothing of what an individual does, but that they see far less of it, making it harder to know if an attack may be in the offing and try to prevent it beforehand, officials said.

Terrorism has made encryption a hotter issue, but police have long complained that it can interfere with investigations of an array of crimes. Some officials cite a 2012 federal appeals court ruling related to a child-pornography case as an example of how encryption can enable dangerous criminals to remain free.

In that case, investigators noticed an individual was using Internet connections at California hotels to access and share videos of child molestation. When they cross-checked the hotels' registries for those dates, a single name came up. Authorities seized the man's computers and hard drives, but all the data was encrypted. He was ordered to enter the password to the devices but he refused and was jailed for contempt of court.

An appeals court eventually ruled the man couldn't be forced to provide a password, because to do so would have infringed his Fifth Amendment rights against self-incrimination. That forced prosecutors to drop the case and the man wasn't charged.

Write to Devlin Barrett at devlin.barrett@wsj.com<<mailto:devlin.barrett@wsj.com>>

(END) Dow Jones Newswires

December 29, 2015 14:42 ET (19:42 GMT)

Copyright (c) 2015 Dow Jones & Company, Inc.

Oconnell, Sasha C. (DO) (FBI)

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Wednesday, December 30, 2015 11:06 AM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: WSJ on encryption ...

Right? No writing awards there.

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

From: Richman, Daniel C. (DO) (OGA)
Sent: Tuesday, December 29, 2015 9:38 PM
To: Oconnell, Sasha C. (DO) (FBI)
Subject: RE: WSJ on encryption ...

Am I the only person who thinks this reads like the product of a random paragraph generator?

At least now we know what hurt apple's feelings _____

From: Oconnell, Sasha C. (DO) (FBI) Sent: Tuesday, December 29, 2015 8:18 PM To: Richman, Daniel C. (DO) (OGA) Subject: Fwd: WSJ on encryption ...

--

----- Original message -----

From: "Raj, Kiran (ODAG)" <Kiran.Raj@usdoj.gov>
Date: 12/29/2015 7:59 PM (GMT-05:00)
To: "Oconnell, Sasha C. (DO) (FBI)" [REDACTED]
Subject: Fwd: WSJ on encryption ...

b7E -3

Sent from my iPhone

Begin forwarded message:

From: "Pierce, Emily (OPA)" <epierce@jmd.usdoj.gov<mailto:epierce@jmd.usdoj.gov>>
Date: December 29, 2015 at 5:44:35 PM EST
To: "Raj, Kiran (ODAG)" <kraj@jmd.usdoj.gov<mailto:kraj@jmd.usdoj.gov>>, "Axelrod, Matthew (ODAG)" <maaxelrod@jmd.usdoj.gov<mailto:maaxelrod@jmd.usdoj.gov>>
Cc: "Newman, Melanie (OPA)" <mnewman@jmd.usdoj.gov<mailto:mnewman@jmd.usdoj.gov>>
Subject: WSJ on encryption ...

FBI Seeks to Reframe Encryption Debate

Print<javascript:void(0)> Share<javascript:void(0)> Font-size<javascript:void(0)> 12/29/15 02:42 PM
EST By Devlin Barrett WASHINGTON--The Federal Bureau of Investigation is issuing a more direct
challenge to technology companies in the wake of terror attacks in Paris and California, urging them in

FBI 18-CV-1833-5232

blunter terms to allow investigators to decrypt private communications during terror probes.

Hoping to escape a continuing debate over the technical feasibility of decryption, which they fear plays into Silicon Valley's hands, FBI Director James Comey and others are pushing executives to move away from a policy they say values customers' privacy over public safety.

"It is a business-model question," Mr. Comey said at a recent congressional hearing, adding that executives "have designed their systems and their devices so that judges' orders cannot be complied with...Should they change their business model? That is a very, very hard question." Challenging tech CEOs like Apple Inc.'s Tim Cook directly suggests that Mr. Comey could be laying the groundwork for a push in Congress for legislation that would force the companies to change their products.

So far, however, there is no indication the tech industry is retreating from its argument that strong encryption is necessary to protect users' information, and that providing a technological "key" or "backdoor" for law enforcement would simply make the information more vulnerable to hackers of all kinds.

Apple, in response to questions for this article, said this isn't a new issue, since the company has used encryption for well over a decade as a vital way to protect customers' personal information.

"As hacking schemes and cybercrimes against individuals, companies and governments have become daily occurrences, we have worked hard to keep pace," Apple said in a statement. "We know that criminals will seek out encryption techniques or develop their own, so weakening encryption in consumer devices will only hurt law-abiding citizens who rely on it to protect their data." Still, not all tech companies are equally firm. John Chen, CEO of cellphone maker BlackBerry Ltd., has declared the company will work with the government to be responsive to court orders, saying, "Our privacy commitment does not extend to criminals." In the wake of the recent mass killings, advocates on both sides are watching closely for a shift in public sentiment that might put more pressure on tech companies to allow law enforcement access to encrypted information if they have a court order. Some members of Congress are highlighting the terror attacks and threatening legislation in an attempt to pressure companies to make changes. Others have urged the creation of a blue-ribbon panel to study the issue and offer recommendations.

The FBI's current reframing of the issue is a shift from past appeals for software designers to find technical solutions. At the same time, law-enforcement officials are citing the menace of terror attacks rather than emphasizing crimes like child abductions, as they've done previously.

Cindy Cohn, executive director of the Electronic Frontier Foundation, a privacy group, said the FBI's shift "means they realize their first strategy wasn't working." She added, "By shifting the conversation to a 'business model,' they may think they have more leverage against those people." When the U.K. recently proposed giving officials more power to monitor communications, Apple fired back with a lengthy response saying the plan would threaten the security of millions of people's data.

Mr. Comey isn't the only law enforcement leader seeking to re-energize the effort to allow investigators pierce encryption in the wake of the terror attacks in Paris and San Bernardino, Calif. In a lengthy report on the issue in November, Manhattan District Attorney Cyrus R. Vance Jr. argued, "Apple and Google are not responsible for keeping the public safe. That is the job of law enforcement. But the consequences of these companies' actions on the public safety are severe." Officials at Google didn't immediately respond to a request for comment.

A year ago, senior Justice Department officials met with Apple lawyers and laid out concerns about "end-to-end" encryption, which makes it impossible for authorities to scrutinize the content of encrypted exchanges.

The meeting followed a decision by Apple to make end-to-end encryption a default setting for some features on its new iPhones. Google announced a similar move around the same time for its Android cellphone operating system, with both companies saying they were focused on protecting their customers' privacy.

At the meeting, government officials raised the specter of a child's murder going unsolved because a suspect's or victim's phone couldn't be accessed. That infuriated the Apple lawyers and widened the

gulf between the two sides, according to people familiar with the discussions. Tempers have cooled since then, but the policy differences remain.

Government officials acknowledge it may be hard to find a case where encryption indisputably prevented the thwarting of a deadly attack. Even where terrorists have used encrypted communications, they say, they generally also have engaged in unencrypted exchanges that law enforcement could monitor.

The problem of suspects "going dark" isn't that investigators see nothing of what an individual does, but that they see far less of it, making it harder to know if an attack may be in the offing and try to prevent it beforehand, officials said.

Terrorism has made encryption a hotter issue, but police have long complained that it can interfere with investigations of an array of crimes. Some officials cite a 2012 federal appeals court ruling related to a child-pornography case as an example of how encryption can enable dangerous criminals to remain free.

In that case, investigators noticed an individual was using Internet connections at California hotels to access and share videos of child molestation. When they cross-checked the hotels' registries for those dates, a single name came up. Authorities seized the man's computers and hard drives, but all the data was encrypted. He was ordered to enter the password to the devices but he refused and was jailed for contempt of court.

An appeals court eventually ruled the man couldn't be forced to provide a password, because to do so would have infringed his Fifth Amendment rights against self-incrimination. That forced prosecutors to drop the case and the man wasn't charged.

Write to Devlin Barrett at devlin.barrett@wsj.com<<mailto:devlin.barrett@wsj.com>>

(END) Dow Jones Newswires

December 29, 2015 14:42 ET (19:42 GMT)

Copyright (c) 2015 Dow Jones & Company, Inc.

Raj, Kiran (ODAG)

From: Raj, Kiran (ODAG)
Sent: Tuesday, January 05, 2016 10:05 PM
To: Richman, Daniel C. (DO) (OGA)
Cc: Oconnell, Sasha C. (DO) (FBI); [REDACTED] (DO) (FBI); Burrell, James C. (OTD) (FBI)
Subject: Re: Apple UK submission

b6 -1
b7C -1

Dan -

I hope you had a nice and relaxing holiday. Here is the latest info we received from the UK:

Apple, along with other US based companies, submitted evidence to the various Parliamentary Committees taking evidence (not to the Government). They have briefed out to the media certain points in their evidence but not actually made it public.

My understanding is that it is the Parliamentary Committee that must agree to make such evidence public. Given the Christmas recess no Committee has yet met since the evidence was submitted. It may well be published on the Parliamentary website Wednesday or Thursday this week following the Joint Committee session scheduled for tomorrow.

Sent from my iPhone

> On Dec 29, 2015, at 3:29 PM, Richman, Daniel C. (DO) (OGA) [REDACTED] wrote:

b6 -2
b7C -2
b7E -3

>
> interesting. I guess Apple's vision of privacy extends to its legislative submissions > Just for kicks, I suggested to [REDACTED] that she query David O'Neil at Debevoise.

>
> d
> _____ > From: Raj, Kiran (ODAG) [Kiran.Raj@usdoj.gov] >
Sent: Tuesday, December 29, 2015 3:22 PM > To: Richman, Daniel C. (DO) (OGA) > Cc: Oconnell, Sasha C. (DO) (FBI); [REDACTED] (DO) (FBI); Burrell, James C. (OTD) (FBI) > Subject: Re: Apple UK submission

b6 -1
b7C -1

>
> I believe we are going to ask the UK Embassy for a copy. Our folks (main DOJ) have not been able to find an online copy either.

>
> Kiran
>
> Sent from my iPhone
>

>> On Dec 29, 2015, at 1:44 PM, Richman, Daniel C. (DO) (OGA) [REDACTED] wrote:

b6 -2
b7C -2
b7E -3

>>
>> Do any of you have a copy of the Apple's submission to Parliament in connection with the Investigatory Powers Bill? Based on the press coverage, I suggested to [REDACTED] who blogs at Lawfare, that she might want to critique it. But neither she nor I can find it -- which is kinda interesting.

FBI 18-CV-1833-5287

Wonder whether Apple likes just using the Guardian as its mouthpiece (at least until Parliament posts the submission online).

>> dan r

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Wednesday, January 06, 2016 9:02 AM
To: Raj, Kiran (ODAG)
Cc: Oconnell, Sasha C. (DO) (FBI); [REDACTED] (DO) (FBI); Burrell, James C. (OTD) (FBI)
Subject: RE: Apple UK submission

b6 -1
b7C -1

Thanks for checking
And Happy new year !

From: Raj, Kiran (ODAG) [Kiran.Raj@usdoj.gov]
Sent: Tuesday, January 05, 2016 10:04 PM
To: Richman, Daniel C. (DO) (OGA)
Cc: Oconnell, Sasha C. (DO) (FBI); [REDACTED] (DO) (FBI); Burrell, James C. (OTD) (FBI)
Subject: Re: Apple UK submission

b6 -1
b7C -1

Dan -

I hope you had a nice and relaxing holiday. Here is the latest info we received from the UK:

Apple, along with other US based companies, submitted evidence to the various Parliamentary Committees taking evidence (not to the Government). They have briefed out to the media certain points in their evidence but not actually made it public.

My understanding is that it is the Parliamentary Committee that must agree to make such evidence public. Given the Christmas recess no Committee has yet met since the evidence was submitted. It may well be published on the Parliamentary website Wednesday or Thursday this week following the Joint Committee session scheduled for tomorrow.

Sent from my iPhone

> On Dec 29, 2015, at 3:29 PM, Richman, Daniel C. (DO) (OGA) [REDACTED] wrote:

b6 -2
b7C -2
b7E -3

>
> interesting. I guess Apple's vision of privacy extends to its legislative submissions > Just for kicks, I suggested to [REDACTED] that she query David O'Neil at Debevoise.

>
> d
> _____ > From: Raj, Kiran (ODAG) [Kiran.Raj@usdoj.gov] >
Sent: Tuesday, December 29, 2015 3:22 PM > To: Richman, Daniel C. (DO) (OGA) > Cc: Oconnell, Sasha C. (DO) (FBI); [REDACTED] (DO) (FBI); Burrell, James C. (OTD) (FBI) > Subject: Re: Apple UK submission

b6 -1
b7C -1

>
> I believe we are going to ask the UK Embassy for a copy. Our folks (main DOJ) have not been able to find an online copy either.

>

FBI 18-CV-1833-5289

> Kiran

>

> Sent from my iPhone

>

>> On Dec 29, 2015, at 1:44 PM, Richman, Daniel C. (DO) (OGA) [REDACTED] wrote:

>>

>> Do any of you have a copy of the Apple's submission to Parliament in connection with the Investigatory Powers Bill? Based on the press coverage, I suggested to [REDACTED] who blogs at Lawfare, that she might want to critique it. But neither she nor I can find it -- which is kinda interesting. Wonder whether Apple likes just using the Guardian as its mouthpiece (at least until Parliament posts the submission online).

>> dan r

b6 -2

b7C -2

b7E -3

Raj, Kiran (ODAG)

From: Raj, Kiran (ODAG)
Sent: Friday, January 08, 2016 5:56 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: Automatic reply: silicon (valley) cosmetic operations

I am out of the office on business travel, and I will have limited access to email. If you need immediate assistance, please contact Winnie Brinkley [REDACTED]. Thank you!

b6 Per DOJ/OIP

Raj, Kiran (ODAG)

From: Raj, Kiran (ODAG)
Sent: Monday, January 11, 2016 10:07 AM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: silicon (valley) cosmetic operations

I miss you, too! But, I have no doubt that you are still on the case.

I have pictures, but they are not on my work phone. Do you have a personal address I can send them to?

Kiran

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

From: Richman, Daniel C. (DO) (OGA) [mailto:[\[REDACTED\]](#)]
Sent: Friday, January 08, 2016 5:54 PM
To: Raj, Kiran (ODAG)
Subject: silicon (valley) cosmetic operations

b7E -3

I hear a good time was had by all. But Sasha says you have cool pictures. Can I see too?
Tho you don't see me (and I miss you), fear not, I'm still on the case :)

Loughnane, Joan (USANYS)

From: Loughnane, Joan (USANYS)
Sent: Tuesday, January 26, 2016 6:26 PM
To: Richman, Daniel C. (DO) (OGA); Raj, Kiran (ODAG) (JMD); Krieger, Paul (USANYS); Oconnell, Sasha C. (DO) (FBI) b5 -1
b6 -1
b7C -1
Cc: [REDACTED] (NY) (INT)
Subject: RE: GD messaging [REDACTED]

Thanks so much, Dan and [REDACTED] This does look like a useful outline, and we'll be sure to reach out if we have any potential additions to it. Hope you're well, Joan

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

From: Richman, Daniel C. (DO) (OGA) [mailto:[REDACTED]] b5 -1
Sent: Tuesday, January 26, 2016 5:18 PM b6 -1
To: Raj, Kiran (ODAG) (JMD); Krieger, Paul (USANYS); Loughnane, Joan (USANYS); Oconnell, Sasha C. (DO) (FBI) b7C -1
b7E -3
Cc: [REDACTED] (NY) (INT) (FBI)
Subject: GD messaging - [REDACTED]

Dear Kiran, Paul & Joan -- As we work to improve the discourse on Going Dark, one piece that we've generally taken for granted but that requires more public articulation is the (obvious to us) point that

[REDACTED]
[REDACTED] ' To prepare for that articulation, I've been working with [REDACTED]
[REDACTED]
[REDACTED] So far, [REDACTED] has come up

with the attached work in progress that (1) you might find useful as you talk to others about the GD problem and (2) you might contribute to as you think of additional points/changes. A big lesson of the public debate so far is that some law enforcement basics need a lot more explanation. And [REDACTED] has done a terrific job of laying the foundation. Contributions will be gratefully received by [REDACTED] Sasha and yours truly thanks dan richman

Thanks,

[REDACTED]

b6 -1
b7C -1
b7E -3

[REDACTED]
Special Counsel
FBI - New York
[REDACTED]

Raj, Kiran (ODAG)

b5 -1
b6 -1
b7C -1

From: Raj, Kiran (ODAG)
Sent: Wednesday, January 27, 2016 9:47 AM
To: Richman, Daniel C. (DO) (OGA); Krieger, Paul (USANYS); Loughnane, Joan (USANYS); Oconnell, Sasha C. (DO) (FBI)
Cc: [REDACTED] (NY) (INT)
Subject: RE: GD messaging - [REDACTED]

Dan,

Thanks very much to you and [REDACTED] for putting this together. I will have a few comments and thoughts to share later today. In the meantime, do you mind if I forward to CRM and NSD, as they will no doubt find this useful.

Best,

Kiran

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

From: Richman, Daniel C. (DO) (OGA) [mailto:[REDACTED]]
Sent: Tuesday, January 26, 2016 5:18 PM
To: Raj, Kiran (ODAG); Krieger, Paul (USANYS); Loughnane, Joan (USANYS); Oconnell, Sasha C. (DO) (FBI)
Cc: [REDACTED] (NY) (INT) (FBI)
Subject: GD messaging - [REDACTED]

b5 -1
b6 -1
b7C -1
b7E -3

Dear Kiran, Paul & Joan -- As we work to improve the discourse on Going Dark, one piece that we've generally taken for granted but that requires more public articulation is the (obvious to us) point that

[REDACTED]
[REDACTED] To prepare for that articulation, I've been working with [REDACTED]

[REDACTED]
[REDACTED]. So far [REDACTED] has come up with the attached work in progress that (1) you might find useful as you talk to others about the GD problem and (2) you might contribute to as you think of additional points/changes. A big lesson of the public debate so far is that some law enforcement basics need a lot more explanation. And [REDACTED] has done a terrific job of laying the foundation. Contributions will be gratefully received by [REDACTED] Sasha and yours truly thanks dan richman

Thanks,

[REDACTED]

b6 -1
b7C -1

[Redacted]

Special Counsel

FBI - New York

[Redacted]

b6 -1

b7C -1

b7E -3

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Wednesday, January 27, 2016 11:00 AM
To: Raj, Kiran (ODAG); Krieger, Paul (USANYS); Loughnane, Joan (USANYS); Oconnell, Sasha C. (DO) (FBI)
Cc: [REDACTED] (NY) (INT)
Subject: RE: GD messaging [REDACTED]

b5 -1
b6 -1
b7C -1

Of course. And changes and suggestions are most welcome. [REDACTED]

From: Raj, Kiran (ODAG) [Kiran.Raj@usdoj.gov]
Sent: Wednesday, January 27, 2016 9:46 AM
To: Richman, Daniel C. (DO) (OGA); Krieger, Paul (USANYS); Loughnane, Joan (USANYS); Oconnell, Sasha C. (DO) (FBI)
Cc: [REDACTED] (NY) (INT)
Subject: RE: GD messaging [REDACTED]

b5 -1
b6 -1
b7C -1

Dan,

Thanks very much to you and [REDACTED] for putting this together. I will have a few comments and thoughts to share later today. In the meantime, do you mind if I forward to CRM and NSD, as they will no doubt find this useful.

Best,

Kiran

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

From: Richman, Daniel C. (DO) (OGA) [mailto:[REDACTED]]
Sent: Tuesday, January 26, 2016 5:18 PM
To: Raj, Kiran (ODAG); Krieger, Paul (USANYS); Loughnane, Joan (USANYS); Oconnell, Sasha C. (DO) (FBI)
Cc: [REDACTED] (NY) (INT) (FBI)
Subject: GD messaging - [REDACTED]

b5 -1
b6 -1
b7C -1
b7E -3

Dear Kiran, Paul & Joan -- As we work to improve the discourse on Going Dark, one piece that we've generally taken for granted but that requires more public articulation is the (obvious to us) point that

[REDACTED]
[REDACTED] To prepare for that articulation. I've been working with [REDACTED]
[REDACTED]

[REDACTED] So far, [REDACTED] has come up with the attached work in progress that (1) you might find useful as you talk to others about the GD problem and (2) you might contribute to as you think of additional points/changes. A big lesson of the public debate so far is that some law enforcement basics need a lot more explanation. And [REDACTED] has done a terrific job of laying the foundation. Contributions will be gratefully received by [REDACTED] Sasha and yours truly thanks dan richman

FBI 18-CV-1833-5567

Thanks,

[Redacted]

b6 -1
b7C -1
b7E -3

[Redacted]
Special Counsel
FBI - New York

[Redacted]

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Tuesday, January 26, 2016 5:18 PM
To: Raj, Kiran (ODAG) (JMD); Krieger, Paul (USANYS); Loughnane, Joan (USANYS);
Oconnell, Sasha C. (DO) (FBI)
Cc: [REDACTED] (NY) (INT)
Subject: GD messaging - [REDACTED]
Attachments: Going Dark Outline.docx

b5 -1
b6 -1
b7C -1

Dear Kiran, Paul & Joan -- As we work to improve the discourse on Going Dark, one piece that we've generally taken for granted but that requires more public articulation is the (obvious to us) point that

[REDACTED]
[REDACTED] To prepare for that articulation, I've been working with [REDACTED]
[REDACTED]
[REDACTED]

[REDACTED] So far [REDACTED] has come up with the attached work in progress that (1) you might find useful as you talk to others about the GD problem and (2) you might contribute to as you think of additional points/changes. A big lesson of the public debate so far is that some law enforcement basics need a lot more explanation. And [REDACTED] has done a terrific job of laying the foundation. Contributions will be gratefully received by [REDACTED] Sasha and yours truly thanks
dan richman

Thanks,
[REDACTED]

b6 -1
b7C -1
b7E -3

[REDACTED]
Special Counsel
FBI - New York
[REDACTED]

Oconnell, Sasha C. (DO) (FBI)

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Monday, February 01, 2016 8:27 AM
To: Richman, Daniel C. (DO) (OGA); Raj, Kiran (ODAG) (JMD)
Subject: FW: NYTimes.com: New Technologies Give Government Ample Means to Track Suspects, Study Finds

here is the report:

https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf

NYTimes.com: New Technologies Give Government Ample Means to Track Suspects, Study Finds

Sent by

b6 -2
b7C -2

 New Technologies Give Government Ample Means to Track Suspects, Study Finds

BY DAVID E. SANGER

Fears that encrypted communication will prevent agencies from tracking terrorists are overstated, according to a study that included current and former intelligence officials.

Or, copy and paste this URL into your browser: <http://nyti.ms/201J601>.

To get unlimited access to all New York Times articles, subscribe today. [See Subscription Options.](#)

To ensure delivery to your inbox, please add nytdirect@nytimes.com to your address book.

ADVERTISEMENT

Copyright 2016 | The New York Times Company | NYTimes.com 620 Eighth Avenue New York, NY 10018



FBI 18-CV-1833-5622

Raj, Kiran (ODAG)

From: Raj, Kiran (ODAG)
Sent: Monday, February 01, 2016 10:15 AM
To: Oconnell, Sasha C. (DO) (FBI); Richman, Daniel C. (DO) (OGA)
Subject: RE: NYTimes.com: New Technologies Give Government Ample Means to Track Suspects, Study Finds

b5 Per DOJ/OIP

My initial take on the report (after skimming it quickly) is that there are many items in the report that we would agree with. For example [REDACTED]

[REDACTED] Thoughts?

Kiran

From: Oconnell, Sasha C. (DO) (FBI) [mailto:[REDACTED]]
Sent: Monday, February 01, 2016 8:27 AM
To: Richman, Daniel C. (DO) (OGA) (FBI); Raj, Kiran (ODAG)
Subject: FW: NYTimes.com: New Technologies Give Government Ample Means to Track Suspects, Study Finds

b6 -2
b7C -2
b7E -3

here is the report:

https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf

NYTimes.com: New Technologies Give Government Ample Means to Track Suspects, Study Finds

Sent by [REDACTED]

☒ **New Technologies Give Government Ample Means to Track Suspects, Study Finds**

BY DAVID E. SANGER

Fears that encrypted communication will prevent agencies from tracking terrorists are overstated, according to a study that included current and former intelligence officials.

Or, copy and paste this URL into your browser: <http://nyti.ms/201J601>

To get unlimited access to all New York Times articles, subscribe today. [See Subscription Options...](#)

To ensure delivery to your inbox, please add nytdirect@nytimes.com to your address book.

FBI 18-CV-1833-5623

ADVERTISEMENT

Copyright 2018 | The New York Times Company | NYTimes.com 620 Eighth Avenue New York, NY 10018



Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Monday, February 01, 2016 11:08 AM
To: Raj, Kiran (ODAG); Oconnell, Sasha C. (DO) (FBI)
Subject: RE: NYTimes.com: New Technologies Give Government Ample Means to Track Suspects, Study Finds

I will read it asap. But this highlights our need to [REDACTED]

b5 -1
b6 -1
b7C -1

[REDACTED]
[REDACTED] The document I started doing with [REDACTED]
provides a good start. But a lot more is needed, tho we'll get some immediate assistance once [REDACTED]
[REDACTED]

From: Raj, Kiran (ODAG) [Kiran.Raj@usdoj.gov]
Sent: Monday, February 01, 2016 10:14 AM
To: Oconnell, Sasha C. (DO) (FBI); Richman, Daniel C. (DO) (OGA)
Subject: RE: NYTimes.com: New Technologies Give Government Ample Means to Track Suspects, Study Finds

b5 Per DOJ/OIP

My initial take on the report (after skimming it quickly) is that there are many items in the report that we would agree with. For example [REDACTED]

[REDACTED]
[REDACTED] Thoughts?

Kiran

From: Oconnell, Sasha C. (DO) (FBI) [mailto:[REDACTED]]
Sent: Monday, February 01, 2016 8:27 AM
To: Richman, Daniel C. (DO) (OGA) (FBI); Raj, Kiran (ODAG)
Subject: FW: NYTimes.com: New Technologies Give Government Ample Means to Track Suspects, Study Finds

b7E -3

here is the report:

https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf

NYTimes.com: New Technologies Give Government Ample Means to Track Suspects, Study Finds

FBI 18-CV-1833-5631

Sent by

b6 -2
b7C -2

[<http://i1.nyt.com/images/misc/nytlogo194x27.gif>]

[<http://static01.nyt.com/images/2016/02/01/world/ENCRYPTION/ENCRYPTION-thumbStandard.jpg>]

New Technologies Give Government Ample Means to Track Suspects, Study Finds

<http://p.nytimes.com/email/re?location=InCMR7g4BCJTYuyKqXu41msqahLDvgRr&user_id=10e19ddc73ebbf7955b5043f055873b2&email_type=eta&task_id=1454332527307540®i_id=0> By DAVID E. SANGER

Fears that encrypted communication will prevent agencies from tracking terrorists are overstated, according to a study that included current and former intelligence officials.

Or, copy and paste this URL into your browser: <http://nyti.ms/201J601> <http://p.nytimes.com/email/re?location=InCMR7g4BCJTYuyKqXu41msqahLDvgRr&user_id=10e19ddc73ebbf7955b5043f055873b2&email_type=eta&task_id=1454332527307540®i_id=0>

To get unlimited access to all New York Times articles, subscribe today. See Subscription Options.

<http://p.nytimes.com/email/re?location=4z5Q7Lhl+KVBjmEgFdYACDuqzkg7rwCljbQiYyNWYJIW5drsCg04xD2q1X6bqVB/vYPHy+JP5GfoOOmI3K0i6GaUY7fZ7jcK869mPAvEGfk=&user_id=10e19ddc73ebbf7955b5043f055873b2&email_type=eta&task_id=1454332527307540*i_id=0>

To ensure delivery to your inbox, please add nytdirect@nytimes.com to your address book.

Advertisement

Copyright 2016<http://p.nytimes.com/email/re?location=4z5Q7Lhl+KVBjmEgFdYACMIehlhWVuPlxganfKahJGpDcKtdpfztygRnz23j1z6nDpx4eAAqQbYRMMI5L56EeQ==&user_id=10e19ddc73ebbf7955b5043f055873b2&email_type=eta&task_id=1454332527307540®i_id=0> | The New York Times Company<http://p.nytimes.com/email/re?location=4z5Q7Lhl+KUv6vqdu/zT/DtUzLIQEcSh&user_id=10e19ddc73ebbf7955b5043f055873b2&email_type=eta&task_id=1454332527307540*i_id=0> | NYTimes.com 620 Eighth Avenue New York, NY 10018

[http://p.nytimes.com/email/re?location=hdaNaYedr2/lomeWRKt0nffrak8aSGLbvtkkq/r7ihwOf5XePlpl1w==&user_id=10e19ddc73ebbf7955b5043f055873b2&email_type=eta&task_id=1454332527307540®i_id=0]

Oconnell, Sasha C. (DO) (FBI)

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Monday, February 01, 2016 12:48 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: NYTimes.com: New Technologies Give Government Ample Means to Track Suspects, Study Finds

Thanks Dan. Hey do you have a few minutes to chat today? Had a prep session about the potential SB filing and wanted to run something by you when you have a minute.

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

From: Richman, Daniel C. (DO) (OGA)
Sent: Monday, February 01, 2016 11:08 AM
To: Raj, Kiran (ODAG) (JMD); Oconnell, Sasha C. (DO) (FBI)
Subject: RE: NYTimes.com: New Technologies Give Government Ample Means to Track Suspects, Study Finds

I will read it asap. But this highlights our need to [REDACTED]
[REDACTED]
[REDACTED] The document I started doing with [REDACTED]
provides a good start. But a lot more is needed, tho we'll get some immediate assistance once [REDACTED]
[REDACTED]

b5 -1
b6 -1
b7C -1

From: Raj, Kiran (ODAG) [Kiran.Raj@usdoj.gov]
Sent: Monday, February 01, 2016 10:14 AM
To: Oconnell, Sasha C. (DO) (FBI); Richman, Daniel C. (DO) (OGA)
Subject: RE: NYTimes.com: New Technologies Give Government Ample Means to Track Suspects, Study Finds

b5 Per DOJ/OIP

My initial take on the report (after skimming it quickly) is that there are many items in the report that we would agree with. For example [REDACTED]
[REDACTED]
[REDACTED]

Thoughts?

Kiran

From: Oconnell, Sasha C. (DO) (FBI) [mailto:[REDACTED]]
Sent: Monday, February 01, 2016 8:27 AM
To: Richman, Daniel C. (DO) (OGA) (FBI); Raj, Kiran (ODAG)
Subject: FW: NYTimes.com: New Technologies Give Government Ample Means to Track Suspects, Study Finds

b7E -3

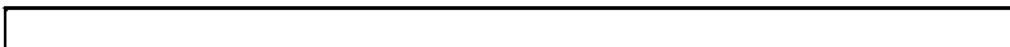
FBI 18-CV-1833-5634

here is the report:

https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf

NYTimes.com: New Technologies Give Government Ample Means to Track Suspects, Study Finds

Sent by



b6 -2
b7c -2

[<http://i1.nyt.com/images/misc/nytlogo194x27.gif>]

[<http://static01.nyt.com/images/2016/02/01/world/ENCRYPTION/ENCRYPTION-thumbStandard.jpg>]

New Technologies Give Government Ample Means to Track Suspects, Study Finds

<http://p.nytimes.com/email/re?location=InCMR7g4BCJTYuyKqXu41msqahLDvgRr&user_id=10e19ddc73ebbf7955b5043f055873b2&email_type=eta&task_id=1454332527307540®i_id=0> By DAVID E. SANGER

Fears that encrypted communication will prevent agencies from tracking terrorists are overstated, according to a study that included current and former intelligence officials.

Or, copy and paste this URL into your browser: <http://nyti.ms/201J601> <http://p.nytimes.com/email/re?location=InCMR7g4BCJTYuyKqXu41msqahLDvgRr&user_id=10e19ddc73ebbf7955b5043f055873b2&email_type=eta&task_id=1454332527307540®i_id=0>

To get unlimited access to all New York Times articles, subscribe today. See Subscription Options.

<http://p.nytimes.com/email/re?location=4z5Q7LhI+KVBjmEgFdYACDuqzkg7rwCljbQiYyNWYJIW5drsCg04xD2q1X6bqVB/vYPHy+JP5GfoOOmI3K0i6GaUY7fZ7jcK869mPAvEGfk=&user_id=10e19ddc73ebbf7955b5043f055873b2&email_type=eta&task_id=1454332527307540*i_id=0>

To ensure delivery to your inbox, please add nytdirect@nytimes.com to your address book.

Advertisement

Copyright 2016<http://p.nytimes.com/email/re?location=4z5Q7LhI+KVBjmEgFdYACMIhWVuPlxganfKahJGpDcKtdpfztygRnz23j1z6nDpx4eAAqQbYRMMI5L56EeQ==&user_id=10e19ddc73ebbf7955b5043f055873b2&email_type=eta&task_id=1454332527307540®i_id=0> | The New York Times Company<http://p.nytimes.com/email/re?location=4z5Q7LhI+KUv6vqdu/zT/DtUzLIQEcSh&user_id=10e19ddc73ebbf7955b5043f055873b2&email_type=eta&task_id=1454332527307540*i_id=0> | NYTimes.com 620 Eighth Avenue New York, NY 10018

[<http://p.nytimes.com/email/re?location=hdaNaYedr2/lomeWRKt0nffrak8aSGLbvtkkq/r7ihwOf5XeP>]

FBI 18-CV-1833-5635

lpJ1w==&user_id=10e19ddc73ebbf7955b5043f055873b2&email_type=eta&task_id=1454332527307
540®i_id=0]

From: Richman, Daniel C. (DO) (OGA)
Sent: Monday, February 01, 2016 2:17 PM
To: Oconnell, Sasha C. (DO) (FBI)
Subject: RE: NYTimes.com: New Technologies Give Government Ample Means to Track Suspects, Study Finds

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Monday, February 01, 2016 12:47 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: NYTimes.com: New Technologies Give Government Ample Means to Track Suspects, Study Finds

From: Richman, Daniel C. (DO) (OGA)
Sent: Monday, February 01, 2016 11:08 AM
To: Raj, Kiran (ODAG) (JMD); Oconnell, Sasha C. (DO) (FBI)
Subject: RE: NYTimes.com: New Technologies Give Government Ample Means to Track Suspects, Study Finds

b5 -1
b6 -1
b7C -1

From: Raj, Kiran (ODAG) [Kiran.Raj@usdoj.gov]
Sent: Monday, February 01, 2016 10:14 AM
To: Oconnell, Sasha C. (DO) (FBI); Richman, Daniel C. (DO) (OGA)
Subject: RE: NYTimes.com: New Technologies Give Government Ample Means to Track Suspects, Study Finds

My initial take on the report (after skimming it quickly) is that there are many items in the report that we would agree with. For example

[illegible]

Kiran

From: Oconnell, Sasha C. (DO) (FBI) [mailto:]
Sent: Monday, February 01, 2016 8:27 AM
To: Richman, Daniel C. (DO) (OGA) (FBI); Raj, Kiran (ODAG)
Subject: FW: NYTimes.com: New Technologies Give Government Ample Means to Track Suspects, Study Finds

b7E -3

here is the report:

https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf

NYTimes.com: New Technologies Give Government Ample Means to Track Suspects, Study Finds

Sent by

b6 -2
b7C -2

[<http://i1.nyt.com/images/misc/nytlogo194x27.gif>]

[<http://static01.nyt.com/images/2016/02/01/world/ENCRYPTION/ENCRYPTION-thumbStandard.jpg>]

New Technologies Give Government Ample Means to Track Suspects, Study Finds

<http://p.nytimes.com/email/re?location=lnCMR7g4BCJTYuyKqXu41msqahLDvgRr&user_id=10e19ddc73ebbf7955b5043f055873b2&email_type=eta&task_id=1454332527307540®i_id=0> By DAVID E. SANGER

Fears that encrypted communication will prevent agencies from tracking terrorists are overstated, according to a study that included current and former intelligence officials.

Or, copy and paste this URL into your browser: <http://nyti.ms/201J601> <http://p.nytimes.com/email/re?location=lnCMR7g4BCJTYuyKqXu41msqahLDvgRr&user_id=10e19ddc73ebbf7955b5043f055873b2&email_type=eta&task_id=1454332527307540®i_id=0>

To get unlimited access to all New York Times articles, subscribe today. See Subscription Options.

<http://p.nytimes.com/email/re?location=4z5Q7Lhl+KVBjmEgFdYACDuqzkg7rwCljbQiYyNWyJIW5drsCg04xD2q1X6bqVB/vYPHY+JP5GfoOOmI3K0i6GaUY7fZ7jcK869mPAvEGfk=&user_id=10e19ddc73ebbf7955b5043f055873b2&email_type=eta&task_id=1454332527307540&i_id=0>

To ensure delivery to your inbox, please add nytdirect@nytimes.com to your address book.

Advertisement

Copyright 2016<<http://p.nytimes.com/email/re?location=4z5Q7Lhl+KVBjmEgFdYACMIEhIhWVuPlxga>

FBI 18-CV-1833-5639

nfKahJGpDcKtdpfztygRnz23j1z6nDpx4eAAqQbYRMMl5L56EeQ==&user_id=10e19ddc73ebbf7955b5043f055873b2&email_type=eta&task_id=1454332527307540®i_id=0> | The New York Times Company<http://p.nytimes.com/email/re?location=4z5Q7Lhl+KUv6vqdu/zT/DtUzLIQEcSh&user_id=10e19ddc73ebbf7955b5043f055873b2&email_type=eta&task_id=1454332527307540*i_id=0> | NYTimes.com 620 Eighth Avenue New York, NY 10018

[http://p.nytimes.com/email/re?location=hdaNaYedr2/lomeWRKt0nffrak8aSGLbvtkkq/r7ihwOf5XePlpJ1w==&user_id=10e19ddc73ebbf7955b5043f055873b2&email_type=eta&task_id=1454332527307540®i_id=0]

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Monday, February 01, 2016 3:00 PM
To: Oconnell, Sasha C. (DO) (FBI)
Subject: RE: NYTimes.com: New Technologies Give Government Ample Means to Track Suspects, Study Finds

perfect

Here's my summary of the Berkman Center report:

no rush for you to read. Main points

1. It really is a business model choice, and we should just accept private choices
2. Don't worry about GD. Between vulnerability exploitation, metadata, and some combination of Barbies and toasters that can be bugged, all will be well.
3. Harvard has spoken.

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Monday, February 01, 2016 2:57 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: NYTimes.com: New Technologies Give Government Ample Means to Track Suspects, Study Finds

Can we try for 4:30? Have a meeting with Baker at 4 can call you when that wraps?

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

From: Richman, Daniel C. (DO) (OGA)
Sent: Monday, February 01, 2016 2:17 PM
To: Oconnell, Sasha C. (DO) (FBI)
Subject: RE: NYTimes.com: New Technologies Give Government Ample Means to Track Suspects, Study Finds

I have a meeting 3:30 to 4 and can talk anytime before or after _____

From: Oconnell, Sasha C. (DO) (FBI) **Sent:** Monday, February 01, 2016 12:47 PM **To:** Richman, Daniel C. (DO) (OGA) **Subject:** RE: NYTimes.com: New Technologies Give Government Ample Means to Track Suspects, Study Finds

Thanks Dan. Hey do you have a few minutes to chat today? Had a prep session about the potential SB filing and wanted to runs something by you when you have a minute.

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

From: Richman, Daniel C. (DO) (OGA)
Sent: Monday, February 01, 2016 11:08 AM
To: Raj, Kiran (ODAG) (JMD); Oconnell, Sasha C. (DO) (FBI)
Subject: RE: NYTimes.com: New Technologies Give Government Ample Means to Track Suspects, Study

FBI 18-CV-1833-5642

Finds

I will read it asap. But this highlights our need to [REDACTED]

b5 -1
b6 -1
b7C -1

[REDACTED]
[REDACTED] The document I started doing with [REDACTED]
provides a good start. But a lot more is needed, tho we'll get some immediate assistance once [REDACTED]

From: Raj, Kiran (ODAG) [Kiran.Raj@usdoj.gov]

Sent: Monday, February 01, 2016 10:14 AM

To: Oconnell, Sasha C. (DO) (FBI); Richman, Daniel C. (DO) (OGA)

Subject: RE: NYTimes.com: New Technologies Give Government Ample Means to Track Suspects, Study Finds

b5 Per DOJ/OIP

My initial take on the report (after skimming it quickly) is that there are many items in the report that we would agree with. For example [REDACTED]

Thoughts?

Kiran

From: Oconnell, Sasha C. (DO) (FBI) [mailto:[REDACTED]]

b7E -3

Sent: Monday, February 01, 2016 8:27 AM

To: Richman, Daniel C. (DO) (OGA) (FBI); Raj, Kiran (ODAG)

Subject: FW: NYTimes.com: New Technologies Give Government Ample Means to Track Suspects, Study Finds

here is the report:

https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf

NYTimes.com: New Technologies Give Government Ample Means to Track Suspects, Study Finds

Sent by [REDACTED]

b6 -2
b7C -2

[<http://i1.nyt.com/images/misc/nytlogo194x27.gif>]

[<http://static01.nyt.com/images/2016/02/01/world/ENCRYPTION/ENCRYPTION-thumbStandard.jpg>]

New Technologies Give Government Ample Means to Track Suspects, Study Finds

<http://p.nytimes.com/email/re?location=InCMR7g4BCJTYuyKqXu41msqahLDvgRr&user_id=10e19ddc73ebbf7955b5043f055873b2&email_type=eta&task_id=1454332527307540®i_id=0> By DAVID E.

FBI 18-CV-1833-5643

SANGER

Fears that encrypted communication will prevent agencies from tracking terrorists are overstated, according to a study that included current and former intelligence officials.

Or, copy and paste this URL into your browser: <http://nyti.ms/201J601> <http://p.nytimes.com/email/re?location=InCMR7g4BCJTYuyKqXu41msqahLDvgRr&user_id=10e19ddc73ebbf7955b5043f055873b2&email_type=eta&task_id=1454332527307540®i_id=0>

To get unlimited access to all New York Times articles, subscribe today. See Subscription Options.
<http://p.nytimes.com/email/re?location=4z5Q7Lhl+KVBjmEgFdYACDuqzkg7rwCljbQiYyNWYJIW5drsCg04xD2q1X6bqVB/vYPHy+JP5GfoOOmI3K0i6GaUY7fZ7jck869mPAvEGfk=&user_id=10e19ddc73ebbf7955b5043f055873b2&email_type=eta&task_id=1454332527307540*i_id=0>

To ensure delivery to your inbox, please add nytdirect@nytimes.com to your address book.

Advertisement

Copyright 2016<http://p.nytimes.com/email/re?location=4z5Q7Lhl+KVBjmEgFdYACMIhWVuPlxganfKahJGpDcKtdpfztygRnz23j1z6nDpx4eAAqQbYRMMI5L56EeQ==&user_id=10e19ddc73ebbf7955b5043f055873b2&email_type=eta&task_id=1454332527307540®i_id=0> | The New York Times Company<http://p.nytimes.com/email/re?location=4z5Q7Lhl+KUv6vqdu/zT/DtUzLIQEcSh&user_id=10e19ddc73ebbf7955b5043f055873b2&email_type=eta&task_id=1454332527307540*i_id=0> | NYTimes.com 620 Eighth Avenue New York, NY 10018

[http://p.nytimes.com/email/re?location=hdaNaYedr2/lomeWRKt0nffrak8aSGLbvtkkq/r7ihwOf5XePlpJ1w==&user_id=10e19ddc73ebbf7955b5043f055873b2&email_type=eta&task_id=1454332527307540®i_id=0]

Oconnell, Sasha C. (DO) (FBI)

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Monday, February 01, 2016 2:57 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: NYTimes.com: New Technologies Give Government Ample Means to Track Suspects, Study Finds

Can we try for 4:30? Have a meeting with Baker at 4 can call you when that wraps?

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

From: Richman, Daniel C. (DO) (OGA)
Sent: Monday, February 01, 2016 2:17 PM
To: Oconnell, Sasha C. (DO) (FBI)
Subject: RE: NYTimes.com: New Technologies Give Government Ample Means to Track Suspects, Study Finds

I have a meeting 3:30 to 4 and can talk anytime before or after _____
From: Oconnell, Sasha C. (DO) (FBI) Sent: Monday, February 01, 2016 12:47 PM To: Richman, Daniel C. (DO) (OGA) Subject: RE: NYTimes.com: New Technologies Give Government Ample Means to Track Suspects, Study Finds

Thanks Dan. Hey do you have a few minutes to chat today? Had a prep session about the potential SB filing and wanted to run something by you when you have a minute.

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

From: Richman, Daniel C. (DO) (OGA)
Sent: Monday, February 01, 2016 11:08 AM
To: Raj, Kiran (ODAG) (JMD); Oconnell, Sasha C. (DO) (FBI)
Subject: RE: NYTimes.com: New Technologies Give Government Ample Means to Track Suspects, Study Finds

I will read it asap. But this highlights our need to _____

b5 -1
b6 -1
b7C -1

_____ The document I started doing with _____
_____ provides a good start. But a lot more is needed, tho we'll get some immediate assistance once _____

From: Raj, Kiran (ODAG) [Kiran.Raj@usdoj.gov]
Sent: Monday, February 01, 2016 10:14 AM
To: Oconnell, Sasha C. (DO) (FBI); Richman, Daniel C. (DO) (OGA)
Subject: RE: NYTimes.com: New Technologies Give Government Ample Means to Track Suspects, Study Finds

b5 Per DOJ/OIP

My initial take on the report (after skimming it quickly) is that there are many items in the report that we would agree with. For example, _____

FBI 18-CV-1833-5645

[Redacted]
[Redacted] Thoughts?

Kiran

From: Oconnell, Sasha C. (DO) (FBI) [mailto:[Redacted]]
Sent: Monday, February 01, 2016 8:27 AM
To: Richman, Daniel C. (DO) (OGA) (FBI); Raj, Kiran (ODAG)
Subject: FW: NYTimes.com: New Technologies Give Government Ample Means to Track Suspects, Study Finds

b7E -3

here is the report:

https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf

NYTimes.com: New Technologies Give Government Ample Means to Track Suspects, Study Finds

Sent by [Redacted]

b6 -2
b7C -2

[<http://i1.nyt.com/images/misc/nytlogo194x27.gif>]

[<http://static01.nyt.com/images/2016/02/01/world/ENCRYPTION/ENCRYPTION-thumbStandard.jpg>]

New Technologies Give Government Ample Means to Track Suspects, Study Finds
<http://p.nytimes.com/email/re?location=InCMR7g4BCJTYuyKqXu41msqahLDvgRr&user_id=10e19ddc73ebbf7955b5043f055873b2&email_type=eta&task_id=1454332527307540®i_id=0> By DAVID E. SANGER

Fears that encrypted communication will prevent agencies from tracking terrorists are overstated, according to a study that included current and former intelligence officials.

Or, copy and paste this URL into your browser: <http://nyti.ms/201J601> <http://p.nytimes.com/email/re?location=InCMR7g4BCJTYuyKqXu41msqahLDvgRr&user_id=10e19ddc73ebbf7955b5043f055873b2&email_type=eta&task_id=1454332527307540®i_id=0>

To get unlimited access to all New York Times articles, subscribe today. See Subscription Options.
<http://p.nytimes.com/email/re?location=4z5Q7Lhl+KVBjmEgFdYACDuqzkg7rwCljbQiYyNWyJIW5drsCg04xD2q1X6bqVB/vYPHy+JP5GfoOOmI3K0i6GaUY7fZ7jcK869mPAvEGfk=&user_id=10e19ddc73ebbf7955b5043f055873b2&email_type=eta&task_id=1454332527307540&i_id=0>

To ensure delivery to your inbox, please add nytdirect@nytimes.com

to your address book.

Advertisement

Copyright 2016<http://p.nytimes.com/email/re?location=4z5Q7Lhl+KVBjmEgFdYACMIhWVuPlxganfKahJGpDcKtdpfztygRnz23j1z6nDpx4eAAqQbYRMMI5L56EeQ==&user_id=10e19ddc73ebbf7955b5043f055873b2&email_type=eta&task_id=1454332527307540®i_id=0> | The New York Times Company<http://p.nytimes.com/email/re?location=4z5Q7Lhl+KUv6vqdu/zT/DtUzLIQEcSh&user_id=10e19ddc73ebbf7955b5043f055873b2&email_type=eta&task_id=1454332527307540*i_id=0> | NYTimes.com 620 Eighth Avenue New York, NY 10018

[http://p.nytimes.com/email/re?location=hdaNaYedr2/lomeWRKt0nffrak8aSGLbvtkkq/r7ihwOf5XePlp1w==&user_id=10e19ddc73ebbf7955b5043f055873b2&email_type=eta&task_id=1454332527307540®i_id=0]

Oconnell, Sasha C. (DO) (FBI)

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Monday, February 01, 2016 3:03 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: NYTimes.com: New Technologies Give Government Ample Means to Track Suspects, Study Finds

Ok that is beautiful. Columbia has spoken :)

Yes, SB isn't a problem bc we can just tap the TV or HVAC.

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

From: Richman, Daniel C. (DO) (OGA)
Sent: Monday, February 01, 2016 3:00 PM
To: Oconnell, Sasha C. (DO) (FBI)
Subject: RE: NYTimes.com: New Technologies Give Government Ample Means to Track Suspects, Study Finds

perfect

Here's my summary of the Berkman Center report:

no rush for you to read. Main points

1. It really is a business model choice, and we should just accept private choices
2. Don't worry about GD. Between vulnerability exploitation, metadata, and some combination of Barbies and toasters that can be bugged, all will be well.
3. Harvard has spoken.

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Monday, February 01, 2016 2:57 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: NYTimes.com: New Technologies Give Government Ample Means to Track Suspects, Study Finds

Can we try for 4:30? Have a meeting with Baker at 4 can call you when that wraps?

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

From: Richman, Daniel C. (DO) (OGA)
Sent: Monday, February 01, 2016 2:17 PM
To: Oconnell, Sasha C. (DO) (FBI)
Subject: RE: NYTimes.com: New Technologies Give Government Ample Means to Track Suspects, Study Finds

I have a meeting 3:30 to 4 and can talk anytime before or after _____
_____ **From:** Oconnell, Sasha C. (DO) (FBI) **Sent:** Monday, February 01, 2016 12:47 PM **To:**

FBI 18-CV-1833-5648

Richman, Daniel C. (DO) (OGA) Subject: RE: NYTimes.com: New Technologies Give Government Ample Means to Track Suspects, Study Finds

Thanks Dan. Hey do you have a few minutes to chat today? Had a prep session about the potential SB filing and wanted to run something by you when you have a minute.

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

From: Richman, Daniel C. (DO) (OGA)
Sent: Monday, February 01, 2016 11:08 AM
To: Raj, Kiran (ODAG) (JMD); Oconnell, Sasha C. (DO) (FBI)
Subject: RE: NYTimes.com: New Technologies Give Government Ample Means to Track Suspects, Study Finds

I will read it asap. But this highlights our need to [REDACTED]

b5 -1
b6 -1
b7C -1

[REDACTED]
[REDACTED] The document I started doing with [REDACTED]
provides a good start. But a lot more is needed, tho we'll get some immediate assistance once [REDACTED]
[REDACTED]

From: Raj, Kiran (ODAG) [Kiran.Raj@usdoj.gov]
Sent: Monday, February 01, 2016 10:14 AM
To: Oconnell, Sasha C. (DO) (FBI); Richman, Daniel C. (DO) (OGA)
Subject: RE: NYTimes.com: New Technologies Give Government Ample Means to Track Suspects, Study Finds

b5 Per DOJ/OIP

My initial take on the report (after skimming it quickly) is that there are many items in the report that we would agree with. For example [REDACTED]
[REDACTED]
[REDACTED] Thoughts?

Kiran

From: Oconnell, Sasha C. (DO) (FBI) [mailto:[REDACTED]]
Sent: Monday, February 01, 2016 8:27 AM
To: Richman, Daniel C. (DO) (OGA) (FBI); Raj, Kiran (ODAG)
Subject: FW: NYTimes.com: New Technologies Give Government Ample Means to Track Suspects, Study Finds

b7E -3

here is the report:

https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf

NYTimes.com: New Technologies Give Government Ample Means to Track Suspects, Study Finds

FBI 18-CV-1833-5649

Sent by



b6 -2
b7C -2

[<http://i1.nyt.com/images/misc/nytlogo194x27.gif>]

[<http://static01.nyt.com/images/2016/02/01/world/ENCRYPTION/ENCRYPTION-thumbStandard.jpg>]

New Technologies Give Government Ample Means to Track Suspects, Study Finds

<http://p.nytimes.com/email/re?location=InCMR7g4BCJTYuyKqXu41msqahLDvgRr&user_id=10e19ddc73ebbf7955b5043f055873b2&email_type=eta&task_id=1454332527307540®i_id=0> By DAVID E. SANGER

Fears that encrypted communication will prevent agencies from tracking terrorists are overstated, according to a study that included current and former intelligence officials.

Or, copy and paste this URL into your browser: <http://nyti.ms/201J601> <http://p.nytimes.com/email/re?location=InCMR7g4BCJTYuyKqXu41msqahLDvgRr&user_id=10e19ddc73ebbf7955b5043f055873b2&email_type=eta&task_id=1454332527307540®i_id=0>

To get unlimited access to all New York Times articles, subscribe today. See Subscription Options.

<http://p.nytimes.com/email/re?location=4z5Q7LhI+KVBjmEgFdYACDuqzkg7rwCljbQjYyNWYJIW5drsCg04xD2q1X6bqVB/vYPHy+JP5GfoOOmI3K0i6GaUY7fZ7jcK869mPAvEGfk=&user_id=10e19ddc73ebbf7955b5043f055873b2&email_type=eta&task_id=1454332527307540*i_id=0>

To ensure delivery to your inbox, please add nytdirect@nytimes.com to your address book.

Advertisement

Copyright 2016<http://p.nytimes.com/email/re?location=4z5Q7LhI+KVBjmEgFdYACMIhWVuPlxganfKahJGpDcKtdpfztygRnz23j1z6nDpx4eAAqQbYRMMI5L56EeQ==&user_id=10e19ddc73ebbf7955b5043f055873b2&email_type=eta&task_id=1454332527307540®i_id=0> | The New York Times Company<http://p.nytimes.com/email/re?location=4z5Q7LhI+KUv6vqdu/zT/DtUzLIQECS&user_id=10e19ddc73ebbf7955b5043f055873b2&email_type=eta&task_id=1454332527307540*i_id=0> | NYTimes.com 620 Eighth Avenue New York, NY 10018

[http://p.nytimes.com/email/re?location=hdaNaYedr2/lomeWRKtOnffrak8aSGLbvtkkq/r7ihwOf5XePlp1w==&user_id=10e19ddc73ebbf7955b5043f055873b2&email_type=eta&task_id=1454332527307540®i_id=0]

Oconnell, Sasha C. (DO) (FBI)

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Thursday, February 04, 2016 9:11 AM
To: Richman, Daniel C. (DO) (OGA)
Subject: Fwd: Cipher Brief (Olsen): Making Progress on the "Going Dark" Debate

----- Original message -----

From: "Ferrante, Anthony J. EOP/NSC" [REDACTED]
Date: 02/04/2016 9:04 AM (GMT-05:00)
To: "Oconnell, Sasha C. (DO) (FBI)" [REDACTED]
Subject: Fw: Cipher Brief (Olsen): Making Progress on the "Going Dark" Debate

b6 Per NSC

b7E -3

Assuming you saw this, below?

-AIF

Anthony J. Ferrante
Director for Cybersecurity Policy
National Security Council
The White House

[REDACTED] desk
[REDACTED] mobile

b6 Per NSC

*This communication has been sent from my wireless device. Please excuse any typographical errors.

From: Price, Ned C. EOP/NSC [REDACTED]
Sent: Thursday, February 4, 2016 08:15
To: #CT; #CYBER; DL-WHO-Press
Subject: Cipher Brief (Olsen): Making Progress on the "Going Dark" Debate

b6 Per NSC

<http://thecipherbrief.com/article/making-progress-%E2%80%9Cgoing-dark%E2%80%9D-debate>

Making Progress on the "Going Dark" Debate

FEBRUARY 3, 2016 | MATTHEW OLSEN

MATTHEW OLSEN

FORMER DIRECTOR, NATIONAL COUNTERTERRORISM CENTER

FBI 18-CV-1833-5710

As the Director of the National Counterterrorism Center, Matthew Olsen oversaw the integration and analysis of all intelligence related to terrorism. He recently co-authored a report for Harvard's Berkman Center for Internet and Society about the ongoing encryption debate, and discussed the report with The Cipher Brief.

The Cipher Brief: Your report concluded that the "going dark" problem may be overstated. Can you tell us a little more about the report and its findings?

Matthew Olsen: First of all, the "going dark" problem is a real problem – the report makes that point clear. The FBI and other intelligence agencies have definitely lost access to communications and other sources of information because that information is now encrypted. There's really no debate about that fact. And the trend towards increased encryption has made the FBI's job more difficult. This is especially true for monitoring terrorists, like ISIS, but it's also true for criminal investigations, like kidnappings. At Harvard, we generally agreed on that point.

What we tried to do in the paper was bring together a diverse group of people and to look at the problem a bit more broadly. We weren't going to agree on a solution to the going dark problem or encryption, but we did agree on a couple of points that I think are helpful in putting the debate in perspective.

One is that there are general economic and technological trends that will help alleviate the challenge of encryption. First, we make the point that Internet companies depend on access to data for their business models, so these companies are not going to adopt encryption across the board. The key here is for these companies to step up, in my view, and to work with the government to provide access to the data they already have.

The second point we tried to make is that the explosion in network sensors, and the Internet of Things provides new channels for the government to collect information – both from a law enforcement and an intelligence perspective. As we looked ahead, we agreed that the proliferation of networked devices would open up new opportunities for the government to collect the information it needs. These new channels will help to mitigate the real loss of access due to encryption.

Our goal with this paper was not take sides in the debate over encryption. It was, rather, to look at the challenge that encryption creates, to think about the problem more broadly, and to find points of consensus among a very diverse set of perspectives.

TCB: You mentioned the profusion of sensor and network enabled objects that are coming about as a result of the Internet of Things (IoT), could you tell us a little more about that, and how it provides opportunities for surveillance?

MO: As a federal prosecutor, I worked for over a decade handling homicide and terrorism cases. Looking at the opportunities to collect information that would be useful in a criminal case or in terrorism investigations, it strikes me that there are a multitude of channels of information, particularly from networked sensors, that weren't available 20 or 10 years ago. You can just think about the ways in which the devices like smart phones and the internet of things—whether it's appliances or products, televisions, door locks, all the wearables that people use now—are all linked to the Internet. These all are potential sources of data that could be quite valuable in either an intelligence or a law enforcement investigation.

TCB: What's the takeaway for the FBI here? Director James Comey has been very vocal about his concerns about encryption. How should law enforcement use the findings of this report to more effectively combat terrorism domestically?

MO: From my perspective, the first take away for the FBI is to keep pressing the argument that they've been making. Director Comey and officials at the Department of Justice are right to raise the encryption issue and put it front and center for public debate. I saw, firsthand, the same problem when I was the director at the National Counterterrorism Center (NCTC). We are losing access to terrorist communications because of encryption. ISIS is aggressively taking advantage of encrypted platforms to communicate and even just released a how-to manual on using encryption which included a 24/7 help desk capability. So there's no doubt that ISIS is using encrypted channels to protect their communications and keep them out of the hands of law enforcement.

I think the FBI should continue to advance the argument and to work, as they have been, with the technology community to address this problem. I think that's the right approach, and it's what we've seen happening more recently, with the technology community. This engagement should enable the FBI and the rest of law enforcement to establish ways to gain effective access with lawful process to information in the possession of these companies. That's been the FBI's strategy, and I think it's the right one.

The second take away is to be creative in thinking about new ways to obtain evidence and intelligence. If one channel goes dark because of encryption, what other channels are open? Again, because of the proliferation of network sensors and the Internet of Things, there are new opportunities for collection to mitigate the loss that is the result of encryption.

TCB: What about privacy concerns as they relate to the Internet of Things? Do you think private companies will push back against the government's use of IoT information as they did over the encryption issue?

MO: I've been very encouraged by what I've observed over the last several months with the level of collaboration and discourse between the government and the technology community. It strikes me that we have crossed over into an environment where these important conversations are occurring. What do these companies collect? What can the government lawfully obtain? How can we work together to address the common problem that terrorists use these platforms to recruit, radicalize, and advance terrorist operations inside the United States? I think the trajectory is a positive one in terms of the level of cooperation.

I think at the same time, there are privacy concerns that are raised by the Internet of Things, just as there have been privacy concerns historically about the government's ability to access telephone communications. And we have processes in place to help address those privacy concerns and to balance the privacy interests with the national security and law enforcement interests on the other side. Those processes will work for new technologies in the same way that they've worked for existing technologies, like the telephone. My view is that what we have in place to reconcile competing interests should be up to the task of dealing with those issues as they arise with new technologies.

TCB: Do you foresee that some of these technology companies associated with the Internet of Things will seek to get encryption on those devices, as telephones have now been encrypted?

MO: As we point out in the paper, there is a limit to what these companies will actually subject to encryption, because the business models for many of the companies depend on having access to clear text. I don't think that encryption will be ubiquitous with the new ways in which they are collecting data. I think that will create opportunities for those companies to work with the government.

Oconnell, Sasha C. (DO) (FBI)

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Thursday, February 18, 2016 4:24 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: FW: Follow up
Attachments: ED 15-0451M Ex Parte Application re Motion to Compel Apple Assistance Pursuant to AWA.pdf; ED 15-0451M Order Compelling Apple Assistance Pursuant to AWA.pdf

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

From: Raj, Kiran (ODAG) [mailto:Kiran.Raj@usdoj.gov]

Sent: Thursday, February 18, 2016 3:10 PM

To: [REDACTED] (DO) (FBI); Oconnell, Sasha C. (DO) (FBI); [REDACTED]

b6 -1,5
b7C -1,5

Subject: Follow up

All -

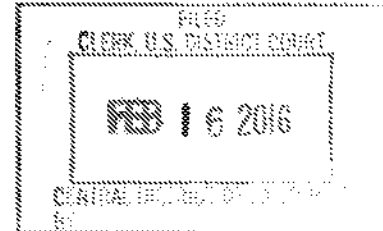
Per the request on the call, I have attached the publicly filed documents from 2/16. Please let me know if you have any questions.

Best,

Kiran

FILED
COPY
2015 FEB 16 AM 11:00

CLERK U.S. DISTRICT COURT
CENTRAL DIST. OF CALIF.
RIVERSIDE



EILEEN M. DECKER
United States Attorney
PATRICIA A. DONAHUE
Assistant United States Attorney
Chief, National Security Division
TRACY L. WILKISON (California Bar No. 184948)
Assistant United States Attorney
Chief, Cyber and Intellectual Property Crimes Section
ALLEN W. CHIU (California Bar No. 240516)
Assistant United States Attorney
Terrorism and Export Crimes Section
1500 United States Courthouse
312 North Spring Street
Los Angeles, California 90012
Telephone: (213) 894-0622/2435
Facsimile: (213) 894-8601
Email: Tracy.Wilkison@usdoj.gov
Allen.Chiu@usdoj.gov

Attorneys for Applicant
UNITED STATES OF AMERICA

UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA

IN THE MATTER OF THE SEARCH OF
AN APPLE IPHONE SEIZED DURING
THE EXECUTION OF A SEARCH
WARRANT ON A BLACK LEXUS IS300,
CALIFORNIA LICENSE PLATE
35KGD203

ED No. 15-0451M

GOVERNMENT'S *EX PARTE* APPLICATION
FOR ORDER COMPELLING APPLE INC. TO
ASSIST AGENTS IN SEARCH;
MEMORANDUM OF POINTS AND
AUTHORITIES; DECLARATION OF
CHRISTOPHER PLUHAR; EXHIBIT

The United States of America, by and through its counsel,
Assistant United States Attorneys Tracy L. Wilkison and Allen W.
Chiu, hereby applies to the Court *ex parte* pursuant to the All Writs
Act, 28 U.S.C. § 1651, for an order that Apple Inc. ("Apple") provide
assistance to agents of the Federal Bureau of Investigation ("FBI")
in their search of a cellular telephone, Apple make: iPhone 5C,
Model: A1532, P/N: MGFG2LL/A, S/N: FFMNQ3MTG2DJ, IMEI:
358820052301412, on the Verizon Network (the "SUBJECT DEVICE"). The
search and seizure of the SUBJECT DEVICE was authorized through a

1 search warrant which was obtained on December 3, 2015, Docket Number
2 ED No. 15-0451M, and was executed on the same day.

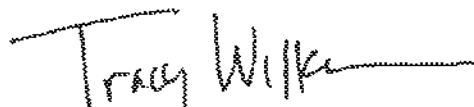
3 This application is based on the attached declaration of FBI
4 Supervisory Special Agent Christopher Pluhar, and the files and
5 records of this case, including the underlying search warrant, which
6 is attached hereto as Exhibit 1.

7 Dated: February 16, 2016

Respectfully submitted,

8 EILEEN M. DECKER
9 United States Attorney

10 PATRICIA A. DONAHUE
11 Assistant United States Attorney
Chief, National Security Division

12 

13 TRACY L. WILKISON
14 ALLEN W. CHIU
Assistant United States Attorneys

15 Attorneys for Applicant
16 UNITED STATES OF AMERICA
17
18
19
20
21
22
23
24
25
26
27
28

1 MEMORANDUM OF POINTS AND AUTHORITIES

2 I. INTRODUCTION

3 In the hopes of gaining crucial evidence about the December 2,
4 2015 massacre in San Bernardino, California, the government has
5 sought to search a lawfully-seized Apple iPhone used by one of the
6 mass murderers. Despite both a warrant authorizing the search and
7 the phone owner's consent, the government has been unable to
8 complete the search because it cannot access the iPhone's encrypted
9 content. Apple has the exclusive technical means which would assist
10 the government in completing its search, but has declined to provide
11 that assistance voluntarily. Accordingly, the government
12 respectfully requests that this Court issue an order compelling
13 Apple to assist in enabling the search commanded by the warrant.

14 II. FACTUAL BACKGROUND

15 The Federal Bureau of Investigation ("FBI") is in possession of
16 a cellular telephone that was used by Syed Rizwan Farook ("Farook"),
17 one of the terrorists who caused the December 2, 2015 shooting death
18 of 14 people, and the shooting and injuring of 22 others, at the
19 Inland Regional Center ("IRC") in San Bernardino, California. The
20 cellular telephone is of Apple make: iPhone 5C, Model: A1532, P/N:
21 MGFQ2LL/A, S/N: FFMNQ3MTG2DJ, IMEI: 358820052301412, on the Verizon
22 Network ("the SUBJECT DEVICE"). The SUBJECT DEVICE was seized
23 pursuant to a federal search warrant for a black Lexus IS300 in
24 Docket Number ED 15-0451M, which was issued by the Honorable David
25 T. Bristow, United States Magistrate Judge, on December 3, 2015.
26 The underlying search warrant, which authorizes the search of the
27 contents of the SUBJECT DEVICE, is attached hereto as Exhibit 1 and
28 incorporated herein by reference.

1 As explained in the attached declaration of FBI Supervisory
2 Special Agent ("SSA") Christopher Pluhar, the underlying search
3 warrant for the SUBJECT DEVICE arose out of an investigation into
4 the IRC shootings, and the participation by Farook and his wife,
5 Tafsheen Malik ("Malik"), in that crime. Subsequent to execution of
6 the search warrant at issue, the FBI obtained numerous search
7 warrants to search the digital devices and online accounts of Farook
8 and Malik. Through those searches, the FBI has discovered, for
9 example, that on December 2, 2015, at approximately 11:14 a.m., a
10 post on a Facebook page associated with Malik stated, "We pledge
11 allegiance to Khalifa bu bkr al bhaghdadi al quraishi," referring to
12 Abu Bakr Al Baghdadi, the leader of Islamic State of Iraq and the
13 Levant ("ISIL"), also referred to as the Islamic State ("IS"), the
14 Islamic State of Iraq and al-sham ("ISIS"), or Daesh. ISIL,
15 formerly known as Al-Qai'da in Iraq ("AQI"), has been designated a
16 foreign terrorist organization by the United States Department of
17 State, and has been so designated since December 2004. Farook and
18 Malik died later that same day in a shoot-out with law enforcement.
19 The government requires Apple's assistance to access the SUBJECT
20 DEVICE to determine, among other things, who Farook and Malik may
21 have communicated with to plan and carry out the IRC shootings,
22 where Farook and Malik may have traveled to and from before and
23 after the incident, and other pertinent information that would
24 provide more information about their and others' involvement in the
25 deadly shooting.

26 The SUBJECT DEVICE is owned by Farook's employer, the San
27 Bernardino County Department of Public Health ("SBCDPH"), and was
28 assigned to, and used by, Farook as part of his employment. The

1 SBCDPH has given its consent to the search of the SUBJECT DEVICE and
2 to Apple's assistance with that search.¹

3 However, despite the search warrant and the owner's consent,
4 the FBI has been unable to search the SUBJECT DEVICE because it is
5 "locked" or secured with a user-determined, numeric passcode. More
6 to the point, the FBI has been unable to make attempts to determine
7 the passcode because Apple has written, or "coded," its operating
8 systems with a user-enabled "auto-erase function" that would, if
9 enabled, result in the permanent destruction of the required
10 encryption key material after 10 erroneous attempts at the passcode
11 (meaning that after 10 failed attempts at inputting the passcode,
12 the information on the device becomes permanently inaccessible).
13 When an Apple iPhone is locked, it is not apparent from the outside
14 whether or not that auto-erase function is enabled; therefore,
15 trying repeated passcodes risks permanently denying all access to
16 the contents. Primarily because of this function and the delays
17 that would be introduced by successive incorrect passcodes
18 (discussed below), the government has not been able to attempt to
19 determine the passcode and decrypt the files on the SUBJECT DEVICE
20 pursuant to the search warrant, and the FBI cannot do so without
21 Apple's assistance.

22 Apple is the manufacturer of the SUBJECT DEVICE, and the
23 creator and owner of its operating system and software. Apple has
24 the ability with older operating systems to obtain the unencrypted
25 file content from phones without the passcode, and has routinely
26 done so for law enforcement with a search warrant and accompanying

27 ¹ In addition, SBCDPH has a written policy that all digital
28 devices are subject to search at any time by the SBCDPH, which
policy Farook accepted via signature upon his employment.

1 All Writs Act order. While Apple has publicized that it has written
2 the software differently with respect to iPhones such as the SUBJECT
3 DEVICE with operating system ("iOS") 9, Apple yet retains the
4 capacity to provide the assistance sought herein that may enable the
5 government to access the SUBJECT DEVICE pursuant to the search
6 warrant.

7 Specifically, and as detailed below, Apple has the ability to
8 modify software that is created to only function within the SUBJECT
9 DEVICE that would ensure that the added auto-erase function is
10 turned off, allow for electronic submission of test passcodes, and
11 ensure additional delays are not created. This would allow the
12 government multiple investigative attempts to determine the passcode
13 in a timely manner, without fear that the data subject to search
14 under the warrant would be rendered permanently inaccessible. It is
15 this assistance from Apple, which is required to execute the search
16 warrant, that the government now asks the Court to order.

17 III. DISCUSSION

18 A. Assistance Sought From Apple

19 In sum, the government seeks an order that Apple assist in
20 enabling the search commanded by the warrant by removing, for the
21 SUBJECT DEVICE only, some of the additional, non-encryption barriers
22 that Apple has coded into its operating system, such as the auto-
23 erase function, the requirement that passwords be entered manually,
24 and any software-invoked delay-upon-failure functions. While the
25 government proposes a specific means of accomplishing this, the
26 government requests that the order allow Apple to achieve the goals
27 of the order in an alternative technical manner if mutually
28 preferable.

1 As an initial matter, the assistance sought can only be
2 provided by Apple. As discussed in the attached declaration of SSA
3 Pluhar, the SUBJECT DEVICE is an iPhone 5c that was designed,
4 manufactured, and sold by Apple. Apple also wrote and owns the
5 software operating system marketed under the name of "iOS," and thus
6 is the owner of the operating system software for the phone at
7 issue. Apple's software licensing agreement specifies that its
8 software is "licensed, not sold," and otherwise prohibits users from
9 transferring any ownership of the iOS software.

10 Further to this point, Apple strictly and exclusively controls
11 the hardware and software that is used to turn on and run its
12 phones. According to Apple's "white papers" and other publicly
13 available information about the security of its iOS programs, Apple
14 has designed its mobile device hardware, as well as its operating
15 system software, to only permit and run software that has been
16 "signed" cryptographically by Apple using its own proprietary
17 encryption methods. These security features prevent other persons,
18 including the government, from running any other software on the
19 SUBJECT DEVICE to attempt to recover data or test passcodes.

20 Apple has designed the iOS 9 operating system for its phones to
21 encrypt the data files by a combination of two components - one
22 user-determined passcode, and one unique 256-bit Advanced Encryption
23 Standard ("AES") key (referred to as a "UID") which is fused into
24 the phone itself during manufacture. Both passcode components are
25 required in combination for the operating system to decrypt the
26 phone's data files. When a user inputs her passcode, the phone
27 conducts a complex calculation as determined by Apple's software
28

1 (and unknown to the government) which combines the UID with the user
2 passcode. If the result is accurate, the data is decrypted.

3 If one does not know the user-determined passcode, it is
4 possible, although time-consuming, to manually input passcodes one
5 at a time until the passcode is determined. Apple, however, has
6 also designed and written code for additional non-encryption-based
7 features which the government cannot overcome on its own.

8 First, Apple has designed a non-encryption, auto-erase function
9 as part of its iOS, which destroys the encryption key materials
10 required for decryption and hence renders the contents of the device
11 permanently incapable of being decrypted after ten consecutive
12 incorrect passcode attempts. If this auto-erase function is
13 enabled, the operating system will instantly, irrecoverably, and
14 without warning erase the encryption keys necessary for accessing
15 stored data. There is no way to know by examining the outside of
16 the phone whether or not this function has been enabled, although,
17 in this instance, the government suspects that it has, for the
18 reasons explained in the attached declaration of SSA Pluhar -
19 including because the SBCDPH has stated that the SUBJECT DEVICE was
20 provided to Farook with that function turned on, and the most recent
21 backup from the iCloud showed the function turned on. Accordingly,
22 trying successive passcodes risks permanently losing the ability to
23 access the data on the SUBJECT DEVICE. Because iOS software must be
24 cryptographically signed by Apple, only Apple is able to modify the
25 iOS software to change the setting or prevent execution of the
26 function.

27 Relatedly, Apple has designed and written code for another non-
28 encryption-based feature in that its iOS operating system is coded

1 to invoke time delays after repeated, unsuccessful passcode entries.
2 This means that after each failed passcode entry, the user must wait
3 a period of time before another attempt can be made, up to a 1-hour
4 delay after the ninth failed attempt. Additional wait times can
5 also be added into the software.

6 In order to overcome these hurdles, the government seeks an
7 order requiring Apple to assist in the execution of a search warrant
8 using the capabilities that Apple has retained along within its
9 encryption software, such that the government can attempt to
10 determine the passcode without these additional, non-encryption
11 features that Apple has coded into its operating system, for the
12 SUBJECT DEVICE only. Apple's assistance would permit the government
13 to electronically test passcodes without unnecessary delay or fear
14 that the data subject to search under the warrant would be rendered
15 permanently inaccessible. Given that these features were designed
16 and implemented by Apple, that Apple writes and cryptographically
17 signs the iOS, and that Apple routinely patches or updates its iOS
18 to address security features or other functionality, modifying these
19 features is well within its technical capabilities.

20 Specifically, in order to perform the search ordered in the
21 warrant, the government requests that Apple be ordered to provide
22 the FBI with a custom signed iPhone Software ("IPSW") file, recovery
23 bundle, or other Software Image File ("SIF")² that can be loaded onto
24 the SUBJECT DEVICE. The SIF would load and run from Random Access
25
26
27

28 ² These are different terms for the essentially same thing: a
software file that will start up/"boot" an iPhone device.

1 Memory ("RAM")³ and accordingly would not change the operating system
2 on the actual SUBJECT DEVICE, the user data partition (i.e., where
3 the contents of files created or modified by the user are stored),
4 or system partition on the device's flash memory. Importantly, the
5 SIF would be created with a unique identifier of the SUBJECT DEVICE
6 so that the SIF would only load and execute on the SUBJECT DEVICE.⁴

7 Once active on the SUBJECT DEVICE, the SIF would have three
8 primary functions: (1) the SIF would bypass or disable the auto-
9 erase function whether or not it has been enabled; (2) the SIF would
10 enable the FBI to submit passcodes to the SUBJECT DEVICE for testing
11 electronically (meaning that the attempts at the passcode would not
12 have to be manually typed on the iPhone's screen; and (3) the SIF
13 would not introduce any additional delay between failed passcode
14 attempts beyond what is incurred by the hardware on the SUBJECT
15 DEVICE. The SIF would be installed on the SUBJECT DEVICE at either
16 a government facility, or alternatively, at an Apple facility (as is
17 done when Apple recovers data from earlier iOS versions), but
18 passcode attempts would be electronically submitted to the device by
19 the government. This would allow the government to conduct the
20 passcode attempts while Apple retains the SIF. The government
21 further requests that the order permit Apple to satisfy these three

22
23
24 ³ RAM is computer memory that is temporary and requires power to
25 maintain the stored information; once the power is turned off, the
memory is lost.

26 ⁴ Since Apple's software currently has the capability to query
27 hardware for unique identifiers (serial numbers, ECID, IMEI, etc.),
the SIF could be created to only function on the SUBJECT DEVICE,
28 which would mitigate any perceived risk to Apple iOS software as to
any other Apple device. As an alternative, the government would be
willing to test the passcodes remotely while the SUBJECT DEVICE is
in Apple's possession.

goals, and installation and operation within the SUBJECT DEVICE, in an alternative technical manner if mutually preferable.

B. The All Writs Act Permits This Order

The All Writs Act provides in relevant part that "all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law." 28 U.S.C. § 1651(a). As the Supreme Court explained, "[t]he All Writs Act is a residual source of authority to issue writs that are not otherwise covered by statute." Pennsylvania Bureau of Correction v. United States Marshals Service, 474 U.S. 34, 43 (1985). The All Writs Act permits a court, in its "sound judgment," to issue orders necessary "to achieve the rational ends of law" and "the ends of justice entrusted to it." United States v. New York Telephone Co., 434 U.S. 159, 172-3 (1977) (citations and internal quotation marks omitted). Courts must apply the All Writs Act "flexibly in conformity with these principles." Id. at 173; accord United States v. Catoggio, 698 F.3d 64, 67 (2d Cir.2012) ("[C]ourts have significant flexibility in exercising their authority under the Act.") (citation omitted).

Pursuant to the All Writs Act, the Court has the power, "in aid of a valid warrant, to order a third party to provide nonburdensome technical assistance to law enforcement officers." Plum Creek Lumber Co. v. Hutton, 608 F.2d 1283, 1289 (9th Cir. 1979) (citing United States v. New York Tel. Co., 434 U.S. 159 (1977)); see also In re U.S. for an Order Directing a Provider of Communication Services to Provide Technical Assistance to Agents of the U.S. Drug Enforcement Administration, 2015 WL 5233551 (D.P.R. August 27, 2015) (granting government's request pursuant to the All Writs Act for

1 technical assistance from provider of electronic communication
2 services to provide information, facilities, and technical
3 assistance to facilitate the consensual recording of all electronic
4 communication to and from a particular mobile phone); United States
5 v. Fricosu, 841 F.Supp.2d 1232, 1238 (D.Colo. 2012) (order issued
6 under All Writs Act requiring defendant to provide password to
7 encrypted computer seized pursuant to a search warrant). In New
8 York Telephone Co., the Supreme Court held that courts have
9 authority under the All Writs Act to issue supplemental orders to
10 third parties to facilitate the execution of search warrants. The
11 Court held that "[t]he power conferred by the Act extends, under
12 appropriate circumstances, to persons who, though not parties to the
13 original action or engaged in wrongdoing, are in a position to
14 frustrate the implementation of a court order or the proper
15 administration of justice, . . . and encompasses even those who have
16 not taken any affirmative action to hinder justice." Id. at 174.
17 In particular, the Court upheld an order directing a phone company
18 to assist in executing a pen register search warrant issued under
19 Rule 41. See id. at 171-76; see also Application of U.S. for an
20 Order Authorizing an In-Progress Trace of Wire Commc'ns over Tel.
21 Facilities (Mountain Bell), 616 F.2d 1122, 1132-33 (9th Cir. 1980)
22 (affirming district court's order compelling Mountain Bell to trace
23 telephone calls on grounds that "the obligations imposed . . . were
24 reasonable ones." (citing New York Tel. Co., 434 U.S. at 172)).

25 New York Telephone Co. also held that "Rule 41 is not limited
26 to tangible items but is sufficiently flexible to include within its
27 scope electronic intrusions authorized by a finding of probable
28 cause." 434 U.S. at 170. The Court relied upon the authority of a

1 search warrant pursuant to Rule 41 to predicate an All Writs Act
2 order commanding a utility to implement a pen register and trap and
3 trace device -- before Congress had passed a law that specifically
4 authorized pen registers by court order. Under New York Telephone
5 Co. and Mountain Bell, the All Writs Act provides authority for this
6 Court to order Apple to assist with steps necessary to perform the
7 search ordered by the warrant for the SUBJECT DEVICE.

8 Further, based on the authority given to the courts under the
9 All Writs Act, courts have issued orders, similar to the one the
10 government is seeking here, that require a manufacturer to assist in
11 accessing a cell phone's files so that a warrant may be executed as
12 originally contemplated. See, e.g., In re Order Requiring [XXX],
13 Inc. to Assist in the Execution of a Search Warrant Issued by This
14 Court by Unlocking a Cellphone, 2014 WL 5510865, at *2 (S.D.N.Y.
15 Oct. 31, 2014); see also United States v. Navarro, No. 13-CR-5525,
16 ECF No. 39 (W.D. Wa. Nov. 13, 2013). Courts have also issued All
17 Writs Act orders in furtherance of warrants in a wide variety of
18 contexts, including: ordering a defendant to produce a copy of the
19 unencrypted contents of a computer seized pursuant to a federal
20 search warrant (Fricosu, 841 F.Supp. 2d at 1238); ordering a phone
21 company to assist with a trap and trace device (Mountain Bell, 616
22 F.2d 1122, 1129 (9th Cir. 1980)); ordering a credit card company to
23 produce customer records (United States v. Hall, 583 F. Supp. 717,
24 722 (E.D. Va. 1984)); ordering a landlord to provide access to
25 security camera videotapes (In re Application of United States for
26 an Order Directing X to Provide Access to Videotapes, No. 03-89,
27 2003 WL 22053105, at *3 (D. Md. Aug. 22, 2003) (unpublished order));
28 and ordering a phone company to assist with consensual monitoring of

1 a customer's calls (In re U.S., No. 15-1242 (M), 2015 WL 5233551, at
2 *4-5 (D.P.R. Aug. 27, 2015) (unpublished order)). Because the
3 orders are typically, as here, sought in the midst of a criminal
4 investigation, they are usually obtained by way of ex parte
5 application and not noticed motion. See, e.g., New York Telephone
6 Co., 434 U.S. at 162; In re U.S., 2015 WL 5233551, at *1; In re
7 [XXX], 2014 WL 5510865, at *1; Application of U.S., 616 F.2d at
8 1122; In re Application of United States, 2003 WL 22053105, at *1.
9 The government is not aware of any case in which the government
10 obtained a Rule 41 search warrant but was denied an All Writs Act
11 Order when necessary to facilitate the execution of the warrant.⁸

12 In New York Telephone Co., the Supreme Court considered three
13 factors in concluding that the issuance of the All Writs Act order
14 to the phone company was appropriate. First, it found that the
15 phone company was not "so far removed from the underlying
16 controversy that its assistance could not be permissibly compelled."
17 Id. at 174. Second, it concluded that the order did not place an
18 undue burden on the phone company. See id. at 175. Third, it
19 determined that the assistance of the company was necessary to
20

21 ⁸ The government is also aware of multiple other unpublished
22 orders in this district and across the country (obtained by ex parte
23 application) compelling Apple to assist in the execution of a search
24 warrant by accessing the data on devices running earlier versions of
25 iOS, orders with which Apple complied. The only exception known to
26 the government is litigation pending before a Magistrate Judge in
27 the Eastern District of New York, where that court sua sponte raised
28 the issue of whether it had authority under the All Writs Act to
issue a similar order. That out-of-district litigation remains
pending without any issued orders, nor would any such order be
binding on this court. In any event, those proceedings represent a
change in Apple's willingness to access iPhones operating prior iOS
versions, not a change in Apple's technical ability. However, based
on that litigation and communications with Apple, the government
anticipates that Apple will avail itself of its ability to apply for
relief pursuant to the proposed order.

1 achieve the purpose of the warrant. See id. Each of these factors
2 supports issuance of the order directed to Apple in this case.

3 1. Apple is not "far removed" from this matter

4 First, Apple is not "so far removed from the underlying
5 controversy that its assistance could not be permissibly compelled."
6 Apple designed, manufactured and sold the SUBJECT DEVICE, and wrote
7 and owns the software that runs the phone -- which software is
8 preventing the execution of the warrant. Indeed, Apple has
9 positioned itself to be essential to gaining access to the SUBJECT
10 DEVICE or any other Apple device, and has marketed its products on
11 this basis. Apple designed and restricts access to the code for the
12 auto-erase function -- the function that makes the data on the phone
13 permanently inaccessible after multiple failed passcode attempts and
14 thus effectively prevents the government from attempting to execute
15 the search warrant without Apple's assistance. The same software
16 Apple is uniquely able to modify also controls the delays Apple
17 implemented between failed passcode attempts -- which makes the
18 process take too long to enable the access ordered by the court.
19 Especially but not only because iPhones will only run software
20 cryptographically signed by Apple, and because Apple restricts
21 access to the code of the software that creates these obstacles,
22 there is no other party that has the ability to assist the
23 government in preventing these features from obstructing the search
24 ordered by the court pursuant to the warrant.

25 Apple is also not made "far removed" by the fact that it is a
26 non-government third party. While New York Telephone Co. involved a
27 public utility, that was not the source of the holding that the All
28 Writs Act order was appropriate. New York Telephone Co. emphasized

1 that "the Company's facilities were being employed to facilitate a
2 criminal enterprise on a continuing basis," and the company's
3 noncompliance "threatened obstruction of an investigation which
4 would determine whether the Company's facilities were being lawfully
5 used." New York Telephone Co., 434 U.S. at 174. By analogy, where
6 Apple manufactured and sold a phone used by a person at the center
7 of a terrorism investigation, where it owns and licensed the
8 software used to "facilitate the criminal enterprise," where that
9 very software now must be used to enable the search ordered by the
10 warrant, compulsion of Apple is permissible under New York Telephone
11 Co. Moreover, other courts have directed All Writs Act orders based
12 on warrants to entities that are not public utilities. For example,
13 neither the credit card company in Hall nor the landlord in Access
14 to Videotapes was a public utility. See Hall, 583 F. Supp. at 722;
15 Access to Videotapes, 2003 WL 22053105, at *3. Apple's close
16 relationship to the iPhone and its software - which are by Apple's
17 design - makes compelling assistance from Apple permissible and the
18 only means of executing the warrant.

19 2. The order does not place an unreasonable burden on
20 Apple

21 Second, the order is not likely to place any unreasonable
22 burden on Apple. Where, as here, compliance with the order would
23 not require inordinate effort, and reasonable reimbursement for that
24 effort is available, no unreasonable burden can be found. New York
25 Telephone, 434 U.S. at 175 (holding that All Writs Act order was not
26 burdensome because it required minimal effort by the company,
27 provided for reimbursement for the company's efforts, and did not
28 disrupt its business operations); Mountain Bell, 616 F.2d at 1132

1 (rejecting telephone company's argument that unreasonable burden
2 would be imposed because of a drain on resources and possibility of
3 system malfunctions because the "Order was extremely narrow in
4 scope, restricting the operation to [electronic switching system]
5 facilities, excluding the use of manual tracing, prohibiting any
6 tracing technique which required active monitoring by company
7 personnel, and requiring that operations be conducted 'with a
8 minimum of interference to the telephone service'").

9 While the order in this case requires Apple to provide modified
10 software, modifying an operating system - writing software code - is
11 not an unreasonable burden for a company that writes software code
12 as part of its regular business. In fact, providers of electronic
13 communications services and remote computing services are sometimes
14 required to write code in order to gather information in response to
15 subpoenas or other process. In addition, the order is tailored for
16 this particular phone, and because it involves preparing a single
17 SIF, it presents no danger of system malfunctions or disrupting
18 business operations. As noted above, Apple designs and implements
19 all of the features discussed, writes and cryptographically signs
20 the iOS, and routinely patches security or functionality issues in
21 its operating system and releases new versions of its operating
22 system to address issues. By comparison, writing a program that
23 turns off non-encryption features that Apple was responsible for
24 writing to begin with would not be unduly burdensome.⁶

27 ⁶ It is worth noting as well that the user of the phone is now
28 dead, the user was made aware of his lack of privacy in the work
phone while alive, and the owner of the phone consents to both the
search of the phone and to Apple's assistance in this matter.

1 However, to the extent that Apple believes that compliance with
2 the order would be unreasonably burdensome, it can make an
3 application to the Court for relief prior to being compelled to
4 provide the assistance. See In re XXX, 2014 WL 5510865, at *2
5 (including in the issued All Writs Act Order a provision that states
6 that "to the extent [the manufacturer] believes that compliance with
7 this Order would be unreasonably burdensome, it may delay compliance
8 provided it makes an application to the Court for relief within five
9 business days of receipt of the Order."). The proposed order in
10 this case includes a similar directive.

11 3. Apple's assistance is necessary to effectuate the
12 warrant

13 Third, Apple's assistance is necessary to effectuate the
14 warrant. In New York Telephone Co., the Court held that the order
15 met that standard because "[t]he provision of a leased line by the
16 Company was essential to the fulfillment of the purpose - to learn
17 the identities of those connected with the gambling operation - for
18 which the pen register order had been issued." 434 U.S. at 175.
19 Here, the proposed All Writs Act order in this matter also meets
20 this standard, as it is essential to ensuring that the government is
21 able to perform the search ordered by the warrant.

22 In this case, the ability to perform the search ordered by the
23 warrant on the SUBJECT DEVICE is of particular importance. The user
24 of the phone, Farook, is believed to have caused the mass murder of
25 a large number of his coworkers and the shooting of many others, and
26 to have built bombs and hoarded weapons for this purpose. The
27 government has been able to obtain several iCloud backups for the
28 SUBJECT DEVICE, and executed a warrant to obtain all saved iCloud

1 data associated with the SUBJECT DEVICE. Evidence in the iCloud
2 account indicates that Farook was in communication with victims who
3 were later killed during the shootings perpetrated by Farook on
4 December 2, 2015, and toll records show that Farook communicated
5 with Malik using the SUBJECT DEVICE. Importantly, however, the most
6 recent backup of the iCloud data obtained by the government was
7 dated October 19, 2015, approximately one-and-a-half months before
8 the shooting. This indicates to the FBI that Farook may have
9 disabled the automatic iCloud backup function to hide evidence, and
10 demonstrates that there may be relevant, critical communications and
11 data around the time of the shooting that has thus far not been
12 accessed, may reside solely on the SUBJECT DEVICE, and cannot be
13 accessed by any other means known to either the government or Apple.

14 As noted above, assistance under the All Writs Act has been
15 compelled to provide decrypted contents of devices seized pursuant
16 to a search warrant. In Fricosu, a defendant's computer -- whose
17 contents were encrypted -- was seized, and defendant was ordered
18 pursuant to the All Writs Act to assist the government in producing
19 a copy of the unencrypted contents of the computer. 841 F.Supp. 2d
20 at 1237 ("There is little question here but that the government
21 knows of the existence and location of the computer's files. The
22 fact that it does not know the specific content of any specific
23 documents is not a barrier to production."). Here, the type of
24 assistance does not even require Apple to assist in producing the
25 unencrypted contents, the assistance is rather to facilitate the
26 FBI's attempts to test passcodes.

1 IV. CONCLUSION

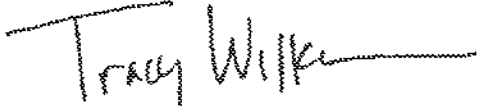
2 For the foregoing reasons, the government respectfully requests
3 that the Court order Apple to assist the FBI in the search of the
4 SUBJECT DEVICE as detailed in the proposed order.

5
6 Dated: February 16, 2016

Respectfully submitted,

7 EILEEN M. DECKER
United States Attorney

8 PATRICIA A. DONAHUE
9 Assistant United States Attorney
Chief, National Security Division

10
11 
12 TRACY L. WILKISON
13 ALLEN W. CHIU
Assistant United States Attorneys

14 Attorneys for Applicant
15 UNITED STATES OF AMERICA
16
17
18
19
20
21
22
23
24
25
26
27
28

1 DECLARATION OF CHRISTOPHER PLUHAR

2 I, Christopher Pluhar, being duly sworn, declare and state as
3 follows:

4 I. INTRODUCTION

5 1. I am a Supervisory Special Agent ("SSA") with the Federal
6 Bureau of Investigation ("FBI"), and Director of the Orange County
7 Regional Computer Forensics Laboratory, Orange, California
8 ("OCRCFL"). The OCRCFL is a state of the art computer forensics
9 laboratory comprised of task force officers from 15 agencies in
10 Orange, Los Angeles, San Bernardino, and Riverside Counties. The
11 laboratory specializes in the archival, preservation, and analysis
12 of items of digital evidence, including computers, mobile devices,
13 removable media (thumb drives, CDs etc) and Audio/Video equipment.

14 2. I have been a computer forensic examiner for the FBI since
15 2001, have attended 700+ hours of specialized training in
16 computer/device forensics, and have certifications to conduct
17 forensic analysis on Windows, Macintosh, and Linux/Unix systems, as
18 well as mobile devices and cell phones. I have been the Director of
19 the OCRCFL since November of 2013.

20 3. I have consulted extensively with the FBI's Cryptographic
21 and Electronic Analysis Unit ("CEAU") in this matter, and bring
22 their experience to bear in this declaration.

23 II. PURPOSE OF DECLARATION

24 4. This declaration is made in support of an application for
25 an order by the Court compelling Apple Inc. ("Apple") to assist the
26 FBI in its effort to search of a cellular telephone, Apple make:
27 iPhone 5C, Model: A1532, P/N:MGFG2LL/A, S/N:FFMNQ3MTG2DJ,
28 IMEI:358820052301412, on the Verizon Network ("SUBJECT DEVICE").

1 III. SEIZURE AND EXAMINATION OF SUBJECT DEVICE

2 5. The SUBJECT DEVICE was seized pursuant to the search
3 warrant in Case No. ED 15-0451M, issued by the Honorable David T.
4 Bristow, United States Magistrate Judge, on December 3, 2015. The
5 SUBJECT DEVICE was found inside of the SUBJECT VEHICLE identified in
6 the warrant. The underlying search warrant is attached hereto as
7 Exhibit 1 and incorporated by reference.

8 6. I know based on my participation in this investigation and
9 conversations with other involved agents and San Bernardino County
10 Information Technology personnel, that the search warrant arose out
11 of an investigation into the December 2, 2015 shooting death of 14
12 people, and the shooting and injuring of 22 others, at the Inland
13 Regional Center ("IRC") in San Bernardino, California, and the
14 participation by Syed Rizwan Farook ("Farook") and his wife Tafsheen
15 Malik ("Malik") in that crime. Subsequent to the search warrant at
16 issue, the FBI has obtained numerous warrants to search the digital
17 devices and online accounts of Farook and Malik. Through those
18 searches the FBI has discovered, for example, that on December 2,
19 2015, at approximately 11:14 a.m., a post on a Facebook page
20 associated with Malik stated, "We pledge allegiance to Khalifa bu
21 bkr al bhaghdadi al guraishi," referring to Abu Bakr Al Baghdadi,
22 the leader of Islamic State of Iraq and the Levant ("ISIL"), also
23 referred to as the Islamic State ("IS"), or the Islamic State of
24 Iraq and al-sham ("ISIS"), or Daesh. ISIL, formerly known as Al-
25 Qa'ida in Iraq ("AQI"), has been designated a foreign terrorist
26 organization by the United States Department of State and has been
27 so designated since December 2004. Farook and Malik died later that
28 same day in a shoot-out with law enforcement.

1 7. The SUBJECT DEVICE is owned by Farook's employer at the
2 San Bernardino County Department of Public Health ("SBCDPH"), and
3 was assigned to, and used by, Farook as part of his employment.
4 While the SBCDPH does not have access to the passcode to the phone,
5 it has given its consent to the search of it and to Apple's
6 assistance with that search.

7 8. The SUBJECT DEVICE is "locked" or secured with a numeric
8 passcode. I have been very involved in the attempts to gain access
9 to the locked phone and comply with the search warrant. With the
10 consent of the SBCDPH, I and other agents have been able to obtain
11 several iCloud backups for the SUBJECT DEVICE, and I am aware that a
12 warrant was executed to obtain from Apple all saved iCloud data
13 associated with the SUBJECT DEVICE. I know from speaking with other
14 FBI agents that evidence in the iCloud account indicates that Farook
15 was in communication with victims who were later killed during the
16 shootings perpetrated by Farook on December 2, 2015. In addition,
17 toll records show that Farook communicated with Malik using the
18 SUBJECT DEVICE between July and November 2015, but this information
19 is not found in the backup iCloud data. Importantly, the most
20 recent backup is dated October 19, 2015, which indicates to me that
21 Farook may have disabled the automatic iCloud backup feature
22 associated with the SUBJECT DEVICE. I believe this because I have
23 been told by SBCDPH that it was turned on when it was given to him,
24 and the backups prior to October 19, 2015 were with almost weekly
25 regularity. I further believe that there may be relevant, critical
26 communications and data on the SUBJECT DEVICE around the time of the
27 shooting which has thus far not been accessed, may reside solely on
28 the SUBJECT DEVICE, and cannot be accessed by any other means known

1 to either the government or Apple. In addition, I have personally
2 examined two other mobile devices belonging to Farook that were
3 physically destroyed and discarded in a dumpster behind the Farook
4 residence.

5 9. I have explored other means of obtaining this information
6 with employees of Apple and with technical experts at the FBI, and
7 we have been unable to identify any other methods feasible for
8 gaining access to the currently inaccessible data stored within the
9 SUBJECT DEVICE.

10 IV. REQUESTED ASSISTANCE

11 10. I know based on my training and experience, knowledge of
12 this case and review of Apple's publicly available information that
13 the SUBJECT DEVICE is an iPhone 5c that was designed, manufactured,
14 and sold by Apple. Apple also wrote and owns the software operating
15 system marketed under the name of "iOS," and thus is the owner of
16 the operating system for the phone at issue. Apple's software
17 licensing agreement specifies that its software is "licensed, not
18 sold," and otherwise prohibits users from transferring any ownership
19 of the iOS software.

20 11. Apple strictly controls the hardware and software that is
21 used to turn on and run its phones. According to Apple's "white
22 papers" and other publicly available information about the security
23 of its iOS programs, Apple has designed its mobile device hardware
24 as well as its operating system software to only permit and run
25 software that has been "signed" cryptographically by Apple using its
26 own proprietary encryption methods. Apple has also added hardware-
27 enforced features to the A6 processor found in the iPhone 5C which
28 verifies software using Apple's cryptographic signature, ensuring

1 that Apple devices can only run verified/signed software during the
2 booting process (when the phone is being turned on). These features
3 prevent the government from running any other software on the
4 SUBJECT DEVICE to attempt to recover data.

5 12. In addition, an iPhone 5c is encrypted by a combination of
6 two components - one user-determined passcode, and one unique 256-
7 bit Advanced Encryption Standard ("AES") key (referred to as a
8 "UID") fused into the phone itself during manufacture. Both
9 passcode components are required in combination for the phone to
10 decrypt its contents. When a user inputs the user-determined
11 passcode, the phone conducts a complex calculation as determined by
12 Apple's software (and unknown to the government) which combines the
13 UID with the user passcode. If the result is accurate, the data is
14 decrypted.

15 13. If one does not know the user-determined passcode, it is
16 possible, although time-consuming, to manually input passcodes one
17 at a time until the passcode is determined. Apple, however, has
18 also designed and written code for additional non-encryption-based
19 features which the government cannot overcome on its own. First,
20 Apple has designed a non-encryption, auto-erase function as part of
21 its iOS, which destroys encryption key material required for
22 decryption, and hence renders the contents of the device incapable
23 of being decrypted after ten consecutive incorrect passcode
24 attempts. If this erase function is enabled, iOS will instantly,
25 irrecoverably, and without warning erase the encryption keys
26 necessary for accessing stored data. Because iOS software must be
27 cryptographically signed by Apple, only Apple is able to modify the
28 iOS software to change the setting or prevent execution of the

1 function. There is no way to know by examining the outside of the
2 phone whether or not this function has been turned on in the SUBJECT
3 DEVICE, although, in this instance, I suspect that it has because I
4 am told by an employee of SBCDPH that the SUBJECT DEVICE was
5 provided to Farook with the auto-erase function turned on, and I
6 know from my review of the most recent backup from the iCloud that
7 it showed the function turned on.

8 14. Relatedly, Apple has designed and written code for another
9 non-encryption based feature in that its iOS operating system is
10 coded to invoke time delays which escalate after repeated,
11 unsuccessful passcode entries. This means that after each failed
12 passcode entry, the user must wait a period of time before another
13 attempt can be made. From Apple documentation and testing, the time
14 delays for the iPhone 5C are invoked by Apple software upon failed
15 login attempts. Apple documentation states that the software
16 invokes no delay for the first four attempts; a 1-minute delay after
17 the fifth attempt; a 5-minute delay after the sixth attempt; a
18 fifteen minute delays after the seventh and eight attempt; and a 1-
19 hour delay after the ninth attempt. Additional wait times can also
20 be added into the software.

21 15. In order to allow the government to perform the search
22 ordered in the warrant, and the ability to test passcodes to decrypt
23 the SUBJECT DEVICE without unnecessary delay or fear that the data
24 subject to search under the warrant would be rendered permanently
25 inaccessible, the government requests that Apple be ordered to
26 provide the FBI with a signed iPhone Software file, recovery bundle,
27 or other Software Image File ("SIF") that can be loaded onto the
28 SUBJECT DEVICE. The SIF would load and run from Random Access

1 Memory ("RAM") and would not modify the iOS on the actual phone, the
2 user data partition or system partition on the device's flash
3 memory. The SIF would be coded by Apple with a unique identifier of
4 the phone so that the SIF would only load and execute on the SUBJECT
5 DEVICE. Since Apple's software currently has the capability to
6 query hardware for unique identifiers (serial numbers, ECID, IMEI,
7 etc.), the SIF could be created to only function on the SUBJECT
8 DEVICE, which would mitigate any perceived security risk to Apple
9 iOS software. The SIF would be loaded via Device Firmware Upgrade
10 ("DFU") mode, recovery mode, or other applicable mode available to
11 the FBI. In addition, Apple could run the SIF from within its
12 facility, allowing passcodes to be tested electronically via remote
13 network connection.

14 16. Once active on the SUBJECT DEVICE, the SIF would have
15 three important functions: (1) the SIF would bypass or disable the
16 auto-erase function whether or not it has been enabled on the
17 SUBJECT DEVICE, meaning that multiple attempts at the passcode could
18 be made without fear that the data subject to search under the
19 warrant would be rendered permanently inaccessible; (2) the SIF
20 would enable the FBI to submit passcodes to the SUBJECT DEVICE for
21 testing electronically via the physical device port, Bluetooth, Wi-
22 Fi, or other protocol available on the SUBJECT DEVICE (meaning that
23 the attempts at the passcode would not have to be manually typed on
24 the phone's screen), or alternately, Apple could be given the phone
25 as is done when Apple recovers data from earlier iOS versions, but
26 provide the government remote access to the SUBJECT DEVICE through a
27 computer allowing the government to conduct passcode recovery
28 analysis. This would allow the government to conduct the analysis

1 without Apple actually providing the government with the SIF; and
2 (3) the SIF would not introduce any additional delay between
3 passcode attempts beyond what is incurred by the Apple hardware.

4 17. Based on my (and the CEAU's) review of available
5 information about Apple's programs, Apple has the technological
6 capability of providing this software without it being an undue
7 burden. Apple routinely patches security or functionality issues in
8 its iOS operating system and releases new versions of its operating
9 system to address issues. I know from my training and experience,
10 and that of my fellow agents, that providers of electronic
11 communications services and remote computing services sometimes must
12 write code in order to gather the information necessary to respond
13 to subpoenas and other process, and that this is not a large burden.

14 18. However, in an abundance of caution, the government also
15 requests that the order permit Apple to satisfy the three goals of
16 the SIF and the loading of the SIF onto the SUBJECT DEVICE in an
17 alternative technical manner if mutually preferable.

18 I declare under penalty of perjury that the foregoing is true
19 and correct to the best of my knowledge and belief.

20 Executed on February 16, 2016, Riverside, California.

21
22
23 
24 Christopher Pluhar
25 FBI Supervisory Special Agent
26
27
28

EXHIBIT 1

ORIGINAL

UNDER SEAL

UNITED STATES DISTRICT COURT

for the
Central District of California

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Black Lexus IS300 California License Plate #5KGD203,
handicap placard 360466F, Vehicle Identification Number
JTHBD192X50094434

ED 15-0451M

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the Central District of California
(Identify the person or describe the property to be searched and give its location):

See Attachment A-2

The person or property to be searched, described above, is believed to conceal (Identify the person or describe the
property to be seized):

See Attachment B

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or
property.

YOU ARE COMMANDED to execute this warrant on or before 14 days from the date of its issuance
(not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10 p.m. ☒ at any time in the day or night as I find reasonable cause has been
established.

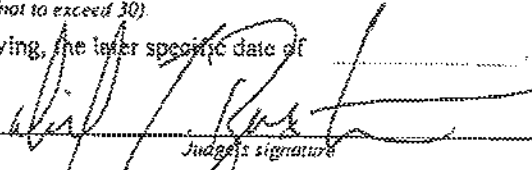
Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property
taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the
place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an
inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge
on duty at the time of the return through a filing with the Clerk's Office.
(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay
of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be
searched or seized (check the appropriate box) ☐ for _____ days (not to exceed 30)

☐ until, the facts justifying, the later specific date of _____

Date and time issued: 12/3/15, 2:27 A.M.



Judge's signature

City and state: Riverside, California

David T. Bristow, U.S. Magistrate Judge

Printed name and title

<i>Return</i>		
<i>Case No.:</i>	<i>Date and time warrant executed:</i>	<i>Copy of warrant and inventory left with:</i>
<i>Inventory made in the presence of:</i>		
<i>Inventory of the property taken and name of any person(s) seized:</i> (Please provide a description that would be sufficient to demonstrate that the items seized fall within the items authorized to be seized pursuant to the warrant (e.g., type of documents, as opposed to "miscellaneous documents") as well as the approximate volume of any documents seized (e.g., number of boxes). If reference is made to an attached description of property, specify the number of pages to the attachment and any case number appearing thereon.)		
<i>Certification (by officer present during the execution of the warrant)</i>		
<i>I declare under penalty of perjury that I am an officer who executed this warrant and that this inventory is correct and was returned along with the original warrant to the designated judge through a filing with the Clerk's Office.</i>		
<i>Date:</i> _____ _____ <i>Executing officer's signature</i> _____ <i>Printed name and title</i>		

ATTACHMENT A-2

PROPERTY TO BE SEARCHED

Black Lexus IS300 California license plate #5KGD203, handicap
placard 360466F, vehicle identification number
JTHBD192X50094434.

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of (1) 18 U.S.C. § 844(d) (Transportation or Receipt of Explosive Devices with the Intent to Injure or Kill); (2) 18 U.S.C. § 844(i) (Attempted Destruction by Explosives of Any Building, Person, or Property); and (3) 18 U.S.C. § 844(n) (Conspiracy):

a. Explosives, smokeless powder, black powder, gunpowder, or any other item that can be pipes, and wires;

b. Pipes and any items that may cause fragmentation;

c. Initiating devices to include burning fuse, hobby fuse, blasting caps, manual or electrical timers, dry cell batteries, electrical wire, alligator clips, electrical tape of assorted colors commonly used to secure exposed electrical wiring;

d. Books related to the construction of explosives;

e. Tools used in the construction of explosives such as include hand held vise grips, table mounted vise grips, pipe cutters, electrical; and non-electrical drills and drill bits.

f. Address and/or telephone books, telephones, pagers, answering machines, customer lists, and any papers reflecting names, addresses, telephone numbers, pager numbers,

fax numbers and/or identification numbers of sources of supply of explosives;

g. No more than 5 documents and records, including electronic mail and electronic messages, reflecting the ownership, occupancy, possession, or control of the SUBJECT LOCATION, including lease/rental agreements, rent receipts, registration documents, bank records, utility bills, telephone bills, other addressed envelopes, and correspondence;

h. Any digital device used to facilitate the above-listed violations and forensic copies thereof.

i. With respect to any digital device used to facilitate the above-listed violations or containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software,

as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created,

modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICES

4. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) to an appropriate law enforcement laboratory or similar facility to be searched at

that location. The search team shall complete the search as soon as is practicable but not to exceed 60 days from the date of execution of the warrant. If additional time is needed, the government may seek an extension of this time period from the Court on or before the date by which the search was to have been completed.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

c. When searching a digital device pursuant to the specific search protocols selected, the search team shall make and retain notes regarding how the search was conducted pursuant to the selected protocols.

d. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

e. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

f. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

g. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of items to be seized, the government may retain forensic copies of the digital device but may not access them (after the time for searching the device has expired) absent further court order.

h. The government may retain a digital device itself until further order of the Court or one year after the

conclusion of the criminal investigation or case (whichever is latest), only if the device is determined to be an instrumentality of an offense under investigation or the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending). Otherwise, the government must return the device.

1. Notwithstanding the above, after the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

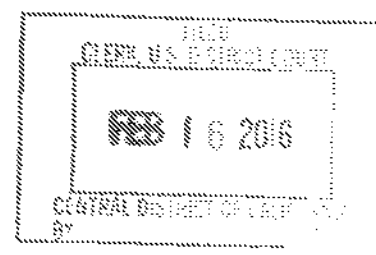
f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

6. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

7. The government is allowed to share the information obtained from this search (to include copies of digital media) with any government agency investigating, or aiding in the investigation of, this case or related matters.

CONFIDENTIAL



EILEEN M. DECKER
United States Attorney
PATRICIA A. DONAHUE
Assistant United States Attorney
Chief, National Security Division
TRACY L. WILKISON (California Bar No. 184948)
Assistant United States Attorney
Chief, Cyber and Intellectual Property Crimes Section
ALLEN W. CHIU (California Bar No. 240516)
Assistant United States Attorney
Terrorism and Export Crimes Section
1500 United States Courthouse
312 North Spring Street
Los Angeles, California 90012
Telephone: (213) 894-0622/2435
Facsimile: (213) 894-8601
Email: Tracy.Wilkison@usdoj.gov
Allen.Chiu@usdoj.gov
Attorneys for Applicant
UNITED STATES OF AMERICA

2016 FEB 16 11:00 AM
FBI - LOS ANGELES
RECEIVED

UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA

IN THE MATTER OF THE SEARCH OF
AN APPLE IPHONE SEIZED DURING
THE EXECUTION OF A SEARCH
WARRANT ON A BLACK LEXUS IS300,
CALIFORNIA LICENSE PLATE
3SKGD203

No. ED 15-0451M
[PROPOSED] ORDER COMPELLING APPLE,
INC. TO ASSIST AGENTS IN SEARCH

This matter is before the Court pursuant to an application pursuant to the All Writs Act, 28 U.S.C. § 1651, by Assistant United States Attorneys Tracy Wilkison and Allen Chiu, requesting an order directing Apple Inc. ("Apple") to assist law enforcement agents in enabling the search of a digital device seized in the course of a previously issued search warrant in this matter.

For good cause shown, IT IS HEREBY ORDERED that:

1. Apple shall assist in enabling the search of a cellular telephone, Apple make: iPhone 5C, Model: A1532, P/N:MGFG2LL/A, S/N:FFMNQ3MTG2DJ, IMEI:358820052301412, on the Verizon Network, (the

1 "SUBJECT DEVICE") pursuant to a warrant of this Court by providing
2 reasonable technical assistance to assist law enforcement agents in
3 obtaining access to the data on the SUBJECT DEVICE.

4 2. Apple's reasonable technical assistance shall accomplish
5 the following three important functions: (1) it will bypass or
6 disable the auto-erase function whether or not it has been enabled;
7 (2) it will enable the FBI to submit passcodes to the SUBJECT DEVICE
8 for testing electronically via the physical device port, Bluetooth,
9 Wi-Fi, or other protocol available on the SUBJECT DEVICE; and (3) it
10 will ensure that when the FBI submits passcodes to the SUBJECT
11 DEVICE, software running on the device will not purposefully
12 introduce any additional delay between passcode attempts beyond what
13 is incurred by Apple hardware.

14 3. Apple's reasonable technical assistance may include, but is
15 not limited to: providing the FBI with a signed iPhone Software
16 file, recovery bundle, or other Software Image File ("SIF") that can
17 be loaded onto the SUBJECT DEVICE. The SIF will load and run from
18 Random Access Memory ("RAM") and will not modify the iOS on the
19 actual phone, the user data partition or system partition on the
20 device's flash memory. The SIF will be coded by Apple with a unique
21 identifier of the phone so that the SIF would only load and execute
22 on the SUBJECT DEVICE. The SIF will be loaded via Device Firmware
23 Upgrade ("DFU") mode, recovery mode, or other applicable mode
24 available to the FBI. Once active on the SUBJECT DEVICE, the SIF
25 will accomplish the three functions specified in paragraph 2. The
26 SIF will be loaded on the SUBJECT DEVICE at either a government
27 facility, or alternatively, at an Apple facility; if the latter,
28 Apple shall provide the government with remote access to the SUBJECT

1 DEVICE through a computer allowing the government to conduct passcode
2 recovery analysis.

3 4. If Apple determines that it can achieve the three functions
4 stated above in paragraph 2, as well as the functionality set forth
5 in paragraph 3, using an alternate technological means from that
6 recommended by the government, and the government concurs, Apple may
7 comply with this Order in that way.

8 5. Apple shall advise the government of the reasonable cost of
9 providing this service.

10 6. Although Apple shall make reasonable efforts to maintain
11 the integrity of data on the SUBJECT DEVICE, Apple shall not be
12 required to maintain copies of any user data as a result of the
13 assistance ordered herein. All evidence preservation shall remain
14 the responsibility of law enforcement agents.

15 7. To the extent that Apple believes that compliance with this
16 Order would be unreasonably burdensome, it may make an application to
17 this Court for relief within five business days of receipt of the
18 Order.

19
20
21
22 DATED: FEB 16 2016

SHERI PYM

UNITED STATES MAGISTRATE JUDGE

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Friday, February 19, 2016 4:15 PM
To: Raj, Kiran (ODAG) (JMD)
Subject: never mind - just found the filing on line. Sorry to bother

Raj, Kiran (ODAG)

From: Raj, Kiran (ODAG)
Sent: Friday, February 19, 2016 5:16 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: never mind - just found the filing on line. Sorry to bother

Dan -

I have been thinking about a way to encapsulate the unfairness of some of the rhetoric against the FBI as of late. What do you think about this response to the question of "aren't you seeking a backdoor"?

[REDACTED]

b5 Per DOJ/OIP

Hope you are doing well -

Kiran

From: Richman, Daniel C. (DO) (OGA) [mailto:[REDACTED]]
Sent: Friday, February 19, 2016 4:15 PM
To: Raj, Kiran (ODAG)
Subject: never mind - just found the filing on line. Sorry to bother

b7E -3

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Friday, February 19, 2016 5:45 PM
To: Raj, Kiran (ODAG)
Subject: RE: never mind - just found the filing on line. Sorry to bother

It is indeed annoying. As a general matter, our GD mantra has been that the "backdoor" trope is totally inapposite as it suggests both that the govt is doing something sneaky and that it has a particular intervention in mind. Neither is true. When the govt usually seeks information from reputable businesses, it usually takes pains to avoid interfering with business operations or even specifying the way evidence should be obtained. It just presents judicial authorization and asks for what it's legally entitled to. All we want is the ability to get plain text -- something that most business can provide, because it suits their interest to have that access. [REDACTED]

b5 -1

[REDACTED] We don't want back doors, we want to walk in thru the same door the company kept for itself.

[REDACTED]

If a house has boarded up, and agents have a search warrant and the owner has a key to the window (that agents can climb thru), can't we demand the key? (I hate this stupid metaphor game)

From: Raj, Kiran (ODAG) [Kiran.Raj@usdoj.gov]
Sent: Friday, February 19, 2016 5:15 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: never mind - just found the filing on line. Sorry to bother

Dan -

I have been thinking about a way to encapsulate the unfairness of some of the rhetoric against the FBI as of late. What do you think about this response to the question of "aren't you seeking a backdoor"?

[REDACTED]

b5 Per DOJ/OIP

Hope you are doing well -

FBI 18-CV-1833-5870

Kiran

From: Richman, Daniel C. (DO) (OGA) [mailto:[\[REDACTED\]](#)]
Sent: Friday, February 19, 2016 4:15 PM
To: Raj, Kiran (ODAG)
Subject: never mind - just found the filing on line. Sorry to bother

b7E -3

Oconnell, Sasha C. (DO) (FBI)

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Wednesday, February 24, 2016 4:46 PM
To: Richman, Daniel C. (DO) (OGA)
Cc: Raj, Kiran (ODAG) (JMD)
Subject: talking tonight

Ok! So at 6pm ABC news is running an exclusive Tim Cook interview (and we hear there will be a gov official response!). Kiran is going to come here to watch it and then call you if that works?

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Wednesday, February 24, 2016 5:41 PM
To: Oconnell, Sasha C. (DO) (FBI)
Cc: Raj, Kiran (ODAG) (JMD)
Subject: RE: talking tonight

sounds good. I'll be working in my office

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Wednesday, February 24, 2016 4:45 PM
To: Richman, Daniel C. (DO) (OGA)
Cc: Raj, Kiran (ODAG) (JMD)
Subject: talking tonight

Ok! So at 6pm ABC news is running an exclusive Tim Cook interview (and we hear there will be a gov official response!). Kiran is going to come here to watch it and then call you if that works?

Raj, Kiran (ODAG)

From: Raj, Kiran (ODAG)
Sent: Wednesday, February 24, 2016 7:07 PM
To: Richman, Daniel C. (DO) (OGA); Oconnell, Sasha C. (DO) (FBI)
Subject: RE: talking tonight

Dan -

Sorry for the delay. Still up for talking? If so, what is the best number to use?

Kiran

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

From: Richman, Daniel C. (DO) (OGA) [mailto:]
Sent: Wednesday, February 24, 2016 5:41 PM
To: Oconnell, Sasha C. (DO) (FBI)
Cc: Raj, Kiran (ODAG)
Subject: RE: talking tonight

b7E -3

sounds good. I'll be working in my office

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Wednesday, February 24, 2016 4:45 PM
To: Richman, Daniel C. (DO) (OGA)
Cc: Raj, Kiran (ODAG) (JMD)
Subject: talking tonight

Ok! So at 6pm ABC news is running an exclusive Tim Cook interview (and we hear there will be a gov official response!). Kiran is going to come here to watch it and then call you if that works?

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Wednesday, February 24, 2016 7:12 PM
To: Raj, Kiran (ODAG)
Subject: RE: talking tonight

office pls

b6 -4
b7C -4

From: Raj, Kiran (ODAG) [Kiran.Raj@usdoj.gov]
Sent: Wednesday, February 24, 2016 7:07 PM
To: Richman, Daniel C. (DO) (OGA); Oconnell, Sasha C. (DO) (FBI)
Subject: RE: talking tonight

Dan -

Sorry for the delay. Still up for talking? If so, what is the best number to use?

Kiran

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

From: Richman, Daniel C. (DO) (OGA) [mailto:]
Sent: Wednesday, February 24, 2016 5:41 PM
To: Oconnell, Sasha C. (DO) (FBI)
Cc: Raj, Kiran (ODAG)
Subject: RE: talking tonight

b7E -3

sounds good. I'll be working in my office

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Wednesday, February 24, 2016 4:45 PM
To: Richman, Daniel C. (DO) (OGA)
Cc: Raj, Kiran (ODAG) (JMD)
Subject: talking tonight

Ok! So at 6pm ABC news is running an exclusive Tim Cook interview (and we hear there will be a gov official response!). Kiran is going to come here to watch it and then call you if that works?

Raj, Kiran (ODAG)

From: Raj, Kiran (ODAG)
Sent: Wednesday, February 24, 2016 8:47 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: talking tonight

Dan -

It was nice to chat (as always). Here is the NYT Article that I mentioned: <http://www.nytimes.com/1997/10/16/opinion/l-fbi-and-encryption-628255.html>

Kiran

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

From: Richman, Daniel C. (DO) (OGA) [mailto:
Sent: Wednesday, February 24, 2016 7:12 PM
To: Raj, Kiran (ODAG)
Subject: RE: talking tonight

b6 -4
b7C -4
b7E -3

office pls

From: Raj, Kiran (ODAG) [Kiran.Raj@usdoj.gov]
Sent: Wednesday, February 24, 2016 7:07 PM
To: Richman, Daniel C. (DO) (OGA); Oconnell, Sasha C. (DO) (FBI)
Subject: RE: talking tonight

Dan -

Sorry for the delay. Still up for talking? If so, what is the best number to use?

Kiran

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

From: Richman, Daniel C. (DO) (OGA) [mailto:
Sent: Wednesday, February 24, 2016 5:41 PM
To: Oconnell, Sasha C. (DO) (FBI)
Cc: Raj, Kiran (ODAG)
Subject: RE: talking tonight

b7E -3

sounds good. I'll be working in my office

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Wednesday, February 24, 2016 4:45 PM
To: Richman, Daniel C. (DO) (OGA)

FBI 18-CV-1833-5960

Cc: Raj, Kiran (ODAG) (JMD)

Subject: talking tonight

Ok! So at 6pm ABC news is running an exclusive Tim Cook interview (and we hear there will be a gov official response!). Kiran is going to come here to watch it and then call you if that works?

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Thursday, February 25, 2016 11:43 AM
To: Raj, Kiran (ODAG)
Subject: RE: talking tonight

Gosh, I remember this. I feel very old

From: Raj, Kiran (ODAG) [Kiran.Raj@usdoj.gov]
Sent: Wednesday, February 24, 2016 8:46 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: RE: talking tonight

Dan -

It was nice to chat (as always). Here is the NYT Article that I mentioned: <http://www.nytimes.com/1997/10/16/opinion/l-fbi-and-encryption-628255.html>

Kiran

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

From: Richman, Daniel C. (DO) (OGA) [mailto:]
Sent: Wednesday, February 24, 2016 7:12 PM
To: Raj, Kiran (ODAG)
Subject: RE: talking tonight

b6 -4
b7C -4
b7E -3

office pls

From: Raj, Kiran (ODAG) [Kiran.Raj@usdoj.gov]
Sent: Wednesday, February 24, 2016 7:07 PM
To: Richman, Daniel C. (DO) (OGA); Oconnell, Sasha C. (DO) (FBI)
Subject: RE: talking tonight

Dan -

Sorry for the delay. Still up for talking? If so, what is the best number to use?

Kiran

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

From: Richman, Daniel C. (DO) (OGA) [mailto:]
Sent: Wednesday, February 24, 2016 5:41 PM
To: Oconnell, Sasha C. (DO) (FBI)
Cc: Raj, Kiran (ODAG)
Subject: RE: talking tonight

b7E -3

sounds good. I'll be working in my office

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Wednesday, February 24, 2016 4:45 PM
To: Richman, Daniel C. (DO) (OGA)
Cc: Raj, Kiran (ODAG) (JMD)
Subject: talking tonight

Ok! So at 6pm ABC news is running an exclusive Tim Cook interview (and we hear there will be a gov official response!). Kiran is going to come here to watch it and then call you if that works?

Oconnell, Sasha C. (DO) (FBI)

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Monday, February 29, 2016 6:46 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: Fwd: Orenstein Opinion
Attachments: [29] ORDER denying motion.pdf; ATT00001.htm

----- Original message -----

From: "Raj, Kiran (ODAG)" <Kiran.Raj@usdoj.gov>
Date: 02/29/2016 5:25 PM (GMT-05:00)
To: "Baker, James A. (OGC) (FBI)" [REDACTED]
Cc: "Oconnell, Sasha C. (DO) (FBI)" [REDACTED] "Anderson, Trisha B.(OGC) (FBI)"
[REDACTED]
Subject: Fwd: Orenstein Opinion

b7E -3

Sent from my iPhone

b5 Per EOUSA
b6 Per DOJ/CRM and EOUSA
b7C Per DOJ/CRM

Begin forwarded message:

From: "Komatireddy, Saritha (USANYE)" [REDACTED]
Date: February 29, 2016 at 5:12:39 PM EST
To: "Raj, Kiran (ODAG)" <kraj@jmd.usdoj.gov><mailto:kraj@jmd.usdoj.gov>>, "Bitkower, David" [REDACTED]@CRM.USDOJ.GOV<mailto:[REDACTED]@CRM.USDOJ.GOV>>, "Downing, Richard" [REDACTED]@CRM.USDOJ.GOV<mailto:[REDACTED]@CRM.USDOJ.GOV>>, "Lynch, John" [REDACTED]@CRM.USDOJ.GOV<mailto:[REDACTED]@CRM.USDOJ.GOV>>, "Stawasz, Michael" [REDACTED]@CRM.USDOJ.GOV<mailto:[REDACTED]@CRM.USDOJ.GOV>>, "Judish, Nathan" [REDACTED]@CRM.USDOJ.GOV<mailto:[REDACTED]@CRM.USDOJ.GOV>>, "Hosid, Jared" [REDACTED]@CRM.USDOJ.GOV<mailto:[REDACTED]@CRM.USDOJ.GOV>>, "Pierce, Emily (OPA)" [REDACTED]@CRM.USDOJ.GOV<mailto:[REDACTED]@CRM.USDOJ.GOV>>
<epierce@jmd.usdoj.gov><mailto:epierce@jmd.usdoj.gov>>
Cc: "Gatta, James (USANYE)" [REDACTED], "DuCharme, Seth (USANYE)" [REDACTED], "Tucker, Richard (USANYE)" [REDACTED], "Elbert, Lauren (USANYE)" [REDACTED], "Kabrawala, Ameet (USANYE)" [REDACTED], "Jager, Hilary (USANYE)" [REDACTED]
Subject: [REDACTED]

b5 Per EOUSA

FBI 18-CV-1833-6099

Saritha Komatireddy
Assistant United States Attorney
United States Attorney's Office
Eastern District of New York
271 Cadman Plaza East
Brooklyn, New York 11201
Tel: 718-254-6054
Fax: 718-254-6076
Email

b6 Per EOUSA

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

-----X
IN RE ORDER REQUIRING APPLE, INC.
TO ASSIST IN THE EXECUTION OF A
SEARCH WARRANT ISSUED BY THIS
COURT.
-----X

MEMORANDUM
AND ORDER

15-MC-1902 (JO)

JAMES ORENSTEIN, Magistrate Judge:

The government seeks an order requiring Apple, Inc. ("Apple") to bypass the passcode security on an Apple device. It asserts that such an order will assist in the execution of a search warrant previously issued by this court, and that the All Writs Act, 28 U.S.C. § 1651(a) (the "AWA"), empowers the court to grant such relief. Docket Entry ("DE") 1 (Application). For the reasons set forth below, I conclude that under the circumstances of this case, the government has failed to establish either that the AWA permits the relief it seeks or that, even if such an order is authorized, the discretionary factors I must consider weigh in favor of granting the motion. More specifically, the established rules for interpreting a statute's text constrain me to reject the government's interpretation that the AWA empowers a court to grant any relief not outright prohibited by law. Under a more appropriate understanding of the AWA's function as a source of residual authority to issue orders that are "agreeable to the usages and principles of law," 28 U.S.C. § 1651(a), the relief the government seeks is unavailable because Congress has considered legislation that would achieve the same result but has not adopted it. In addition, applicable case law requires me to consider three factors in deciding whether to issue an order under the AWA: the closeness of Apple's relationship to the underlying criminal conduct and government investigation; the burden the requested order would impose on Apple; and the necessity of imposing such a burden on Apple. As explained below, after reviewing the facts in the record and the parties' arguments, I conclude that none of those factors justifies imposing on Apple the obligation to assist the government's investigation against its will. I therefore deny the motion.

I. Background

On June 6, 2014, a magistrate judge of this court granted the government's applications for a warrant to search the Queens, New York residence of Jun Feng ("Feng"), whom it suspected of involvement in drug trafficking, as well as for warrants to arrest Feng and other suspected coconspirators. *United States v. The premises known and described as 41-21 149th Street, 1st Fl., Queens, NY*, 14-MJ-0530 (MDG), DE 2 (search warrant) (sealed); *United States v. Shu Yong Yang, et al.*, 14-CR-0387 (MKB), DE 1 (complaint) & DE 2 (arrest warrants). Feng was arrested on June 11, 2014, and initially ordered detained; he was subsequently released on conditions on July 18, 2014. *Yang*, DE 25 (minute entry); DE 26 (detention order); DE 50 (minute order reflecting release). On July 9, 2014, a grand jury sitting in this district issued an indictment accusing Feng and four other named defendants, together with unnamed others, of conspiracy to traffic in methamphetamine. *See Yang*, DE 47 ¶ 2.

In executing the warrant to search Feng's residence, agents of the United States Drug Enforcement Agency ("DEA") properly seized several mobile devices, including Feng's mobile telephone. *See Govt. II* at 5.¹ As agents later learned, that telephone was an iPhone 5s that used Apple's iOS 7 for its operating system.² *See id.*; *Tr.* at 7.³

¹ To the extent that the Application also constitutes the government's initial memorandum in support of its request for relief, *see id.* at 2, I will alternatively cite it as "Govt. I." I cite other sources of the parties' arguments as follows. *See* DE 11 (Apple's initial memorandum in partial opposition) ("Apple I"); DE 15 (government's reply) ("Govt. II"); DE 16 (Apple's supplemental opposition, addressing additional issues at my request) ("Apple II"); DE 19 (transcript of hearing dated Oct. 26, 2015) ("Tr."); DE 20 (Apple's post-hearing supplemental letter dated Oct. 28, 2015) ("Apple III"); DE 21 (government's post-hearing supplemental memorandum dated Oct. 28, 2015) ("Govt. III").

² The DEA agents never returned the warrant with the inventory of seized items as required. *See* Fed. R. Crim. P. 41(f)(1)(D). I assume that the warrant was executed during the authorized two-week period that expired on June 20, 2014. The date of Feng's arrest – which coincided with the arrests of all of his codefendants – fell within that period, and thus seems likely to have been the date of the search as well.

³ The record does not reveal the precise version of iOS 7 installed on Feng's iPhone, but neither the government nor Apple has suggested that any differences among the several versions of that operating system – as opposed, for instance, to the important differences between iOS 7 on one hand and iOS 8

Over the course of the next year, although the prosecution of Feng and his codefendants moved forward (as did, presumably, the government's investigation of the unknown others mentioned in the indictment), the government apparently did nothing at all to discover what evidence, if any, could be gleaned from Feng's iPhone. Instead, it waited until July 6, 2015, to seek a warrant to search that device and the others seized from Feng's residence. *See United States v. Cellular Telephone Devices Seized On Or About June 11, 2014 From Premises Located At 41-21 149th Street, First Floor, In Queens, NY*, 15-MJ-0610 (VVP), DE 1 (application for warrant to search devices) (the "Device Application"). A magistrate judge of this court granted the latter application and issued a warrant to search the devices that same day. *Id.*, DE 2 (the "Device Warrant"). Like the earlier warrant to search Feng's residence, this warrant set a two-week time limit on its execution. *Id.*

At some point during the following two weeks, the government "initiate[d] the execution of the search warrant [for Feng's iPhone] by attempting to search the device, turning it on and placing it in airplane mode. The [DEA] agents ... began that search but were unable to complete [it] because" the device required a password to allow access to certain information. Tr. at 6. The DEA agents then sought the assistance of the Federal Bureau of Investigation ("FBI"), but remained unable to bypass the iPhone's passcode security. *Id.* at 6-7; *see also* Govt. II at 5.

At that point – after the expiration of the two-week period during which agents were permitted to execute the Device Warrant – the government sought Apple's technical assistance. *See* Govt. II at 6; Tr. at 6. There appears to be no dispute that Apple's response, consistent with its past practice in at least 70 instances, was that it could and would unlock Feng's phone for the agents, but only if a court issued a lawful order requiring it to do so. *See* Govt. II at 6-7; Tr. at 7-8. Also consistent with past

and later versions on the other in terms of the difficulty of bypassing passcode security – has any bearing on the technical issues pertinent to this matter.

practice, Apple provided the agents with the specific technical language it deemed sufficient to make clear its obligation to provide the services that would allow the agents to gain access to the iPhone's passcode-protected data. *See* Govt. II at 6-7; Tr. at 7-8, 56-57.¹

On October 8, 2015, the government filed the instant Application, together with the proposed order that Apple had helped it draft. Relying exclusively on the AWA (and cases interpreting it) for authority, the government made several pertinent factual assertions beyond those recounted above:

- "Because the iOS device is locked, law enforcement agents are not able to examine the data stored on the iOS device as commanded by the search warrant." Govt. I at 1.
- "[I]n other cases, courts have ordered Apple to assist in effectuating search warrants under the authority of the All Writs Act. Additionally, Apple has complied with such orders." *Id.* at 2.
- "The requested order would enable agents to comply with this Court's warrant commanding that the iOS device be examined for evidence identified by the warrant." *Id.*
- "Examining the iOS device further without Apple's assistance, if it is possible at all, would require significant resources and may harm the iOS device." *Id.* at 2-3.

¹ The government's assertion that "Apple ... provided the government with specific language to submit to the Court[.]" Govt. II at 2, could be read to suggest that Apple somehow proposed or approved the government's reliance on the AWA as authority for the request. I note, however, that it is only the Application itself that cites the AWA; the proposed order submitted with it does not, but instead contains the technical language specifically describing the assistance the government wants Apple to provide. *See* DE 1-1; Tr. at 57. Also, the reference above to "the iPhone's passcode-protected data" is deliberately circumscribed. It omits information that the agents could, under certain circumstances, access without entering the correct passcode, such as a log of recent telephone calls made or received on the device. *See* DE 15-4 (Govt. II, Ex. D; excerpt from Apple on-line user's manual) ("Allow Access When Locked: Allow access to some features when your device is locked, including Notifications View, Siri, and Control Center."). It also omits other types of data that might be stored on the device (such as information relating to third-party applications that Feng had installed on the device) that could be encrypted or protected by different passcodes and therefore inaccessible to someone using the device's passcode without additional assistance that the government does not seek here. The record does not reveal whether the government's agents, in their attempts to execute the warrant to date, have tried to access information on Feng's device that is not passcode protected and, if so, what they found as a result.

- "[T]he [requested] order is not likely to place any unreasonable burden on Apple." *Id.* at 3.

On October 9, 2015, I issued a Memorandum and Order that declined to rule on the Application *ex parte*, and instead afforded Apple an opportunity to be heard in advance of any decision about the applicability of the AWA in the circumstances of this case. DE 2, *In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court*, 2015 WL 5920207 (E.D.N.Y. Oct. 9, 2015). I simultaneously directed the Clerk to maintain the Application – but not the Memorandum and Order, which revealed no factual details of the matter – under seal, on the mistaken assumption that its public dissemination could adversely affect an ongoing criminal investigation. DE 3. In its subsequent submission, the government stated that it had never intended to submit under seal either the Application or the proposed order (both of which it attached to its publicly filed legal memorandum), and also noted that the 2015 search warrant authorizing the search of Feng's iPhone was already available on the public docket. *See* Govt. II at 2 n.1 & Ex. A.

Apple submitted its initial opposition to the Application on October 19, 2015; the government replied on October 22, 2015; Apple filed a supplemental response on October 23, 2015;⁵ and I heard oral argument on October 26, 2015. *See* Apple I; Govt. II; Apple II; DE 18 (minute entry). At oral argument, it became apparent that there were a number of factual and legal issues that the government and Apple should have further opportunity to address, and I therefore set a schedule for them to file

⁵ Apple, in its initial submission, took pains to avoid addressing any issue other than the feasibility and burdensomeness of the requested relief – explaining that that was all I had asked it to do. In particular, it did not provide its views on the legal question of whether the AWA empowers the court to grant the Application, and it apparently sought no opportunity to do so later. *See* Apple I at 1 & n.2 ("Apple is not requesting oral argument."). Because I concluded that Apple was in the best position to knowledgeably litigate the legal issue presented here – and in particular, in a better position to do so than the American Civil Liberties Union ("ACLU"), which had offered to submit its own brief on behalf of itself and other *amici curiae*, *see* DE 10 – I asked Apple to file a supplemental response addressing the legal issue and to appear at oral argument, if only to answer my questions; I simultaneously denied the ACLU's motion to file an *amicus* brief. *See* Orders dated Oct. 20, 2015.

post-hearing submissions. DF 18. Apple and the government filed their respective supplemental briefs on October 28, 2015. *See* Govt. III; Apple III.

The accelerated briefing and argument schedule described above was not a reflection of the simplicity of the issues in dispute. Rather, it accommodated the government's interest in resolving the matter (both before me and on review of my decision by a district judge) in sufficient time to use any evidence it might secure with Apple's assistance at Feng's trial, which was then scheduled to begin on November 16, 2015. *See* Govt. II at 4. However, just one day after the oral argument in this case, the court scheduled a proceeding to have Feng enter a new plea; two days later, on October 29, 2015, Feng pleaded guilty pursuant to an agreement with the government. *See Yang*, Scheduling Order dated Oct. 27, 2015; *id.*, DF 119 (transcript of plea allocution dated Oct. 29, 2015) ("Allocution") at 12-13 (confirming Feng's agreement with the government). In notifying me of Feng's plea on the day it was entered, the government wrote that it "persists" in the pending Application, "but in view of the guilty plea, no longer requests expedited treatment." DF 22.

Because the desire to secure potential evidence for Feng's trial was the only basis for seeking Apple's assistance that the government had identified up to that point, *see* Govt. II at 3 ("[t]he government seeks evidence relevant to a defendant's guilt in a federal criminal case"), I promptly directed the government to explain why the Application was not moot. Order dated Oct. 30, 2015. The government responded that same day. It noted that Feng has yet to be sentenced, and that his case therefore remains open – although it did not attempt to explain how any information on the iPhone might alter the advisory sentencing guidelines range that would apply based on factors, including the amount and type of drugs involved in the offense, that the parties agreed the court could take into account. *See* DF 25 at 2; Allocution at 14-16. In addition to relying on the continuing potential need for evidence against Feng, the government also proffered a new theory: it noted that "Feng pleaded guilty

to a narcotics conspiracy, and the government's investigation into that conspiracy is ongoing. The underlying search warrant authorizes the government to seize evidence relating to Feng 'and others,' including 'customers' and 'sources of drugs.'" DF 25 at 1 (quoting Application, Ex. A, Attachment B).⁶

For several months after Feng's plea and the government's letter, this case progressed no further. On February 12, 2016 – apparently unprompted by any development in this case, but just as apparently, in hindsight, reacting to developments elsewhere – Apple filed a letter in response to the government's submission about the procedural viability of the Application in light of Feng's plea. Apple eschewed comment on whether the government's ongoing hunt for unindicted others, or the prospect of Feng's sentencing, sufficed to keep the controversy alive. Instead, Apple alluded to "additional requests similar to the one underlying the case before this Court" and the fact that it has "been advised that the government intends to continue to invoke the All Writs Act in this and other districts in an attempt to require Apple to assist in bypassing the security of other Apple devices in the government's possession." DF 26 (letter dated Feb. 12, 2016) at 1. Based on those similar requests and the anticipation of further motions under the AWA, Apple asserted that this matter "is not moot because it is capable of repetition, yet evading review." *Id.* at 2 (citing *United States v. N.Y. Tel. Co.*, 434 U.S. 159, 190 n.6 (1977)).

I recognized that while Apple's letter identified a sound legal theory, it did not supply a sufficiently particularized factual basis for applying it in this case. Moreover, it was apparent that those

⁶ The pretrial proceedings in Feng's case had lasted for nearly a year after the defendants' arrest when, at a status conference on June 3, 2015, Feng made clear his intention to proceed to trial (notwithstanding the other remaining defendants' announced intentions to enter guilty pleas) and the court indicated a desire to begin the trial in August. *See Yang*, Minute Entry dated June 3, 2015. On July 10, 2015, the court in Feng's case acceded to the parties' need to translate and review extensive recordings in Chinese and set a trial date of November 16, 2015. *See Yang*, Minute Entry dated July 10, 2015. It was only at that point that the government, on July 6, 2015, sought the warrant it seeks to have the court enforce here.

unreported facts might bear on a number of legal issues about which the parties had disagreed at oral argument. I therefore directed Apple to provide, among other things, specific details of the requests it had received from the government during the pendency of this action, the position Apple had taken in response, and the results of those requests. *See* Order dated Feb. 16, 2016. Although I did not require a response until March 1, 2016, Apple supplied the requested information the next day. DF 27 (letter dated Feb. 17, 2016). In that response, Apple identified nine requests filed in federal courts across the country from October 8, 2015 (the date of the instant Application) through February 9, 2016. *Id.* at 2. In each, Apple has been ordered under the authority of the AWA (or has been told that an order has been requested or entered) to help the government bypass the passcode security of a total of twelve devices; in each such case in which Apple has actually received a court order, Apple has objected. *Id.* None of those cases has yet been finally resolved, and Apple reports that it has not to date provided the requested assistance in any of them. *Id.* at 2-3.

In addition to the nine new cases described above, Apple also reported that as recently as February 16, 2016, shortly after my own order of the same date, the United States District Court for the Central District of California had entered an *ex parte* order under the AWA directing Apple

to perform even more burdensome and involved engineering than that sought in the case currently before this Court – *i.e.*, to create and load Apple-signed software onto the subject iPhone device to circumvent the security and anti-tampering features of the device in order to enable the government to hack the passcode to obtain access to the protected data contained therein.

Id. at 1 (citing DF 27-1 (copy of *In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203*, No. EID 15-0451M) (the "California" action), Order Compelling Apple, Inc. to Assist Agents in Search (C.D. Cal. Feb. 16, 2016)). On February 22, 2016, the government confirmed that Apple's description of the recent requests could properly be filed on the public docket without jeopardizing any pending criminal

investigation; in doing so, it noted the existence of yet one more case in which a court has ordered Apple to help the government bypass the passcode security of a locked device. DE 28. This matter is therefore one of a dozen pending cases in which the government and Apple disagree as to the court's authority to command Apple to assist the government in defeating the passcode security of devices Apple has manufactured.⁷

II. Discussion

A. Mootness

As a threshold matter, I agree with the government that its Application is not moot as a result of Feng's guilty plea. Whether the government will ever actually use any information it may find on Feng's phone either to litigate the sentencing phase of Feng's prosecution or to identify and prosecute the coconspirators, customers, and suppliers the government is pursuing, is ultimately of no moment. The government enjoys the prerogative to conduct lawful investigations into suspected criminal activity as it sees fit, and in this case it chooses to search for evidence on Feng's iPhone notwithstanding the fact that Feng's guilt has been established. Having made that choice, it is free to take the position it does here, and a ruling on the Application will therefore resolve a live dispute about whether Apple must unwillingly be compelled to provide the assistance the government seeks. The matter is therefore not moot.⁸

⁷ In addition, the government has identified three other closed cases in which a court issued an order under the AWA requiring Apple to extract information from a passcode-protected device, all without objection from Apple. *See* Govt. II at 9-10.

⁸ I do not rely on Apple's assertion that the case is justiciable on the ground that the dispute here is capable of repetition yet evading review. This case would obviously not be moot if Feng had continued to insist on his right to a trial; and there is no reason to suppose that in the dozen pending cases there are none in which Apple's objection to an order under the AWA requiring its assistance can be litigated and resolved before being mooted by a defendant's plea. Indeed, it is entirely possible that some of those cases – such as the *California* action, in which the only known participants in the crime under

B. The All Writs Act

For as long as this nation has had courts established by Congress pursuant to Article III of the Constitution, those courts have been endowed with broad statutory authority to ensure they could effectively carry out the duties of an independent judiciary by issuing the orders necessary to do so – even if Congress had not had the foresight to create all of the procedural mechanisms that might be required. As initially enacted by the First Congress in 1789, the AWA provided:

That all the before-mentioned courts of the United States, shall have power to issue writs of *scire facias*, *habeas corpus*, and all other writs not specially provided for by statute, which may be necessary for the exercise of their respective jurisdictions, and agreeable to the principles and usages of law.

Judiciary Act of 1789, 1 Stat. 73, § 14 (Sept. 24, 1789); *see id.* §§ 1-5 (establishing the courts mentioned in Section 14). That language has been amended only twice in the succeeding centuries, and never in any substantive way. In 1948, when Congress codified federal criminal law in Title 18 of the United States Code, it rendered the statute's text in a more modern style by removing the reference to two specific common law writs, it updated the language to reflect the broader array of federal courts then in existence, it expanded "necessary" to "necessary or appropriate", and it decided (for reasons that I cannot imagine have any impact on this case) to switch the order of words "principles" and "usages":

The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions agreeable to the usages and principles of law.

80 Pub. L. 772, 62 Stat. 683, 944 (June 25, 1948). A year later, Congress merely inserted the word "and" before the word "agreeable". *See* 81 Pub. L. 72, § 90, 63 Stat. 89, 102 (May 24, 1949). Thus, as currently formulated, the AWA provides, in pertinent part:

investigation have died, and where, as a result, there are no defendants with pending charges at all – cannot be concluded without the court first resolving the dispute arising under the AWA.

The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law.

28 U.S.C. § 1651(a).

The plain text of the statute thus confers on all federal courts the authority to issue orders where three requirements are satisfied:

1. issuance of the writ must be "in aid of" the issuing court's jurisdiction;
2. the type of writ requested must be "necessary or appropriate" to provide such aid to the issuing court's jurisdiction; and
3. the issuance of the writ must be "agreeable to the usages and principles of law."

If an application under the AWA meets all three of those requirements, the court "may" issue the requested writ in the exercise of its discretion – but it is never required to do so. *See, e.g., Application of U.S. in Matter of Order Authorizing Use of a Pen Register*, 538 F.2d 956, 961 (2d Cir. 1976), *rev'd on other grounds*, *United States v. N.Y. Tel. Co.*, 434 U.S. 159 (1977); *Morrow v. District of Columbia*, 417 F.2d 728, 736 (D.C. Cir. 1969); *Paramount Film Distributing Corp. v. Civic Center Theatre, Inc.*, 333 F.2d 358, 360 (10th Cir. 1964); *Chemical & Indus. Corp. v. Druffel*, 301 F.2d 126, 129 (6th Cir. 1962). A court deciding whether to take such discretionary action should consider three additional factors:

1. the closeness of the relationship between the person or entity to whom the proposed writ is directed and the matter over which the court has jurisdiction;
2. the reasonableness of the burden to be imposed on the writ's subject; and
3. the necessity of the requested writ to aid the court's jurisdiction (which does replicate the second statutory element, despite the overlapping language).

See N.Y. Tel. Co., 434 U.S. at 174-78.

As set forth below, I conclude that in the circumstances of this case, the government's application does not fully satisfy the statute's threshold requirements: although the government easily

satisfies the statute's first two elements, the extraordinary relief it seeks cannot be considered "agreeable to the usages and principles of law." In arguing to the contrary, the government posits a reading of the latter phrase so expansive – and in particular, in such tension with the doctrine of separation of powers – as to cast doubt on the AWA's constitutionality if adopted. Moreover, I further conclude that even if the statute does apply, all three discretionary factors weigh against issuance of the requested writ, and that the Application should therefore be denied as a matter of discretion even if it is available as a matter of law.

C. Statutory Requirements

1. Aid of Jurisdiction

Controlling case law conclusively demonstrates that the government seeks relief that is in aid of this court's jurisdiction for purposes of the AWA. To be sure, Justice Stevens, in a dissenting opinion in *N.Y. Tel. Co.* (reflecting the views of himself and Justices Brennan, Marshall, and Stewart), persuasively explained the important distinction between the judiciary's interest in authorizing a search and the executive's wholly different agenda in using that authority to gather evidence – and simultaneously demonstrated that the case law interpreting the AWA had consistently reflected that distinction. *See N.Y. Tel. Co.*, 434 U.S. at 186-90 (Stevens, J., dissenting); *id.* at 178 (Stewart, J., concurring in part and dissenting in part) (joining Part II of Justice Stevens' dissent).

The *N.Y. Tel. Co.* majority, however, decisively rejected the dissenters' arguments:

The dissent's attempt to draw a distinction between orders in aid of a court's own duties and jurisdiction and orders designed to better enable a party to effectuate his rights and duties ... is specious. Courts normally exercise their jurisdiction only in order to protect the legal rights of parties. In *Price v. Johnston*, 334 U.S. 266 (1948), for example, the production of the federal prisoner in court was required in order to enable him to effectively present his appeal which the court had jurisdiction to hear. Similarly, in *Harris v. Nelson*, 394 U.S. 286 (1969), discovery was ordered in connection with a habeas corpus proceeding for the purpose of enabling a prisoner adequately to protect his rights. Here, we have held that Fed. Rule Crim. Proc. 41 provided the District Court with power to authorize the FBI to install pen registers. The order

issued by the District Court compelling the Company to provide technical assistance was required to prevent nullification of the court's warrant and the frustration of the Government's right under the warrant to conduct a pen register surveillance, just as the orders issued in *Price* and *Harris* were necessary to protect the rights of prisoners.

Id. at 175 n.23. Thus, regardless of the persuasiveness of any argument to the contrary, I am constrained to conclude that, as a general matter, it would normally be in aid of the court's jurisdiction to order Apple to assist the government in executing a valid warrant to search Feng's device.

Further, the fact that the warrant to be enforced expired long before the government sought to compel Apple's assistance in executing it does nothing to extinguish the court's jurisdiction. Although the general rule is that the government must execute a search warrant no more than fourteen days after its issuance, Fed. R. Crim. P. 41(c)(2)(A)(i), in the context of a warrant to seize electronic storage media such as Feng's device, that time limit "refers to the seizure or on-site copying of the media ... and not to any later off-site copying or review." Fed. R. Crim. P. 41(c)(2)(B). Accordingly, ordering Apple to help the government bypass the passcode security on Feng's device would be in aid of this court's jurisdiction for purposes of the AWA.

2. Necessary or Proper

I likewise readily conclude that the requested order to Apple is "necessary or appropriate" within the meaning of the AWA. "Indeed, '[u]nless appropriately confined by Congress, a federal court may avail itself of all auxiliary writs as aids in the performance of its duties, when the use of such historic aids is calculated in its sound judgment to achieve the ends of justice entrusted to it.'" *N.Y. Tel. Co.*, 434 U.S. at 172-73 (quoting *Adams v. United States ex rel. McCann*, 317 U.S. 269, 273 (1942)).⁹

⁹ I explain below, in discussing the statute's "usages and principles" requirement, why I reject the government's assertion that the AWA empowers a court to take any action not prohibited by act of Congress. As the passage from *N.Y. Tel. Co.* quoted above demonstrates, however, the government's position is not wholly divorced from prior judicial interpretation of the Act. I agree that only a Congressional prohibition may place a judicial action beyond the bounds of what would otherwise be "necessary or appropriate in aid of" the court's jurisdiction. But that does not mean that every writ

3. Agreeable to the Usages and Principles of Law

The question whether the AWA permits the relief sought here thus reduces to whether it is "agreeable to the usages and principles of law" to compel Apple – a private party with no alleged involvement in Feng's criminal activity – to perform work for the government against its will. Federal case law offers little if any guidance on how to understand that term in the context of this case.¹⁰ I therefore consider this aspect of the statute in the context of case law that more generally discusses the AWA's overall function as a "gap filler" – that is, a source of interstitial authority that renders it unnecessary for Congress to anticipate every circumstance in which a federal court might properly act to vindicate the rights of parties before it. *See, e.g., Harris*, 394 U.S. at 300 ("the purpose and function of the All Writs Act to supply the courts with the instruments needed to perform their duty") (citations omitted); *Michael v. I.N.S.*, 48 F.3d 657, 669 (2d Cir. 1995) ("[T]he scope of the all writs provision

Congress has not proscribed is necessarily "agreeable to the usages and principle of law." Indeed, ascribing such parallel meaning to the latter clause would strip it of any independent effect, and thereby run afoul of an established rule of statutory construction. *Duncan v. Walker*, 533 U.S. 167, 174 (2001) ("It is our duty 'to give effect, if possible, to every clause and word of a statute.'") (quoting *United States v. Menasche*, 348 U.S. 528, 538-39 (1955)); *cf., Marx v. Gen. Revenue Corp.*, 133 S. Ct. 1166, 1177 (2013) ("The canon against surplusage is not an absolute rule [it] assists only where a competing interpretation gives effect to every clause and word of a statute.") (internal quotations omitted). Thus, the government's attempt to rely on the quoted passage from *N.Y. Tel. Co.* as a basis for satisfying the "usages and principles" prong of the AWA, rather than the "necessary or appropriate" prong to which the Court directly relates it, is entirely misplaced. *See* Govt. III at 7.

¹⁰ The Supreme Court wrote in 1952 that, "[i]n determining what auxiliary writs are 'agreeable to the usages and principles of law,' we look first to the common law." *United States v. Hayman*, 342 U.S. 205, 221 n.35 (1952) (quoting *Price*, 334 U.S. at 281). But that observation – made in the context of determining whether a particular type of writ of habeas corpus was available under common law, and therefore under the AWA – has no bearing on the instant dispute. Similarly, the Tenth Circuit's citation to *Hayman* for the same point in the context of determining the availability of a collateral challenge to a criminal conviction also offers no interpretive assistance here. *See Rawlins v. Kansas*, 714 F.3d 1189, 1196 (10th Cir. 2013) (citing *Hayman*, 342 U.S. at 221 n.35). In both cases, the discussion of the "usages and principles" clause was largely directed to identifying the types of writs that could be so described. Apple does not object that the type of assistance the government seeks here cannot find a close enough antecedent in the common law; the issue here – which *Hayman* and *Rawlins* had no need to address – is whether the issuance of such a writ is an appropriate application of the AWA's gap-filling function.

confine[s] it to filling the interstices of federal judicial power when these gaps threaten[] to thwart the otherwise proper exercise of federal courts' jurisdiction.") (quoting *Pennsylvania Bureau of Correction v. U.S. Marshals Serv.*, 474 U.S. 34, 41 (1985)).

The limits of such gap-filling authority are easily discerned. At one end of the spectrum, the AWA cannot be interpreted to empower courts to do something that another statute already authorizes (but that might have threshold requirements that cannot be satisfied in the circumstances of a particular case). *See Pennsylvania Bureau of Correction*, 474 U.S. at 43. At the other end, the government allows that a court cannot rely on the AWA (or, presumably, anything else) to issue an order that is explicitly or implicitly prohibited under a federal statute. *See Govt. III* at 7.

The gap between those two poles is large indeed, and the crux of Apple's dispute with the government about the meaning of the AWA's requirement that a writ be "agreeable to the usages and principles of law" is whether the statute fills all of that gap, as the government contends, or only some of it. In particular, unlike the government, Apple contends that a court order that accomplishes something Congress has considered but declined to adopt – albeit without explicitly or implicitly prohibiting it – is not agreeable to the usages and principles of law. *See Apple II* at 4; *Apple III* at 4. As explained below, I agree. Before discussing that matter, however, I first briefly consider how this case would come out if, instead of rejecting the government's understanding of the AWA's gap-filling function, I adopted it. Even under that reading of the law, I believe Apple has the better argument – both because it is arguable that CALFA¹¹ explicitly absolves a company like Apple of any responsibility to provide the assistance the government seeks here and also because even if CALFA does not have such an explicit prohibition, it is part of a larger legislative scheme that is so

¹¹ The acronym refers to the Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279, *codified at* 47 U.S.C. §§ 1001-1010.

comprehensive as to imply a prohibition against imposing requirements on private entities such as Apple that the statute does not affirmatively prescribe.

a. CALFA

i. The Statute's Purpose and Text

Congress enacted CALFA in 1994 to address its concern that "new and emerging telecommunications technologies pose problems for law enforcement[.]" *U.S. Telecom Ass'n v. F.C.C.*, 227 F.3d 450, 454 (D.C. Cir. 2000) (quoting H.R. rep. No.103-827 ("CALFA House Report"), pt. 1, at 14 (1994)). It designed the statute "to preserve the government's ability, pursuant to court order or other lawful authorization, to intercept communications involving advanced technologies such as digital or wireless transmission modes, or features and services such as call forwarding, speed dialing and conference calling, while protecting the privacy of communications and without impeding the introduction of new technologies, features, and services[.]" *Id.* (quoting CALFA House Report at 9).¹²

As part of its effort to ensure that the law would not stem technological progress, the legislature included several provisions exempting certain kinds of entities from the more general requirement to assist law enforcement in the execution of court orders authorizing various forms of electronic surveillance. These "Limitations" on CALFA's scope, 47 U.S.C. § 1002(b), fell into three categories. First, Congress limited the ability of law enforcement to prescribe or constrain the services communications companies could offer their customers and the equipment and systems used to market them:

¹² Although designed primarily to preserve the ability of law enforcement agencies to engage in lawful electronic surveillance, the statute was not limited to that topic. For example, it also addressed the responsibilities of private companies to preserve and allow access to records relating to wire and electronic communications. *See, e.g.*, 47 U.S.C. § 1002(a)(2)-(4) (prescribing responsibilities concerning "call-identifying information").

Design of features and systems configurations. This subchapter does not authorize any law enforcement agency or office

(a) to require any specific design of equipment, facilities, services, features, or system configurations to be adopted by any provider of a wire or electronic communication service, any manufacturer of telecommunications equipment, or any provider of telecommunications support services;

(b) to prohibit the adoption of any equipment, facility, service, or feature by any provider of a wire or electronic communication service, any manufacturer of telecommunications equipment, or any provider of telecommunications support services.

47 U.S.C. § 1002(b)(1).

Second, Congress explicitly exempted certain types of businesses from the statute's obligations to assist law enforcement:

Information services; private networks and interconnection services and facilities.

The requirements of subsection (a) of this section do not apply to –

(A) information services; or

(B) equipment, facilities, or services that support the transport or switching of communications for private networks or for the sole purpose of interconnecting telecommunications carriers.

Id. § 1002(b)(2).

Finally, Congress largely (but not completely) exempted from CALFA's general requirement of private assistance to law enforcement a requirement that businesses help agents bypass any encryption that might shield communications from surveillance:

Encryption. A telecommunications carrier shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication.

Id. § 1002(b)(3).¹³

¹³ This provision precludes the government from requiring carriers to build into the encryption measures they make available to their subscribers a "back door" that enables law enforcement access

ii. Application to Construction of the AWA

Both the government and Apple agree that CALFA does not compel a private company such as Apple to provide the kind of assistance the government seeks here. *See* Govt. II at 22; Apple II at 5. They disagree as to why that is so: the government contends that CALFA simply has nothing to say on the matter, while Apple argues that the omission reflects a legislative choice. As explained below, Apple's argument has more merit.

The government suggests that CALFA imposes duties on telecommunications carriers only with respect to what it calls "data 'in motion'" and then adds that "[b]y contrast, this case involves evidence already stored on a cell phone (data 'at rest')." Govt. II at 22; *see also* Govt. III at 9-10.¹¹ From there, it argues that the statutory language exempting "information services" from comparable duties is irrelevant, regardless of whether Apple qualifies as such a service, because the information it seeks to seize from Feng's iPhone is data "at rest." *See* Govt. II at 22 ("CALFA is entirely inapplicable to the present dispute").

The proposition that CALFA makes a distinction between data "at rest" and "in motion" is largely correct as far as it goes, but ultimately misses the point. Even if Congress did not in any way

to encrypted communications. It does no more than provide that law enforcement is entitled to have carriers assist in securing access to encrypted information where the carrier in making such encryption available, has also retained a decryption key for its own purposes that would allow such access.

¹¹ In seeking to explain CALFA's purported irrelevance to this case, the government observes that the instant application does not seek "to compel Apple to develop a technical capability that Apple does not already possess." Govt. III at 9. Such more intrusive relief, however, is precisely what the government seeks in the *California* action – relying, as it does here, on the proposition that the requested order is "agreeable to the usages and principles of law." As discussed below, that fact is pertinent to a consideration in this case of the reasonableness of the burden the government seeks to impose on Apple.

regulate data "at rest" in CALFA,¹⁵ it plainly could, and did, enact such legislation elsewhere. *See, e.g.*, 18 U.S.C. § 2703(f)(1) (requiring "[a] provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, [to] take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process"). Thus, long before the instant Application was filed, Congress enacted legislation to prescribe the private sector's duties to assist a wide variety of law enforcement investigations – relating to data both "in motion" and "at rest." Those laws defined the extent to which all sorts of service providers had such duties: telecommunications service providers, information service providers, and the providers of wire and electronic communications. None of those laws imposed any obligation on Apple to provide the assistance at issue here, and in particular, CALFA expressly stated that the assistance requirement did not apply to "information services." 47 U.S.C. § 1002(b)(2)(A).¹⁶

The latter point is pertinent because, as Apple persuasively argues, "Apple is substantially engaged in the provision of 'information services' as that term is defined under CALFA, and thus could be considered an information services provider." Apple III at 1 (citing 47 U.S.C. § 1001(6)). As Apple notes:

¹⁵ *But see* 47 U.S.C.A. § 1002(a)(2)(B) (requiring telecommunications service providers to have the ability to provide "call-identifying information" to law enforcement even after a call's conclusion – when, presumably, such information would be "at rest" within the government's meaning).

¹⁶ As a fallback position, the government writes that "even if it were applicable, CALFA addresses a provider's capability to produce information when it receives a court order, not the government's authority to obtain information pursuant to a court order in the first place." Govt. II at 22. Here again, the government fails to take into account the reality that Congress does not always place all related regulations of a given subject into a single section of the United States Code. While it is true enough that a service provider's technical capabilities are prescribed in CALFA, Congress has also elsewhere defined "the government's authority to obtain [the] information [a provider must make accessible] pursuant to a court order in the first place." *See, e.g.*, 18 U.S.C. §§ 2518, 2522 (prescribing requirements for the interception of communications and providing for means to thereupon require the pertinent communications service providers to render the assistance necessary to accomplish such interception).

Under CALFA "information services" means the "offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications," and "includes a service that permits a customer to retrieve stored information from, or file information for storage in, information storage facilities; electronic publishing; and electronic messaging services." [47 U.S.C.] § 1001(6).

Apple is substantially engaged in developing and offering products that provide such capabilities. For example, Apple's iTunes service allows customers to purchase, store, and access music, movies, television shows, games and apps via an Internet-connected Apple device, such as an iPhone[.] iTunes thus constitutes an "information service" under CALFA by providing "a capability for ... acquiring, storing ... [and] retrieving . . . information via telecommunications." *Id.* Similarly, iMessage allows Apple customers (connected over the Internet) to communicate by messages sent and received via their iPhone[.]

Apple III at 1-2.

CALFA thus prescribes for telecommunications carriers certain obligations with respect to law enforcement investigations that it does not impose on a category of other entities – described as "information service providers" – that easily encompasses Apple. Thus, as Apple argues with some justification, "the bounds of mandatory law enforcement assistance were drawn by CALFA, and drawn in such a way to exclude the relief the government seeks." *Id.* at 4.

To be sure, CALFA by itself has limits that render that one statute less than comprehensive. But considered together with other statutes prescribing the extent to which law enforcement may secure access to a wide array of data – both "in motion" and "at rest" – as well as the obligations of some private entities but not others to provide affirmative assistance to such investigations, the statute is easily seen as part of a comprehensive legislative scheme. The absence from that comprehensive scheme of any requirement that Apple provide the assistance sought here implies a legislative decision to prohibit the imposition of such a duty.¹⁷ Thus, even under the government's reading of the AWA,

¹⁷ A similar argument can be made with respect to the various statutes and rules authorizing a court to authorize the seizure of various kinds of evidence. Here again, Congress manifestly knows how to explicitly impose an obligation on private parties to provide assistance to law enforcement in the

I would conclude that while the matter is a close call, the Application seeks an order that is not "agreeable to the usages and principles of law."

b. Statutory Construction

If the best reading of CALFA produces a conclusion that it prohibits the relief the government seeks here, then the Application must be denied even under the government's understanding of what it means for a judicial order to be "agreeable to the usages and principles of law." But if CALFA, considered in the context of a larger statutory scheme, does not erect such a barrier to relief on its own terms, then resolution of the Application turns on whether the gap in laws that the AWA fills is, as the government argues, the entire space between authorizing statutes and legislative prohibitions or if, as Apple would have it, it only reaches to such legislative powers as Congress has not considered and either adopted or rejected. As explained below, I conclude that Apple's position is more consistent than the government's with the rule of statutory construction that requires giving meaning to all statutory words and clauses as well as the rules prohibiting interpretations that produce absurd results or are of suspect constitutionality.

First, as a matter of technical statutory construction, I can find no way to read the statute in a way that gives the required independent meaning to three distinct terms in the AWA – "usages", "principles", and "law" – that conforms to the government's view of the statute. *See, e.g., Duncan*, 533 U.S. at 174 (courts have a "duty to give effect, if possible, to every clause and word of a statute") (quoting *Menasche*, 348 U.S. at 538-539); *United States v. Nordic Vill. Inc.*, 503 U.S. 30, 36 (1992) ("a statute must, if possible, be construed in such fashion that every word has some operative effect"); *Am. Civil*

execution of such court orders. Thus, Congress has explicitly required private parties to assist in the execution of warrants authorizing wiretaps and pen registers, *see* 18 U.S.C. §§ 2518(4), 3123(b)(2), but it has imposed no corresponding obligation on private parties to assist in the execution of search and seizure warrants under Federal Rule of Criminal Procedure 41.

Liberties Union v. Clapper, 804 F.3d 617, 623 (2d Cir. 2015) (courts "must ... strive to avoid interpretations of a statute that would render any phrase or provision superfluous") (citing *TRW Inc. v. Andrews*, 534 U.S. 19, 31 (2001)).

"[A]greeable to" means, in essence, "consistent with." *See, e.g., Webster's Third New International Dictionary of the English Language Unabridged* at 43 (Merriam-Webster 2002) (defining "agreeable" to mean, among other things, "in harmony or keeping : CONSISTENT, CONSONANT"). Congress could easily have written the AWA to mean what the government says it means simply by requiring that a court's orders under the statute must be "agreeable to the law" – because any action not prohibited by law is, by definition, agreeable to the law.¹⁸ But the AWA requires an order issued under its aegis to be agreeable not merely to some part of the entire body of law, but to the law's "usages" and "principles" – which must mean something else. The most natural reading gives meaning to the whole phrase by limiting the permissible orders to those that not only fail to violate legislative prohibitions, but that also are consonant with both the manner in which the laws were developed (that is, the "principles" that the laws reflect) and the manner in which the laws have been interpreted and implemented (that is, the "usages" of the various laws). Others may propose plausible alternative interpretations of "agreeable to the usages and principles of law."¹⁹ But whatever each of its words may mean in isolation, the rules of

¹⁸ Indeed, later Congresses have endorsed just such simple formulations in approving rules that give the judiciary the flexibility it needs to conduct its business. *See* Fed. R. Crim. P. 57(b) ("A judge may regulate practice in any manner consistent with federal law, these rules, and the local rules of the district."); Fed. R. Civ. P. 83(a)(1) (authorizing promulgation of local rules that "must be consistent with – but not duplicate – federal statutes and rules adopted under 28 U.S.C. §§ 2072 and 2075"); Fed. R. Civ. P. 83(b) ("A judge may regulate practice in any manner consistent with federal law, rules adopted under 28 U.S.C. §§ 2072 and 2075, and the district's local rules.").

¹⁹ To date, however, the government has not come up with any such permissible alternative construction, let alone a better one. At oral argument, when I invited the government to reconcile its broad reading of the AWA "with a statute that includes not just agreeable to law but agreeable to principles and usages of law [sic]," Tr. at 38, it acknowledged my concern but then went on to answer a different question by discussing the extent to which a particular statute is sufficiently comprehensive

statutory construction compel me to conclude that their meanings are distinct – and the government's preferred reading of the AWA does not permit that.

Second, the implications of the government's position are so far-reaching – both in terms of what it would allow today and what it implies about Congressional intent in 1789 – as to produce impermissibly absurd results. *See, e.g., United States v. Dauray*, 215 F.3d 257, 264 (2d Cir. 2000) ("A statute should be interpreted in a way that avoids absurd results."); *United States v. Wilson*, 503 U.S. 329, 334 (1992) ("absurd results are to be avoided").

At the heart of the government's reading is the assuredly correct observation that there are any number of ways in which Congress may fairly be said to have considered legislation that does not result in the enactment of legislation, and that as a result the only practical way to discern what is agreeable to the usages and principles of law from what is not is to draw a bright line around what Congress has prohibited – either explicitly or implicitly via the omission of authority from a comprehensive legislative scheme. *See* Govt. II at 24; Tr. at 15, 37. I agree with the government that "[c]ongressional inaction lacks persuasive significance because several equally tenable inferences may be drawn from such inaction." *Zino Davidoff v. CVS*, 571 F.3d 238, 243 (2d Cir. 2009) (quoting *Cent. Bank of Denver, N.A. v. First Interstate Bank of Denver, N.A.*, 511 U.S. 164, 187 (1994)) (quoted in Govt. II at 24). But the choice is not quite so binary as the government implies: a reliance on outright

as to suggest that its limitations imply a legislative prohibition of other actions. *Id.* at 38-39. The government did not thereafter return to the question of statutory construction, and it similarly deflected the question in its post-hearing submission. *See* Govt. III at 7 (acknowledging the need to interpret the "usages and principles of law" clause as a whole, and citing cases in support of its view on the matter, but offering no argument about how to give independent meaning to both "usages" and "principles" consistent with that view). Moreover, as explained above, *see* n.9, *supra*, the principal authority on which the government relies in that argument – and indeed the source of the sole rationale, namely, that "federal courts may avail themselves of all auxiliary writs 'unless appropriately confined by Congress[.]" *id.* (quoting *N.Y. Tel. Co.*, 434 U.S. at 171) – does not actually purport to interpret the AWA's "usages and principles of law" clause, but rather its "necessary or appropriate" clause.

prohibition is not the sole alternative to the chaos of attributing significance to mere legislative inaction. As this case makes clear, the record available to a court considering an application under the AWA will likely have a wealth of information beyond mere congressional inaction – including an array of legislative proposals and hearings that provide a stronger basis for the inferences to be drawn from the ultimate absence of enacted legislation.

As a threshold matter, I respectfully disagree with the government's view of what is and is not practical. The duty of faithful adherence to statutory text does not relieve the courts of the frequent need to make judgments about legislative intent, nor does it restrict them to only such interpretive tools as a dictionary may provide.²⁰ There is no reason that a judge, ably guided by competent counsel for adversarial parties as I am here, cannot compare a proposed order under the AWA with the surrounding body of pertinent laws to determine how consonant the two may be.²¹

²⁰ For example, in the conceptually similar context of preemption analysis, the Second Circuit recently observed that even the absence of a full legislative record, which may impede such analysis, "does not change the fact that a court's primary purpose in statutory interpretation is to discern legislative intent." *Entergy Nuclear Vermont Yankee, LLC v. Shamlin*, 733 F.3d 393, 420 (2d Cir. 2013) (internal quotation marks, citation, and footnote omitted); see also *Loyal Tire & Auto Ctr., Inc. v. Town of Woodbury*, 445 F.3d 136, 145 (2d Cir. 2006) (Sotomayor, J.) (holding, in the context of Interstate Commerce Act preemption, that a court "must consider any specific expressions of legislative intent in the statute itself as well as the legislative history").

²¹ That is precisely what the Supreme Court did in *N.Y. Tel. Co.* Instead of simply observing that no law prohibited the court from ordering the telephone company to make its facilities available to install a pen register – which is all that would have been necessary under the government's reading of the AWA – the Court took pains to explain why such an order was consistent with "more recent congressional actions." 434 U.S. at 176. It discerned what "Congress clearly intended to permit[.]" *id.*, and rested its decision on "the clear indication by Congress that the pen register is a permissible law enforcement tool[.]" *Id.* at 178. The results and opinions in other cases are likewise inherently in tension with the government's understanding of the breadth of the AWA's gap-filling function. See, e.g., *Pennsylvania Bureau of Correction*, 474 U.S. at 39 (denying request for AWA order requiring Marshals Service to transport state prisoners to federal courthouses because the applicable statutory language required such assistance from the custodian "but extends this duty to no other"); *Application of the United States for Relief*, 427 F.2d 639, 644 (9th Cir. 1970) (denying request for AWA order to telephone company to provide needed technical assistance for wiretap because Congress "omitted any reference to judicial power to require" such assistance).

Beyond its unduly pessimistic assumptions about a court's practical ability to properly apply the "usages and principles" clause unless strictly constrained, the government's construction of the AWA produces absurd results in application. If, for example the President sent to Congress a bill explicitly authorizing a court to issue the kind of order the government seeks here, and if every single member of the House and Senate were to vote against the enactment of such a law citing the kinds of data security and personal privacy concerns that Apple now embraces, the government would nevertheless describe the order sought here as permissible because Congress had merely rejected the bill – however emphatically, and however clear its reasons for doing so – rather than affirmatively passing legislation to prohibit the executive branch's proposal. Yet in such circumstances, it would be absurd to posit that the authority the government sought was anything other than obnoxious to the law.²²

An even starker illustration of the absurdity the government's construction produces is that it does not allow a court to deem an action beyond the AWA's reach even if it is an exercise of authority that had formerly been available under a statute that Congress elected to repeal because it was persuaded on policy grounds to retract such authority from the executive. Thus, for example, if communications service providers were to persuade Congress that CALEA had imposed unreasonable burdens on them that threatened their ability to remain in business, Congress could make the choice to repeal that law – thereby removing the statutory obligation to provide certain types of assistance to law enforcement. And yet in the absence of a statute affirmatively prohibiting the

²² A legislature so united in its opposition to a presidential proposal could of course, in an effort to conclusively forestall the possibility that a court might endorse such absurdity, pass a prohibiting statute. But if the President's proposal, while overwhelmingly opposed, nevertheless had the support of the bare minimum number of legislators required to sustain a presidential veto, Congress could defeat the President's proposal but could not enact affirmative legislation prohibiting it. Under such circumstances, however, it would still be easy – and, in my view, correct – for a court to conclude that the proposed order could not fairly be described as agreeable to the usages and principles of law.

government from requiring a company to provide such assistance, the government would read the AWA to nevertheless allow a court to order those same companies to provide precisely the same assistance to law enforcement that Congress had decided no longer to compel.

In short, whatever else the AWA's "usages and principles" clause may be intended to accomplish, it cannot be a means for the executive branch to achieve a legislative goal that Congress has considered and rejected. But because such rejection can take many forms, only one of which (and arguably the least likely in most circumstances) is outright prohibition, the government's argument here is manifestly irreconcilable with the statute.

The government's position also produces a wholly different kind of absurdity: the idea that the First Congress might so thoroughly undermine fundamental principles of the Constitution that many of its members had personally just helped to write or to ratify. Its preferred reading of the law – which allows a court to confer on the executive branch any investigative authority Congress has decided to withhold, so long as it has not affirmatively outlawed it – would transform the AWA from a limited gap-filing statute that ensures the smooth functioning of the judiciary itself into a mechanism for upending the separation of powers by delegating to the judiciary a legislative power bounded only by Congress's superior ability to prohibit or preempt. I conclude that the constitutionality of such an interpretation is so doubtful as to render it impermissible as a matter of statutory construction.

The AWA was enacted as part of the Judiciary Act of 1789, which Justice O'Connor has described as "the last great event in our Nation's founding" and part of "the triad of founding documents, along with the Declaration of Independence and the Constitution itself[.]" Sandra Day O'Connor, *The Judiciary Act of 1789 and the American Judicial Tradition*, 59 U. Cin. L. Rev. 1, 3 (1990); *see also* Dimitri D. Portnoi, *Resorting to Extraordinary Writs: How the All Writs Act Rises to Fill the Gaps in the Rights of Enemy Combatants*, 83 N.Y.U. L. Rev. 293, 296 (2008) (quoting same and providing further

discussion of the AWA's importance). It is no coincidence that an act of such foundational importance, and so essential to the implementation of the constitutional scheme of a government of limited powers carefully allocated among three separate branches, was enacted during the First Session of the First Congress – because so many of that legislature's members had themselves taken part in creating the Constitution itself. Indeed, more than half of the delegates to the Constitutional Convention who signed the Constitution (as well as several dozen delegates to the various state ratifying conventions) were involved in the enactment of Judiciary Act of 1789.²³

It is wholly implausible to suppose that with so many of the newly-adopted Constitution's drafters and ratifiers in the legislature, the First Congress would so thoroughly trample on that document's very first substantive mandate: "All legislative Powers herein granted shall be vested in a Congress of the United States[.]" U.S. Const. Art. I, § 1. And yet that is precisely the reading the government proposes when it insists that a court may empower the executive to exercise power that the legislature has considered yet declined to allow. It is a reading that thoroughly undermines both the legislature's own prerogative to reject a legislative proposal effectively and efficiently (without the need to affirmatively ban the proposed authority) and the more general protection against tyranny that the Founders believed required the careful separation of governmental powers. *See, e.g., Mistretta v. United States*, 488 U.S. 361, 380 (1989) ("[T]he separation of governmental powers into three coordinate

²³ Seventeen delegates to the Constitutional Convention served as members of the First Congress, including, most tellingly, James Madison – the author of the Federalist papers' explication of the principle of separation of powers. In addition, President Washington, who signed the Judiciary Act into law, had likewise represented Virginia at the Convention. *See* The Federalist Nos. 47, 51 (James Madison); Paul Taylor, *Congress's Power to Regulate the Federal Judiciary: What the First Congress and the First Federal Courts Can Teach Today's Congress and Courts*, 37 Pepp. L. Rev. 847, 868 (2010) (detailing the extensive support for the Judiciary Act of 1789 among member of the First Congress who had been delegates to either the Constitutional Convention or the several state ratification conventions) (citing, *inter alia*, Encyclopedia of American History 145 (Richard B. Morris ed., 6th ed. 1982)); About the Signers, <http://www.constitutionfacts.com/us-constitution-amendments/about-the-signers/> (last visited Feb. 29, 2016).

Branches is essential to the preservation of liberty.... Madison ... said: 'No political truth is certainly of greater intrinsic value or is stamped with the authority of more enlightened patrons of liberty.'") (quoting *The Federalist* No. 47, p. 324 (J. Cooke ed. 1961); case citations omitted).

The proposition that the government's interpretation of the AWA produces such a violation of the separation-of-powers doctrine is not simply a matter of taking an argument to a speculative, albeit logical, conclusion. To the contrary, it reflects what is going on right now, in this case. The Application before this court is by no means singular: the government has to date successfully invoked the AWA to secure Apple's compelled assistance in bypassing the passcode security of Apple devices at least 70 times in the past, *see* Tr. at 8; it has pending litigation in a dozen more cases in which Apple has not yet been forced to provide such assistance; and in its most recent use of the statute it goes so far as to contend that a court – without any legislative authority other than the AWA – can require Apple to create a brand new product that impairs the utility of the products it is in the business of selling. It is thus clear that the government is relying on the AWA as a source of authority that is legislative in every meaningful way: something that can be cited as a basis for getting the relief it seeks in case after case without any need for adjudication of the particular circumstances of an individual case (as the arguments that the government relies on here to justify entering an AWA order against Apple would apply with equal force to any instance in which it cannot bypass the passcode security of an Apple device it has a warrant to search).²¹

²¹ Assuming that the power the government believes the AWA to confer on the court can properly be characterized as legislative does not, standing alone, necessarily mean that it runs afoul of the separation of powers doctrine. "Congress may delegate to the Judicial Branch nonadjudicatory functions that do not trench upon the prerogatives of another Branch and that are appropriate to the central mission of the Judiciary." *Mistretta*, 488 U.S. at 388. But as explained above, the government's reading would indeed trench upon the legislature's prerogative, by making it impossible in some circumstances to effectively prohibit the executive from gaining a power it seeks unless it can do so with a veto-proof supermajority.

It is also clear that the government has made the considered decision that it is better off securing such crypto-legislative authority from the courts (in proceedings that had always been, at the time it filed the instant Application, shielded from public scrutiny) rather than taking the chance that open legislative debate might produce a result less to its liking. Indeed, on the very same day that the government filed the *ex parte* Application in this case (as well as a similar application in the Southern District of New York, *see* DF 27 at 2), it made a public announcement that after months of discussion about the need to update CALFA to provide the kind of authority it seeks here, it would *not* seek such legislation. *See* James B. Comey, "Statement Before the Senate Committee on Homeland Security and Governmental Affairs," (Oct. 8, 2015), <https://www.fbi.gov/news/testimony/threats-to-the-homeland> ("The United States government is actively engaged with private companies to ensure they understand the public safety and national security risks that result from malicious actors' use of their encrypted products and services. However, the administration is not seeking legislation at this time.").

The government's interpretation of the breadth of authority the AWA confers on courts of limited jurisdiction thus raises serious doubts about how such a statute could withstand constitutional scrutiny under the separation-of-powers doctrine. It would attribute to the First Congress an anomalous diminishment of its own authority (to deny a request to increase the executive's investigative powers it deemed inadvisable simply by declining to enact it) as well as an equally implausible intention to confer essentially unlimited legislative powers on the judiciary. Adopting that interpretation

would fly in the face of the doctrine of constitutional avoidance, which "allows courts to *avoid* the decision of constitutional questions" by providing "a tool for choosing between competing plausible interpretations of a statutory text, resting on the reasonable presumption that Congress did not intend the alternative which raises serious constitutional doubts."

Am. Civil Liberties Union v. Clapper, 785 F.3d 787, 808 (2d Cir. 2015) (quoting *Clark v. Martinez*, 543 U.S. 371, 381 (2005)) (emphasis in original); *see also Clark*, 543 U.S. at 380-81 ("If one of [two plausible statutory constructions] would raise a multitude of constitutional problems, the other should prevail – whether or not those constitutional problems pertain to the particular litigant before the Court."). I therefore reject the government's interpretation of the AWA's gap-filling function, and conclude that a judicial order that would confer authority that Congress has considered and decided not to enact is not "agreeable to the usages and principles of law."

Applying that interpretation in this case compels the conclusion that the AWA does not authorize the relief the government seeks. In my initial Memorandum and Order in this case, I discussed at some length the history of Congressional consideration in the decades since CALFA's enactment of updates to the statute that would confer – or withhold – the kind of authority at issue here to compel private actors to assist the government in technologically complex investigations. *See* 2015 WL 5920207, at *1-3.²⁵ After reviewing that history, I concluded that "the absence of any explicit statutory authority for the relief the government seeks cannot be attributed to a failure of legislators to consider such an enactment." *Id.* at *3. Nothing in the subsequent submissions from the government or Apple suggests a basis for abandoning that conclusion. I therefore conclude that what the government seeks here is "to have the court give it authority that Congress chose not to confer." *Id.* at

²⁵ That history includes the FBI's briefing of Congress in 2009 about the so-called "Going Dark" problem and drafting legislation to address it in part by amending CALFA to cover companies such as Apple; then-Senator Biden's 1991 bill requiring companies to ensure law enforcement access to the plain text contents of communications when authorized by law; a legislative hearing before the House Subcommittee on Counterterrorism and Intelligence addressing in part law enforcement agencies' challenges in overcoming technological barriers to accessing data; another hearing before the Senate Judiciary Committee in 2015 entitled "Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy" during which the Deputy Attorney General and FBI Director jointly called on Congress to legislate on the matter; and the submission of three separate bills in 2015, each of which would have precluded the government from forcing a private entity such as Apple to provide the kind of assistance at issue here. *See* 2015 WL 5920207, at *1-3.

*1 – and that, for the reasons explained above, granting such a request is not "agreeable to the usages and principles of law."

Accordingly, because the government's Application fails to satisfy the AWA's statutory requirements, I must deny the request for relief regardless of any analysis of the discretionary factors under *N.Y. Tel. Co.* As discussed below, however, consideration of those factors would in any event lead to the same result.

D. Discretionary Factors

1. Closeness

a. Apple's Relationship to Feng's Criminal Activity

In *N.Y. Tel. Co.*, the Supreme Court held that where there was probable cause to believe that a telephone company's own property was "being employed to facilitate a criminal enterprise on a continuing basis[,]," and where the company was "a highly regulated public utility with a duty to serve the public," the company was not "so far removed from the underlying controversy that its assistance could not be permissibly compelled." 434 U.S. at 174. I explained in the Memorandum and Order why it appeared that the circumstances of this case are materially different. *See* 2015 WL 5920207, at *5. After considering the later-submitted arguments from the government and Apple, I adhere to that view, and conclude that unlike the public utility in *N.Y. Tel. Co.*, Apple is too far removed from Feng's criminal conduct to have any obligation to assist the DEA's investigation.

To the extent that Feng used his iPhone in committing crimes, he used his own property, not Apple's. Unlike the telephone company in *N.Y. Tel. Co.*, which owned the facility used for criminal communications, Apple has no ownership interest in anything that the record reveals Feng used to commit a crime. And unlike the telephone company – "a highly regulated public utility with a duty to

serve the public," 434 U.S. at 174 – Apple is a private entity with no greater duty to serve the public than any other business.

The government argues that Apple's relationship to Feng's criminal activity is sufficiently close, notwithstanding those differences, because, while Feng owned the device itself, he merely licensed from Apple the iOS software on which it runs. *See* Govt. II at 13. But while the government ably demonstrates what the license forbade Feng from doing – he could not lawfully "rent, lease, lend, sell, redistribute or sublicense the iOS Software[.]" *id.* (quoting license agreement ¶ B(3)) – it does not explain the significance of that fact in determining the proximity of Apple's relationship to Feng's conduct. As far as I can discern from the record, Feng did not at any time "rent, lease, lend, sell, redistribute, or sublicense" Apple's software; what he did "sell" or "redistribute" was methamphetamine – a course of conduct in which Apple was not involved. Nor does the record support an inference that Feng in any way used the licensed software itself – as opposed to the data it allowed Feng to store on the hardware Apple no longer owns – to facilitate his crimes; to the contrary the record contains an explicit description of the ways in which the government believes Feng used his iPhone to commit his crimes as well as the types of evidence the DEA agents expected to find on it. *See* Device Application ¶¶ 7-28 & Attachment B. Nothing in that description even remotely suggests that the licensed software played any meaningful role in Feng's crime comparable to the role the telephone company's property played in the crimes under investigation in *N.Y. Tel. Co.*²⁶

²⁶ If Apple's retention of intellectual property rights in the software deployed in a device sold to the public sufficed to render it sufficiently close, for purposes of the AWA, to any crime committed by any user of such a device, it would eventually render the first discretionary factor under *N.Y. Tel. Co.* a dead letter. As constantly increasing computing power is continually squeezed into ever smaller storage devices, the category of consumer products containing licensed software will continue to grow. In a world in which so many devices, not just smartphones, will be connected to the Internet of Things, the government's theory that a licensing agreement allows it to compel the manufacturers of such products to help it surveil the products' users will result in a virtually limitless expansion of the government's legal authority to surreptitiously intrude on personal privacy.

Ultimately, the government's point is not that Apple in any way facilitated Feng's criminal conduct, but rather that it reaps profits from selling devices (and leasing the software on which those devices run) to a vast group of consumers among whom there are inevitably some criminals. From that premise it draws the following conclusion: "Apple cannot reap the legal benefits of licensing its software in this manner and then later disclaim any ownership or obligation to assist law enforcement when that same software plays a critical role in thwarting execution of a search warrant." Govt. II at 13-14. That opinion may be perfectly defensible as moral precept (however much it may be in tension with the legal system's otherwise broad support for free enterprise), but it has nothing to do with the pertinent legal inquiry.²⁷ Apple had no involvement in Feng's crime, and it has taken no affirmative action to thwart the government's investigation of that crime (a matter discussed in greater detail below). Apple lawfully sold to Feng, as it sells to millions of law-abiding individuals and entities (including the government itself), a product that can effectively secure its stored data for the protection of its owner.²⁸ Feng used that device for criminal purposes and left it locked, and the government says

²⁷ It is no surprise that references to the idea that all citizens have some sort of a duty – moral, if not legal – to assist law enforcement upon demand can occasionally be found in judicial opinions. For example, in an 1895 decision upholding a citizen's right to assist the government in enforcing the law by providing information about suspected criminal activity, the Supreme Court held that "such information given by a private citizen, is a privileged and confidential communication, for which no action of libel or slander will lie[.]" *In re Quarles*, 158 U.S. 532, 535-36 (1895). In introducing the topic, the Court included dicta suggesting – without any citation to authority – that that right is also an obligation. *Id.* at 535 ("It is the duty and the right, not only of every peace officer of the United States, but of every citizen, to assist in prosecuting, and in securing the punishment of, any breach of the peace of the U.S. It is the right, as well as the duty, of every citizen, when called upon by the proper officer, to act as part of the posse comitatus in upholding the laws of his country."). Nothing in *Quarles* suggests that the "duty" to which the Court referred is legal rather than moral.

²⁸ Just as the criminal Feng has done, the United States government has chosen to entrust extremely sensitive communications and secret documents – including those of many of the prosecutors and judges who work in this court – to the passcode protections and other robust data security measures available on a variety of Apple devices. That observation does not mean Apple should have any greater or lesser obligation, as a matter of law or morality, to accede to the demands of law enforcement

it cannot open the lock without Apple's help. Nothing in *N.Y. Tel. Co.* remotely suggests that in such circumstances, Apple is so closely related to the crime under investigation that a court can order its assistance under the AWA.

b. Apple's Relationship to the Government's Investigation

The government alternatively posits that Apple is sufficiently close to the underlying controversy for purposes of the AWA because its "software now thwarts the execution of the search warrant" for Feng's iPhone. Govt. II at 15. That formulation comes after (but subtly reinterprets) an earlier quotation from the opinion in *N.Y. Tel. Co.* As the government notes, in arguing that the court has authority to grant relief under the AWA (as opposed to the distinct question of whether such authority should be exercised as a matter of discretion),

The Court held that "[t]he power conferred by the Act extends, under appropriate circumstances, to persons who, though not parties to the original action or engaged in wrongdoing, are in a position to frustrate the implementation of a court order or the proper administration of justice, ... and encompasses even those who have not taken any affirmative action to hinder justice."

Govt. II at 11 (quoting *N.Y. Tel. Co.*, 434 U.S. at 174).

There is no question that the court has the authority under the AWA to compel Apple – or anyone else for that matter – to take action regardless of whether it was involved in the underlying criminal conduct, so long as it does so "under appropriate circumstances." *N.Y. Tel. Co.*, 434 U.S. at 174. But the proposition that Apple's purported ability to "thwart" the government's investigation renders it sufficiently close to the underlying controversy as to make such an order appropriate is ultimately unpersuasive. Apple is not doing anything to keep law enforcement agents from conducting

agencies. But it does highlight the proposition that forcing Apple to compromise the data security measures it offers its customers may adversely affect many who rely on such technology for purposes the government would endorse.

their investigation. Apple has not conspired with Feng to make the data on his device inaccessible.²⁹ More importantly, perhaps, it has not even done what the telephone company did in *N.Y. Tel. Co.* – namely, it has not barred the door to its property to prevent law enforcement agents from entering and performing actions they were otherwise competent to undertake in executing the warrant for themselves.³⁰

Indeed, the government's complaint is precisely that Apple is doing nothing at all. If Feng had not engaged the passcode security on his device, or if the government had been able to secure an order compelling Feng to unlock the phone on pain of contempt sanctions, the government might well be in a position to seize the iPhone's data without Apple's assistance. *See* 2015 WL 5920207, at *5 & n.3.³¹

²⁹ In making this point, I do not simply rest on precise requirements for holding a party liable as a coconspirator. Not only has Apple done nothing wrong in marketing devices with such strong data security features, it has exercised a freedom that Congress explicitly deemed appropriate in balancing the needs of law enforcement against the interests of private industry. Specifically, in writing CALFA, Congress included a provision making clear that the statute "does not authorize any law enforcement agency or office ... to prohibit the adoption of any equipment, facility, service, or feature by ... any manufacturer of telecommunications equipment, or any provider of telecommunications support services." 47 U.S.C. § 1002(b)(1)(B). In other words, CALFA provides that law enforcement agencies cannot do precisely what the government suggests here: dictate to a private company in the business of manufacturing smartphones the extent to which it may install data security features on such devices.

³⁰ In *N.Y. Tel. Co.*, the agents would normally have been able to install the authorized pen register without the company's assistance but for the fact that the subject telephone's wires were so placed as to prevent the agents from gaining surreptitious access. The agents thus needed the telephone company not to provide technical expertise they lacked, but only to step out of the way and let them perform their authorized surveillance on company property. *See* 434 U.S. at 162-63.

³¹ The government argues that a court order compelling Feng to unlock the iPhone would be futile because he claims to have forgotten the passcode. *See* Govt. II at 20. More surprisingly, it takes the position that "[c]ompelled decryption raises significant Fifth Amendment issues and creates risk that the fruit of the compelled decryption could be suppressed." *Id.* at 21. I assume the government is not concerned that such an order of compulsion would violate Feng's Fifth Amendment privilege against self-incrimination. *See* Govt. II at 19 (citing *United States v. I.A.*, 55 F.3d 325, 329 (7th Cir. 1995) for the proposition that "an [AWA] order may be used to require the production of a handwriting exemplar ... even though the subject may face criminal sanctions as a result of his compliance"); *Com. v. Gelfgatt*, 11 N.E.3d 605, 612 (Mass. 2014) (compelling defendant to enter passcode into encrypted computers did not violate the Fifth Amendment right against self-incrimination); *Schmerber v. California*, 384 U.S. 757, 760-65 (1966) (compelled extraction and analysis of blood sample is not compelled testimony and

Thus, Apple is not "thwarting" anything – it is instead merely declining to offer assistance. There may well be some for whom the distinction between a third-party's active obstruction of law enforcement and its passive refusal to help is meaningless as a matter of policy. But it is hardly meaningless as a matter of legal analysis.³² In any event, the distinction is one that precludes a finding that Apple's relationship either to Feng's crime or to the government's investigation of it is sufficiently similar to the telephone company's corresponding role in *N.Y. Tel. Co.* as to justify an order compelling Apple's assistance.³³

therefore does not violate the Fifth Amendment right against self-incrimination). It may well be, as the government suggests, that "[c]ompelled decryption raises significant Fifth Amendment issues" relating to the due process rights of Feng or anyone else who might be compelled to perform such decryption, but I need not address such concerns to resolve the issue now before the court.

³² The distinction also helps to understand why so many of the cases that the government cites as precedent for using the AWA "in support of warrants in a wide variety of contexts[.]" Govt. II at 11-12, offer little if any useful guidance here. In two of the cases, lower courts simply followed *N.Y. Tel. Co.* to order telephone companies to assist with trap and trace devices – orders wholly comparable in every meaningful respect to the pen register order at issue in *N.Y. Tel. Co.* itself. See *In re Application*, 610 F.2d 1148, 1155 (3d Cir. 1979); *In re Application*, 616 F.2d 1122, 1129 (9th Cir. 1980). In four other cases on the government's list, the subject of the order was in possession of evidence of the crime under investigation and was ordered to produce or allow law enforcement access to that evidence – a circumstance wholly inapposite here, as Apple is not alleged to possess any evidence of Feng's crimes. See *United States v. Doe*, 537 F. Supp. 838, 840 (E.D.N.Y. 1982) (telephone company ordered to produce toll records); *United States v. X*, 601 F. Supp. 1039, 1042 (D. Md. 1984) (same); *United States v. Hall*, 583 F. Supp. 717, 722 (E.D. Va. 1984) (bank ordered to produce credit card records); *In re Application of the United States for an Order Directing X to Provide Access to Videotapes*, 2003 WL 22053105, at *3 (D. Md. Aug. 22, 2003) (landlord ordered to provide access to security camera video recordings).

³³ I address below, in the context of analyzing whether the relief sought here is unduly burdensome, the hypothetical example an application under the AWA to compel a drug company that had decided to get out of the business of producing drugs used in executions to supply such drugs to the government if they were otherwise unavailable. At oral argument, the government faulted the hypothetical as "inflammatory," see Tr. at 47, but did not contend that it was unrealistic. Nor could it fairly raise such an objection. Before writing the Court's opinion in opinion in *Glossip v. Gross*, 135 S. Ct. 2726 (2015), Justice Alito posed the following question at oral argument:

JUSTICE ALITO: ... Now, this Court has held that the death penalty is constitutional. It's controversial as a constitutional matter. It certainly is controversial as a policy matter. Those who oppose the death penalty are free to try to persuade legislatures to

c. "Minimum Contacts"

In its post-hearing brief, the government offered no new argument about what Apple has done that renders it close enough to Feng's crime for purposes of *N.Y. Tel. Co.*, but it did posit a new legal standard to apply in considering that discretionary factor. It suggests that all that is required is that Apple have "minimum contacts" – although to what, the government does not say. *See* Govt. III at 6. It wrests that suggestion from the wholly inapposite usage of the phrase in *United States v. Int'l Brotherhood of Teamsters*, 907 F.2d 277, 281 (2d Cir. 1990). As explained below, the argument is unpersuasive.

As another court aptly summarized the nature of the dispute in *Teamsters*:

[T]he All Writs Act was used in *Teamsters* to remove state court litigation so as to aid in the enforcement of a district court's order and to prevent repetitive and burdensome litigation and promote judicial economy, that result was necessary because a consent decree that had been in place for three years was threatened by collateral state lawsuits. The district court determined that an injunction was needed to protect the district court's jurisdiction over the parties to the consent decree, and proceeded under the authority of the All Writs Act.

Nat'l Fuel Gas Supply Corp. v. 138 Acres of Land in Vill. of Springville, City of Erie, State of New York, 186 F. Supp. 2d 339, 345 (W.D.N.Y. 2001).

abolish the death penalty. Some of those efforts have been successful. They're free to ask this Court to overrule the death penalty.

But until that occurs, is it appropriate for the judiciary to countenance what amounts to a guerilla war against the death penalty which consists of efforts to make it impossible for the States to obtain drugs that could be used to carry out capital punishment with little, if any, pain?

Glossip v. Gross, 2015 WL 1929998 (U.S. Apr. 29, 2015) (transcript of oral argument) at *14. If the government can discern in Apple's conduct here a level of obstruction sufficient to allow a court to compel assistance under AWA, Justice Alito's question in *Glossip* would easily provide the basis for a judge to find that a drug company's "guerilla war[fare]" served only to thwart a state's lawful implementation of a constitutionally sound execution, and would therefore make the company eligible for an order of compulsion. The possibility is anything but fanciful.

Thus, in *Teamsters*, there was no question about whether the parties affected by the court's use of an AWA order were too far removed from involvement in the underlying dispute – the question was instead whether the court had personal jurisdiction over those non-parties who were located outside of New York. *See Teamsters*, 907 F.2d at 281. Unsurprisingly, the court answered that question of personal jurisdiction by invoking the applicable constitutional standard for a court's assertion of personal jurisdiction – the "minimum contacts" standard. *See id.* (citing *International Shoe Co. v. Washington*, 326 U.S. 310, 316 (1945)). Here, by contrast, the question is precisely what it was not in *Teamsters*: there is no dispute about the court's personal jurisdiction over Apple, but there is a dispute about whether Apple is too far removed from involvement Feng's conduct to be subject to an order under the AWA.

2. Burdensomeness

The Supreme Court acknowledged in *N.Y. Tel. Co.* that a court exercising its authority under the AWA may not impose "unreasonable burdens" on the subjects of its orders. 434 U.S. at 172. In explaining why compelling the telephone company to help the government install a pen register imposed no such unreasonable burden in that case, the Court wrote the following:

[I]t can hardly be contended that the Company, a highly regulated public utility with a duty to serve the public, had a substantial interest in not providing assistance. Certainly the use of pen registers is by no means offensive to it. The Company concedes that it regularly employs such devices without court order for the purposes of checking billing operations, detecting fraud, and preventing violations of law. It also agreed to supply the FBI with all the information required to install its own pen registers. Nor was the District Court's order in any way burdensome. The order provided that the Company be fully reimbursed at prevailing rates, and compliance with it required minimal effort on the part of the Company and no disruption to its operations.

Id. at 174-75 (citations omitted).

The salient points that the Court highlighted as the basis for finding a lack of unreasonable burdens in *N.Y. Tel. Co.* are virtually all absent here. First, Apple is not a "highly regulated public utility

with a duty to serve the public" – the government does not suggest that it is subject to greater regulation than other businesses, it is not a public utility, and it has a duty is to serve its shareholders rather than the public. Second, Apple has indeed contended that it is in its interest as a private company not to provide the assistance sought here: Apple seeks to succeed in a competitive market by being seen to assume "a leadership role in the protection of its customers' personal data against any form of improper access." Apple I at 4. Further, Apple claims to fear – reasonably or otherwise – that providing the requested assistance in the absence of clear legal authority (as I conclude is lacking) "could threaten the trust between Apple and its customers and substantially tarnish the Apple brand." *Id.*

Third, unlike the pen register at issue in *N.Y. Tel. Co.*, the assistance the government seeks here – bypassing a security measure that Apple affirmatively markets to its customers – is not something that Apple would normally do in the conduct of its own business and is, at least now, plainly "offensive to it." *N.Y. Tel. Co.*, 434 U.S. at 174.³⁴ To be sure, Apple's view of what it finds offensive appears to have changed since the days when it routinely voiced no objection to cooperating with AWA orders, and the government's displeasure with that change is as understandable as it is vehement. But however

³⁴ In considering the burden the requested relief would impose on Apple, it is entirely appropriate to take into account the extent to which the compromise of privacy and data security that Apple promises its customers affects not only its financial bottom line, but also its decisions about the kind of corporation it aspires to be. The fact that the government or a judge might disapprove Apple's preference to safeguard data security and customer privacy over the stated needs of a law enforcement agency is of no moment: in the absence of any other legal constraint, that choice is Apple's to make, and I must take into account the fact that an order compelling Apple to abandon that choice would impose a cognizable burden on the corporation that is wholly distinct from any direct or indirect financial cost of compliance.

late Apple may have come to its current view about the way it wishes to exercise its autonomy, the record offers no reason to question its sincerity.³⁵

Fourth, again unlike the telephone company in *N.Y. Tel. Co.*, which "agreed to supply the FBI with all the information required to install its own pen registers[.]" 434 U.S. at 175, the record suggests that Apple has never offered the government the information needed to bypass an iPhone's passcode security on its own – and would never do so. To the contrary, Apple is clearly staking out the position that as a matter of protecting its customers' privacy and data security (and as a matter of securing the benefits it derives from doing so), it does not want the government or anyone else to have access to the information the government would compel it to use to provide the requested assistance at issue here. Apple has explicitly stated that it will comply with a lawful court order to assist in bypassing the passcode security on Peng's iPhone, *see* Tr. at 10, but it has never hinted that it would prefer to simply let the government have the information necessary to do so.

Fifth, yet again unlike the telephone company in *N.Y. Tel. Co.*, which could install a pen register "with ... minimal effort ... and no disruption to its operations[.]" 434 U.S. at 175, the record

³⁵ I thus respectfully disagree with the government's contention that Apple's objection is not "conscientious" but merely a matter of "its concern with public relations." Govt. III at 5. First, I see no reason why a company that succeeds or fails based largely on its ability to maintain congenial relations with the public – that is, with its potential customers – should not be concerned about public relations. Moreover, for all of the government's manifest outrage, there is simply nothing in the record that leads me to question that Apple's recent stance against being compelled to assist the government in bypassing the security it markets to its customers is anything other than a genuine reflection of both how it perceives its private interest in commercial success and the policy preferences of its leaders. The tension between law enforcement and data security in this case and others like it presents a genuine dilemma for people of good faith – indeed, in congressional testimony on February 25, 2016, the FBI's Director described it as "the hardest question I've seen in government." House of Representatives, Permanent Select Committee on Intelligence, Committee Hearing, 2016 WL 755376 (transcript). The fact that Apple resolves that question in a way not to the government's liking does not mean that it is acting in bad faith, or even that it is necessarily putting selfish interests above the public good. As far as I can discern from the record, it means only that the parties have an honest disagreement about how best to accommodate competing legitimate interests.

demonstrates that bypassing the passcode security of just one iPhone "diverts man hours and hardware and software from Apple's normal business operations." Apple I at 3. And while that burden by itself is not substantial in the case of "a single device in good working order, running an operating system earlier than iOS 8," *id.*, the record of this case makes clear that the burdens the government seeks to impose on Apple under the authority of the AWA are not nearly so limited. The government has already secured such assistance at least 70 times before filing the instant petition, it has a dozen more such applications pending, and it clearly intends to continue seeking assistance that is similarly burdensome – if not far more so – for the foreseeable future. In this context, the government's assurance that "any cumulative burden is minimal and likely to decrease *with regard to the type of relief requested here*[" Govt. II at 16 (emphasis added) is particularly unconvincing: the government predicates its argument on the fact that devices using pre-iOS 8 software are becoming an ever smaller slice of Apple's market. *See id.* But that argument omits the fact that the advent of more recent operating systems has done nothing to slow the government's requests – instead, the government continues to seek orders compelling Apple's assistance in bypassing the passcode security of more recent models and operating systems, notwithstanding the fact that such requests are more burdensome than the one pending here.³⁶

³⁶ Even taking the government's argument at face value, I find it unpersuasive because there are at least two reasons why a court considering the reasonableness of the burdens to be imposed by compelling a private party to assist the government under the AWA should take into account cumulative burdens beyond the financial costs directly associated with carrying out that order in isolation. First, as discussed above, the authority the government asks the court to exercise is essentially legislative in nature – and the record makes clear that the government has chosen to rely on the judiciary to achieve such effectively legislative results. It is therefore all the more important for the court, if it is going to engage in such law-making based on an embrace of the government's understanding of what is "agreeable to the usages and principle of law," to exercise such authority in the same way that a legislature would. Congress typically enacts legislation that imposes ongoing burdens on private parties only after developing a full and transparent record in open hearings about the costs and benefits of the proposed law, based on input from all potential stakeholders. It generally does not (or, at a minimum, should not) impose such burdens based on information received *ex parte*

Thus, the government's argument that the burdens an AWA order here would impose on Apple are as negligible as those imposed on the telephone company in *N.Y. Tel. Co.* cannot withstand scrutiny. The government's remaining arguments against a finding of burden are similarly unpersuasive. The government essentially argues that having reaped the benefits of being an American company, it cannot claim to be burdened by being seen to assist the government. *See* Govt. II at 19 (noting the "significant legal, infrastructural, and political benefits" Apple derives from being an American company, as well as its "recourse to the American courts" and to the protection of "American law enforcement ... when it believes that it has been the victim of a crime"); *id.* at 19-20 ("This Court should not entertain an argument that fulfilling basic civic responsibilities of any American citizen or company ... would 'tarnish' that person's or company's reputation.").

Such argument reflects poorly on a government that exists in part to safeguard the freedom of its citizens – acting as individuals or through the organizations they create – to make autonomous choices about how best to balance societal and private interests in going about their lives and their businesses. The same argument could be used to condemn with equal force any citizen's chosen form of dissent. All American citizens and companies "derive significant legal, infrastructural, and political benefits from [their] status [as such,]" *id.* – but that cannot mean that they are not burdened in a legally

and considered in secret proceedings absent some compelling reason not present here. Congress would undoubtedly consider in this context all of the potential harms to Apple, not just the financial ones; a court should do no less. Second, a court's decision in a case such as this, although plainly not controlling in other cases, can nevertheless have some precedential value. It is therefore entirely possible that a decision in this case that did not take into account the cumulative costs Apple faces as the government increases its reliance on the AWA to force it to provide investigative assistance in case after case would effectively limit Apple's ability to have a future court take such rising burdens, no matter how great, into meaningful consideration.

cognizable way when forced unwillingly to comply with what they sincerely believe to be an unlawful government intrusion.³⁷

Similarly, the government's contention that "the burden associated with compliance with legal process is measured on the direct costs of compliance, not on other more general considerations about reputations or the ramifications of compliance[.]" *id.* at 19, is irreconcilable with the opinion in *N.Y. Tel. Co.* itself. The Court in that case did not just cite the lack of financial burden on the telephone company; instead, it took pains to refute the lower appellate court's stated concern about the "severe threat to the autonomy of third parties who for whatever reason prefer not to render such assistance." 434 U.S. at 171. Indeed, part of its showing in that regard was the observation that the company's installation of a pen register would not be "offensive to it" – an observation that would be wholly

³⁷ In its post-hearing submission, the government discusses the significance to this case, and to the Supreme Court's opinion in *N.Y. Tel. Co.*, of Chief Judge Cardozo's observation that "the citizenry may be called upon to enforce the justice of the State, not faintly and with lagging steps, but honestly and bravely and with whatever implements and facilities are convenient and at hand." *Babington v. Yellow Taxi Corp.*, 250 N.Y. 14, 17 (1928) (quoted in *N.Y. Tel. Co.*, 434 U.S. at 175). As I pointed out at oral argument, *Babington* involved a state statute that explicitly allowed an officer to conscript private assistance. *Babington*, 250 N.Y. at 16 (quoting N.Y. Penal Law (Consol. Laws, c. 40) § 1848: "A person who after having been lawfully commanded to aid an officer in arresting any person ... willfully neglects or refuses to aid such officer is guilty of a misdemeanor."). In *N.Y. Tel. Co.*, in contrast, no such specific authority justified the government's demand for the telephone company's assistance, and the question was whether the AWA provided such authority. The government assures me that such a distinction "is of no moment." Govt. III at 4. As it explains:

[T]he Supreme Court in *N.Y. Telephone Co.* cited *Babington* to emphasize the more general proposition that it is neither improper nor unusual to expect civilians to assist law enforcement. As the *N.Y. Telephone Co.* opinion confirms, just as there is no impropriety in requiring civilian assistance under a statute, there is likewise no impropriety in requiring civilian assistance under the All Writs Act.

Govt. III at 4.

Such argument misses an important point by conflating substantive policy questions with procedural questions about how policy is set. A legislature is of course free to explicitly authorize law enforcement agents to conscript private assistance under such circumstances as the legislature deems fit. But citizens are under no such obligation in the absence of such legislation, and *Babington* cannot help a court to understand whether the All Writs Act can properly be read to permit a judge, rather than a legislature, to compel such assistance.

irrelevant, if not counter-productive, to a decision intended to establish that the only cognizable burdens under the AWA are financial. Finally, the government makes no effort to explain why cognizable burdens should be so limited: as the Court explained in *N.Y. Tel. Co.*, the AWA does not empower a court to impose any burdens that are "unreasonable" – and it said nothing to suggest that only financial burdens could prove unreasonable.

Finally, I return to the point that the Supreme Court addressed in reversing the Second Circuit's decision in *N.Y. Tel. Co.*: the concern that an AWA order compelling a private party to provide service to the government the non-party finds offensive would "pose a severe threat to [their] autonomy[.]" 434 U.S. at 171. As discussed above, the Court concluded that no such threat was posed in that case by the imposition of an obligation on a public utility to perform for the government a task that it would in any event perform in the pursuit of its own business. But the concern about whether the AWA, as construed by the government, would confer on the judiciary an overbroad authority to override individual autonomy cannot be so easily avoided in this case. Nothing in the government's arguments suggests any principled limit on how far a court may go in requiring a person or company to violate the most deeply-rooted values to provide assistance to the government the court deems necessary.

To try to gauge that limit – and to see if one even exists – I deliberately asked the government at oral argument the provocative question noted above, *see* n.34 *supra*, about whether a court could invoke the AWA to force a drug maker to supply lethal injection drugs notwithstanding the manufacturer's conscientious objection to capital punishment. *See* Tr. at 43-48. That the government had no ready answer at oral argument to a question it deemed so inflammatory was not surprising. But even in its post-hearing submission, the government offers nothing more than deflection: "Resolution of the death penalty hypothetical would depend on the particular law, facts, and circumstances if such

a case were to present itself." Govt. III at 5. That is undoubtedly true, but equally unsatisfactory. If the government cannot explain why the authority it seeks here cannot be used, based on the same arguments before this court, to force private citizens to commit what they believe to be the moral equivalent of murder at the government's behest, that in itself suggests a reason to conclude that the government cannot establish a lack of unreasonable burden.

If, as the government would have it, the only cognizable measure of an unreasonable burden in this case is the extent to which Apple might have unreimbursed financial costs arising directly from the work needed to bypass the passcode security on Feng's iPhone, then granting the requested order would not impose an unreasonable burden. But the category of unreasonable burdens is not nearly so narrow, not even as described in the Supreme Court opinion on which the government primarily relies. Taking into account the several other burdens to which Apple objects – burdens that are no less real or cognizable simply because they are harder to quantify – I conclude that granting the government's Application would impose an unreasonable burden on Apple.

3. Necessity

The government contends that it cannot successfully search Feng's device without Apple's assistance. *See* Govt. I at 1-2; Govt. III at 7 ("The government is unable to perform a safe passcode bypass on its own[.]"). If that assertion is true, the government may be entitled to relief under the AWA if it can satisfy the remaining statutory requirements and discretionary factors. But if it is false – if the government has access to resources that would in fact allow it to vindicate this court's jurisdiction without compelling Apple to take action it finds objectionable – that fact would weigh heavily against granting relief. As the movant, it is the government's burden to establish the factual assertions upon which it claims to be entitled to relief. I conclude that it has failed to do so because of

the conflicting evidence in the record about the availability, from private sources other than Apple, of technology that would allow the government to bypass the passcode security on Feng's device.³⁸

In its Application in this case, the government originally asserted that its agents cannot bypass the passcode security of an Apple iPhone. *See* Govt. I at 1-2. Two months earlier, however, in opposing a suppression motion in an unrelated criminal case in this district, the government said something quite different:

[T]he lack of a passcode is not fatal to the government's ability to obtain the records. That is because [the Department of Homeland Security ("DHS"), Homeland Security Investigations ("HSI")] is in possession of technology that would allow its forensic technicians to override the passcode security feature on the Subject iPhone and obtain the data contained therein. In other words, even if HSI agents did not have the defendant's passcode, they would nevertheless have been able to obtain the records stored in the Subject iPhone using specialized software. The software works to bypass the passcode entry requirement and "unlock" the cellular telephone without having to

³⁸ Because I conclude that the government has failed to establish necessity for the reasons set forth below, I need not determine whether its refusal to disclose whether federal intelligence agencies have the ability to unlock Feng's device is an independent basis for finding a lack of necessity. While the government's hesitation to reveal what its intelligence agencies can and cannot do is entirely understandable, and may well be an appropriate exercise of discretion to promote national security, that does not mean that the choice must be cost-free for the government in this litigation. In some contexts, such as where the law imposes an affirmative disclosure obligation on the government, it is reasonable to restrict that obligation to pertinent parts of the executive branch rather than insist that the government is a unitary whole. *See, e.g., United States v. Avellino*, 136 F.3d 249, 255 (2d Cir. 1998) (for purposes of the prohibition against the suppression of materially exculpatory information in a criminal case, imputing to each federal prosecutor constructive knowledge of any information known to any government office "would inappropriately ... adopt a monolithic view of government that would condemn the prosecution of criminal cases to a state of paralysis") (internal quotation marks and citations omitted). But this case is not a matter of the government, in response to some external obligation, seeking to be excused from an unreasonable burden. It is instead a matter of determining whether the government, in coming forward to seek affirmative relief that requires a factual showing, can be allowed to withhold information that might demonstrate the falsity of its assertion. As a legal matter, a court might determine that an intelligence agency's ability to accomplish the technical task at issue here does not render Apple's assistance unnecessary. But to the extent the government seeks to avoid having a court make that legal decision by offering the unconditional assertion that "*the government is unable to perform a safe passcode bypass on its own*[" Govt. III at 7 (emphasis added), it has an obligation to prove that assertion rather than simply tell the court that such inquiry is off limits. *See id.* at 8 ("The government is not required to consult with intelligence agencies[.]").

enter the code. Once the device is "unlocked" all records in it can be accessed and copied.

United States v. Adamou Djibo, 15-CR-0088 (SJ), DF 27 at 5 (government's letter to court dated July 9, 2015). At a hearing on the suppression motion in *Djibo*, the government presented the testimony of a DIIS expert who testified that although the "IP-Box" technology on which the government relied was both "fairly new" and "finicky," he and others had succeeded in using that technology to bypass passcode security on some Apple devices, if not the precise kind seized from *Djibo*. See *United States v. Djibo*, --- F. Supp. 3d ---, 2015 WL 9274916, at *6 (E.D.N.Y. Dec. 16, 2015).³⁹

In response to my questions at oral argument about the tension between the factual assertions the government had offered in the two cases, the government proffered yet a third. Specifically, the government wrote:

The government has consulted with the testifying agent in *Djibo*, who noted that the government's ability to bypass the passcode on an iPhone is highly device-specific, and depends in part on the specific hardware and software in place. The investigators in this case have examined the possibility of using various third-party technologies, including the hacking tool referenced in *Djibo*, and determined that, in this case, using such technology on the Target Phone [*i.e.*, Feng's iPhone] presents a non-trivial risk of data destruction. Specifically, the tool, which serially tests various passcodes until detecting the correct one, could activate the "erase data" feature of the iPhone and render the data in the Target Phone permanently inaccessible. By contrast, in this case, Apple has the unique ability to safely perform a passcode bypass on the Target Phone without risking such data destruction.

Govt. III at 8. In short, the government, having previously stated both that it cannot bypass an Apple's passcode security without Apple's help and that it can do so, now says that it depends – and that what

³⁹ The device at issue in *Djibo* was "an iPhone 5 installed with the iOS 8.1.2 operating system." *Id.* The parties appear to agree that the passcode security on that operating system is harder to bypass – even for Apple – than the software (an iteration of iOS 7) installed on Feng's iPhone 5s. Indeed, at the oral argument in this case, Apple stated that while it could indeed bypass the passcode security on Feng's device, it would be impossible to do so on any device running iOS 8 or later versions of the operating system. Tr. at 58. As the public record of the California action reveals, the government now appears to believe otherwise. See DF 27-2 (government's memorandum in the *California* action) at 4-8 (describing proposed method for Apple to use in bypassing passcode security on a device running iOS 9).

it depends on is not just which device and which operating system is in question, but also on which government expert makes the attempt.

In *Djibo*, the result of that morass of conflicting statements was a finding that the government had failed to establish that it would inevitably have succeeded in bypassing the passcode security on Djibo's iPhone. *Djibo*, 2015 WL 9274916, at *11. That result does not remotely establish the proposition the government supports here – namely, that it is impossible for it to bypass the security of an earlier operating system without Apple's help. What it does establish is simply that the government has made so many conflicting statements in the two cases as to render any single one of them unreliable. Because it is the government's burden, as the movant seeking relief, to demonstrate a basis for granting its request, I necessarily conclude that it has failed to establish that the help it seeks from Apple is necessary for purposes of the test under *N.Y. Tel. Co.*⁴⁰

III. Conclusion

In deciding this motion, I offer no opinion as to whether, in the circumstances of this case or others, the government's legitimate interest in ensuring that no door is too strong to resist lawful entry should prevail against the equally legitimate societal interests arrayed against it here. Those competing

⁴⁰ Even accepting at face value the government's most recent statement – that the government has access to third-party technology that might work in this case but that might also risk data destruction – the history recounted above undermines the government's assertion of necessity in a different way. That is, read in the light of its most recent statement, the government's position in *Djibo* was that it would have inevitably discovered the evidence on the defendant's iPhone because it would have used the IP-Box technology to secure it – notwithstanding the risk that doing so might destroy the evidence being sought (the way in which that proposition undermines the government's assertion of inevitable discovery is an issue in *Djibo* but not in this case). If that is so, that means that there are some cases – demonstrably including *Djibo* – in which Apple's help in bypassing an iPhone's passcode security is unnecessary not because the government will inevitably succeed in securing evidence on its own, but rather because the risk of destroying evidence in the attempt to seize it is acceptable. That begs the question, which the government leaves unanswered here, why such a risk was acceptable in prosecuting Djibo but not acceptable in prosecuting Feng. Thus, even taking the government at the most recent of its words, there is no showing that Apple's assistance will accomplish something that the government itself deems to be a necessity.

values extend beyond the individual's interest in vindicating reasonable expectations of privacy – which is not directly implicated where, as here, it must give way to the mandate of a lawful warrant. They include the commercial interest in conducting a lawful business as its owners deem most productive, free of potentially harmful government intrusion; and the far more fundamental and universal interest – important to individuals as a matter of safety, to businesses as a matter of competitive fairness, and to society as a whole as a matter of national security – in shielding sensitive electronically stored data from the myriad harms, great and small, that unauthorized access and misuse can cause.

How best to balance those interests is a matter of critical importance to our society, and the need for an answer becomes more pressing daily, as the tide of technological advance flows ever farther past the boundaries of what seemed possible even a few decades ago. But that debate must happen today, and it must take place among legislators who are equipped to consider the technological and cultural realities of a world their predecessors could not begin to conceive. It would betray our constitutional heritage and our people's claim to democratic governance for a judge to pretend that our Founders already had that debate, and ended it, in 1789.⁴¹

⁴¹ Indeed, as FBI Director Comey observed in the context of the *California* action:

[W]e have awesome new technology that creates a serious tension between two values we all treasure: privacy and safety. That tension should not be resolved by corporations It also should not be resolved by the FBI It should be resolved by the American people deciding how we want to govern ourselves in a world we have never seen before.... I also hope all Americans will participate in the long conversation we must have about how to both embrace the technology we love and get the safety we need.

James Comey, *We Could Not Look the Survivors in the Eye if We Did Not Follow this Lead*, Lawfare (Feb. 21, 2016, 9:03 p.m.) <https://www.lawfareblog.com/we-could-not-look-survivors-eye-if-we-did-not-follow-lead>. That "long conversation" among "people deciding how we want to govern ourselves in a world we have never seen before" will of course be moot if courts presume to make that decision for the American people based on a perceived assignment of extraordinary authority by 18th Century legislators. Director Comey's salutary call for meaningful public debate can therefore be

Ultimately, the question to be answered in this matter, and in others like it across the country, is not whether the government should be able to force Apple to help it unlock a specific device; it is instead whether the All Writs Act resolves that issue and many others like it yet to come. For the reasons set forth above, I conclude that it does not. The government's motion is denied.

SO ORDERED.

Dated: Brooklyn, New York
February 29, 2016

/s/
JAMES ORENSTEIN
U.S. Magistrate Judge

achieved only by recognizing that the All Writs Act does not serve as a mechanism for courts to give the executive branch authority it fails to secure from the legislature.

Richman, Daniel C. (DO) (OGA)

From: Richman, Daniel C. (DO) (OGA)
Sent: Monday, February 29, 2016 7:00 PM
To: [REDACTED]
Subject: FW: Orenstein Opinion
Attachments: [29] ORDER denying motion.pdf; ATT00001.htm

b6 -2
b7C -2

you'll want to look at Orenstein's opinion before tomorrow Heavy reliance on separation of powers and the AWA. No reason why a NY court shouldn't give the matter a try

From: Oconnell, Sasha C. (DO) (FBI)
Sent: Monday, February 29, 2016 6:46 PM
To: Richman, Daniel C. (DO) (OGA)
Subject: Fwd: Orenstein Opinion

--

----- Original message -----

From: "Raj, Kiran (ODAG)" <Kiran.Raj@usdoj.gov>
Date: 02/29/2016 5:25 PM (GMT-05:00)
To: "Baker, James A. (OGC) (FBI)" [REDACTED]
Cc: "Oconnell, Sasha C. (DO) (FBI)" [REDACTED] "Anderson, Trisha B.(OGC) (FBI)" [REDACTED]
Subject: Fwd: Orenstein Opinion

b7E -3

Sent from my iPhone

Begin forwarded message:

b6 Per DOJ/CRM and EOUSA
b7C Per DOJ/CRM

From: "Komatireddy, Saritha (USANYE)" [REDACTED]
Date: February 29, 2016 at 5:12:39 PM EST
To: "Raj, Kiran (ODAG)" <kraj@jmd.usdoj.gov<mailto:kraj@jmd.usdoj.gov>>, "Bitkower, David" [REDACTED]<[REDACTED]@CRM.USDOJ.GOV<mailto:[REDACTED]@CRM.USDOJ.GOV>>, "Downing, Richard" [REDACTED]<[REDACTED]@CRM.USDOJ.GOV<mailto:[REDACTED]@CRM.USDOJ.GOV>>, "Lynch, John" [REDACTED]<[REDACTED]@CRM.USDOJ.GOV<mailto:[REDACTED]@CRM.USDOJ.GOV>>, "Stawasz, Michael" [REDACTED]<[REDACTED]@CRM.USDOJ.GOV<mailto:[REDACTED]@CRM.USDOJ.GOV>>, "Judish, Nathan" [REDACTED]<[REDACTED]@CRM.USDOJ.GOV<mailto:[REDACTED]@CRM.USDOJ.GOV>>, "Hosid, Jared" [REDACTED]<[REDACTED]@CRM.USDOJ.GOV<mailto:[REDACTED]@CRM.USDOJ.GOV>>, "Pierce, Emily (OPA)" [REDACTED]<epierce@jmd.usdoj.gov<mailto:epierce@jmd.usdoj.gov>>
Cc: "Gatta, James (USANYE)" [REDACTED] "DuCharme, Seth (USANYE)" [REDACTED] "Tucker, Richard" [REDACTED]

FBI 18-CV-1833-6151

(USANYE)" [REDACTED] "Elbert, Lauren (USANYE)"
[REDACTED] "Kabrawala, Ameet (USANYE)"
[REDACTED] , "Jager, Hilary (USANYE)"

Subject [REDACTED]

b5 Per EOUSA

Saritha Komatireddy
Assistant United States Attorney
United States Attorney's Office
Eastern District of New York
271 Cadman Plaza East
Brooklyn, New York 11201
Tel: 718-254-6054
Fax: 718-254-6076
Email: [REDACTED]

b6 Per EOUSA