FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
2nd Interim Release
Civil Action# 18-cv-1833, FOIA 1404359-0

Total Withheld Page(s) = 212

Bates Page Reference	Reason for Withholding (i.e., exemptions with coded rationale, duplicate, sealed by order of court, etc.)
18-cv-1833 – 530-531	Duplicate of 532-533
620-622	Duplicate of 662-664
623-625	Duplicate of 662-664
701-736	Duplicate of 626-661
819-820	Duplicate 821-823
824-825	Duplicate 737-738
826-986	Duplicate 740-818
990-992	Duplicate 993-995

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

[redacted] b7E 3

From: [redacted]
Sent: Wednesday, July 08, 2015 12:34 PM
To: RICHMAN, DANIEL C (DO)(OGA)
Subject: Asset Management System (AMS) Account Assignment - RICHMAN

Classification: UNCLASSIFIED
==========

You have been assigned a self-service account in the Asset Management System (AMS). You may sign in to AMS to view your Personal Inventory Report, update vehicle mileage, or request service from property managers to add, modify, or dispose of FBI property.

To access AMS, type "AMS" into your browser address bar, or access the link at the Finance Division's Asset Management Unit web site. Sign in using your network ID (e.g. jsmith) and password.

This is an automated notification. Replies to this e-mail address will not be answered. If you believe you have received this notification in error, please contact the Asset Management Unit, Finance Division. If you have questions about AMS, please call "Ask Finance!" at [redacted] e-mail [redacted] or submit a ticket using Employee Self Service through Service Manager. When submitting a ticket, enter "AMS" in the Property # field. b7E 3

==========
Classification: UNCLASSIFIED

[redacted](OGC)(FBI) b6 1 b7C 1

From: [redacted](OGC)(FBI)
Sent: Wednesday, August 05, 2015 9:37 AM
To: RICHMAN, DANIEL C (DO)(OGA)
Subject: Expansion of your remit at the FBI --- UNCLASSIFIED//FOUO
Attachments: Richman_Appointment_letter.pdf

Classification: UNCLASSIFIED//FOUO
==========

Sent for Approval for RECORD//Sentinel Case 319T-HQ-A1487667-OGC

Dan,

Our folks would like to expand the projects you are working on to include an examination of the implications of federal investigations being brought to state and local prosecutors. This project will be in addition to the Going Dark work mentioned in your appointment documentation. While Going Dark is obviously an issue for state and local prosecutions and investigations, we believe this topic is distinct enough to warrant documenting that this has now become part of your official tasking. This email will serve as the documentation of the expansion of your role and will supplement the appointment letter (attached) and related correspondence concerning your initial appointment. Everything else in that initial documentation remains the same, including your status as an unpaid SGE.

I am going to upload this to the relevant OGC file on Sentinel so it can be found with the other documentation.

Thanks,

[redacted]

<<Richman_Appointment_letter.pdf>>

(U) [redacted] b6 1 b7C 1

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]

b6 1
b7C 1

==========

Classification: UNCLASSIFIED//FOUO

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

Appointment Letter as a Special Government Employee

Dear Professor Richman,

This confirms your appointment as a consultant of the Office of the General Counsel (OGC). You will advise FBI senior leadership related to the "Going Dark" issue and provide your insight into possible solutions. You will serve without compensation on a part-time and/or intermittent basis; however, you will be provided reimbursement for payment of travel expenses and per diem allowance.

Because you are expected to perform duties as an OGC consultant for no more than 130 days in any 365-day period, you will be classified as a Special Government Employee (SGE). SGEs are government employees subject to some of the laws governing employees of the United States, including the Standards of Ethical Conduct for the Executive Branch and the conflict-of-interests statutes. If, after beginning to serve, it appears that you will perform your duties for more than 130 days during any 365 day period, please alert your FBI sponsor/point-of-contact so that appropriate action may be taken. Enclosed with this letter is a general guide on the ethics rules that apply to SGEs; please review it. Contact the Office of Integrity and Compliance if you have any questions.

You serve at the pleasure of the Director. Your initial term is one year from the date of this letter. You may be reappointed for additional one year terms. By virtue of this appointment, you are required to file a confidential financial disclosure (OGE-450) report with your sponsoring division within 30 calendar days of receipt of this letter, but before any advice or other services are rendered. Please keep in mind that you may not serve as a federally registered lobbyist while serving as an advisor or consultant to the FBI, or engage in conduct that would require you to so register.

If you have any questions regarding the capacity in which you will serve, or any related questions, please contact Associate General Counsel [redacted] I look forward to your participation as a member of OGC and

b6 1
b7C 1

obtaining your guidance and advice on the issues related to existing and emerging communication services and technologies and the overlapping challenges they pose to law enforcement.

Please see the attached general terms of your appointment. Please sign and acknowledge these terms as a condition of your appointment and return to Associate General Counsel [redacted]

b6 1
b7C 1

Thank you for your service to the FBI and the Nation.

Sincerely,

Timothy P. Groh
Deputy Assistant Director
FBI Human Resources Division

I understand that under the conditions of my appointment as a consultant with the Federal Bureau of Investigation:

1. I do not acquire competitive status as a career Federal employee.

2. I will not receive any special consideration for a career position with the Federal Government based on this appointment.

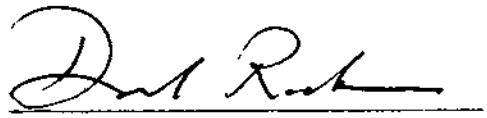
3. I serve at the pleasure of the Director. My initial appointment may not exceed one year, but if required, I may be reappointed for successive one-year terms.

4. I have received and reviewed the Office of Government Ethics (OGE) guide: "To Serve With Honor" A Guide on the Ethics Rules that Apply to Advisory Committee Members Serving as Special Government Employees.

5. I agree to take the OGE training course "Ethics Training for Special Government Employees" available on the internet no later than 30 days after my initial appointment, but before any advice or services are rendered.

6. The terms and conditions regarding remuneration for my services or expenses are set forth in my appointment letter. If I am serving without pay I agree to waive any claims for compensation for my services.

7. I, Daniel Charles Richman, do solemnly swear (or affirm) that I will support and defend the Constitution of the United States against all enemies, foreign and domestic; that I will bear true faith and allegiance to the same; that I take this obligation freely, without any mental reservation or purpose of evasion; and that I will well and faithfully discharge the duties of the office on which I am about to enter, so help me God.



Signature

6/30/2015

Date

[redacted] b7E 3

From: [redacted]
Sent: Friday, September 11, 2015 1:05 PM
To: RICHMAN, DANIEL C (DO)(OGA)
Subject: Interaction SD1409444/15 has been closed and a Customer Satisfaction Survey has been generated for you --- UNCLASSIFIED/~~FOUO~~

Classification: UNCLASSIFIED//~~FOUO~~

==========

ITB Service Manager - Survey Notification

Dear Sir/Madam,

[redacted] Interaction SD1409444/15 has been closed. b7E 7

Your feedback is important to us! Please use the following link to rate our service and provide any comments you may have regarding the service that you have received: Customer Satisfaction Survey

If you have any questions, please contact the Enterprise Operations Center (EOC) EOC Service Desk at [redacted] b7E 3

If you disagree with the solution, you may resubmit the interaction by clicking the following hyperlink: Interaction SD1409444/15

Interaction details are as follows, or you can click the following hyperlink to view the Interaction ticket details: SD1409444/15.

Title:	DOMAIN UNLOCK
Interaction Number:	SD1409444/15
Primary Contact:	RICHMAN DANIEL CHARLES [redacted] b6 4 b7C 4
Service Recipient (if different from Primary Contact):	RICHMAN DANIEL CHARLES [redacted]
Affected CI:	
Affected Service:	b7E 7
Closure Code:	
Closure Comments:	

Area:	
Subarea:	
Impact:	
Urgency:	
Priority:	

Please do not reply to this one-way e-mail.

==========

Classification: UNCLASSIFIED//~~FOUO~~

[redacted] b7E 3

From: [redacted]
Sent: Friday, September 11, 2015 1:07 PM
To: RICHMAN, DANIEL C (DO)(OGA)
Subject: Interaction SD1409489/15 has been closed and a Customer Satisfaction Survey has been generated for you --- UNCLASSIFIED/~~FOUO~~

Classification: UNCLASSIFIED//~~FOUO~~
==========

ITB Service Manager - Survey Notification

Dear Sir/Madam,

[redacted] Interaction SD1409489/15 has been closed. b7E 7

Your feedback is important to us! Please use the following link to rate our service and provide any comments you may have regarding the service that you have received: Customer Satisfaction Survey

If you have any questions, please contact the Enterprise Operations Center (EOC) EOC Service Desk at [redacted] b7E 3

If you disagree with the solution, you may resubmit the interaction by clicking the following hyperlink: Interaction SD1409489/15

Interaction details are as follows, or you can click the following hyperlink to view the Interaction ticket details: SD1409489/15.

Title:	UNET PW RESET.
Interaction Number:	SD1409489/15
Primary Contact:	RICHMAN DANIEL CHARLES [redacted] b6 4 b7C 4
Service Recipient (If different from Primary Contact):	RICHMAN DANIEL CHARLES [redacted]
Affected CI:	b7E 7
Affected Service:	
Closure Code:	
Closure Comments:	

Area:	
Subarea:	
Impact:	
Urgency:	
Priority:	

Please do not reply to this one-way e-mail.

==========

Classification: UNCLASSIFIED/~~FOUO~~

[redacted] b7E 3

From: [redacted]
Sent: Thursday, September 17, 2015 8:21 AM
To: RICHMAN, DANIEL C (DO)(OGA)
Subject: Mandatory Training Assignment Deadline Approaching: Information Security (INFOSEC) Awareness 2015
Importance: High

Dear DANIEL RICHMAN,

The deadline for a completing the following required training assignment is approaching:

Title: Information Security (INFOSEC) Awareness 2015
Type: Online
Training Period: 7/27/2015 8:39 AM - 9/30/2015 11:59 PM

You must complete this assignment by 9/30/2015 11:59 PM. 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.

b7E 3

If you have any questions regarding this training assignment, please contact the Virtual Academy for assistance.

Thank you,
Virtual Academy
Training Division

For Technical Issues: contact EOC Helpdesk [redacted]

[redacted] b7E 3

From: [redacted]
Sent: Thursday, September 10, 2015 2:21 PM
To: RICHMAN, DANIEL C (DO)(OGA)
Subject: Enrollment in Online Course: Information Security (INFOSEC) Awareness 2015

Dear DANIEL RICHMAN,

Your enrollment in the Information Security (INFOSEC) Awareness 2015 online course is confirmed.

The course will appear in the My Learning Plan section under the My Workspace tab until it is completed.

You may access the course by following the link below:

[redacted]

If you have any questions regarding your enrollment in the online course, please contact the Virtual Academy for assistance.

b7E 3

Thank you,
Virtual Academy
Training Division

For Technical Issues: contact EOC Helpdesk, [redacted]

[redacted] b7E 3

From: [redacted]
Sent: Tuesday, October 06, 2015 3:27 PM
To: RICHMAN, DANIEL C (DO)(OGA)
Subject: New Mandatory Training Assignment: Insider Threat and Media Contact Awareness
Importance: High

Dear DANIEL RICHMAN,

You are required to complete the following mandatory training assignment by 1/30/2016 11:59 PM:

Title: Insider Threat and Media Contact Awareness
Type: Online
Training Sponsor: FBI - Inspection Division
Number of Training Hours: .5
Mandate Type: Policy - Other Govt. Agency

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 1/30/2016 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 [redacted] 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.

[redacted] b7E 3

From: [redacted]
Sent: Sunday, November 08, 2015 1:03 AM
To: RICHMAN, DANIEL C (DO)(OGA)
Subject: Incomplete Mandatory Training Assignment: Information Security (INFOSEC) Awareness 2015
Importance: High

Dear DANIEL RICHMAN,

You were assigned the following required training:

Title: Information Security (INFOSEC) Awareness 2015

Type: Online

Training Period: 7/27/2015 8:39 AM - 9/30/2015 11:59 PM.

This assignment was not completed by the due date so you have a status of incomplete for this assignment's training period displayed on your Training Progress option under the My Learning tab.

If you have any questions, please contact the Virtual Academy for assistance.

Thank you,
Virtual Academy
Training Division

For Technical Issues: contact EOC Helpdesk [redacted] b7E 3

[redacted] b7E 3

From: [redacted]
Sent: Sunday, November 08, 2015 2:40 AM
To: RICHMAN, DANIEL C (DO)(OGA)
Subject: Incomplete Mandatory Training Assignment: Information Security (INFOSEC) Awareness 2015
Importance: High

Dear DANIEL RICHMAN,

You were assigned the following required training:

Title: Information Security (INFOSEC) Awareness 2015

Type: Online

Training Period: 7/27/2015 8:39 AM - 9/30/2015 11:59 PM.

This assignment was not completed by the due date so you have a status of incomplete for this assignment's training period displayed on your Training Progress option under the My Learning tab.

If you have any questions, please contact the Virtual Academy for assistance.

Thank you,
Virtual Academy
Training Division

For Technical Issues: contact EOC Helpdesk, [redacted] b7E 3

EPAS

From:	EPAS
Sent:	Friday, November 20, 2015 2:42 PM
To:	RICHMAN, DANIEL C (DO)(OGA)
Subject:	SRSP Update: Thank you for submitting the FD-772 - Foreign Travel form

UNCLASSIFIED

This is an automated message from the Enterprise Process Automation System (EPAS). **Please do not reply to this message.**

Dear DANIEL RICHMAN,

Thank you for submitting the FD-772 - Foreign Travel form. You will be contacted by a Security Officer if any clarification is required. You may review the form by clicking here or by visiting your Items of Interest list in EPAS.

Ticket #: FD772 - 00157250

For additional information please visit the SRSP Bureaupedia page.

[redacted] b7E 3

From: [redacted]
Sent: Monday, December 07, 2015 1:31 PM
To: RICHMAN, DANIEL C (DO)(OGA)
Subject: Interaction SD1549463/15 has been closed and a Customer Satisfaction Survey has been generated for you --- UNCLASSIFIED//~~FOUO~~

Classification: UNCLASSIFIED//~~FOUO~~
==========

ITB Service Manager - Survey Notification

Dear Sir/Madam,

[redacted] Interaction SD1549463/15 has been closed. b7E 7

Your feedback is important to us! Please use the following link to rate our service and provide any comments you may have regarding the service that you have received: Customer Satisfaction Survey

If you have any questions, please contact the Enterprise Operations Center (EOC) EOC Service Desk at [redacted] b7E 3

If you disagree with the solution, you may resubmit the interaction by clicking the following hyperlink: Interaction SD1549463/15

Interaction details are as follows, or you can click the following hyperlink to view the Interaction ticket details: SD1549463/15.

Title:	UNET PW RESET.
Interaction Number:	SD1549463/15
Primary Contact:	RICHMAN DANIEL CHARLES [redacted] b6 4 b7C 4
Service Recipient (If different from Primary Contact):	RICHMAN DANIEL CHARLES [redacted]
Affected CI:	b7E 7
Affected Service:	
Closure Code:	
Closure Comments:	

Area:	
Subarea:	
Impact:	
Urgency:	
Priority:	

b7E 7

Please do not reply to this one-way e-mail.

==========

Classification: UNCLASSIFIED//~~FOUO~~

EPAS

From:	EPAS
Sent:	Saturday, December 19, 2015 12:00 AM
To:	RICHMAN, DANIEL C (DO)(OGA)
Subject:	SRSP Update: URGENT: Please complete your Foreign Travel Debriefing

UNCLASSIFIED

This is an automated message from the Enterprise Process Automation System (EPAS). **Please do not reply to this message.**

Dear DANIEL RICHMAN,

Please submit a foreign travel debriefing form for your foreign travel trip. Make sure to complete the form within five business days. If the debriefing form is not submitted within five days, you will be contacted by your Security Officer. You may submit the form by clicking here or by visiting your To Do list in EPAS. Please select the **Submit** action at the bottom of the form to submit.

Ticket #: FD772b - 00089091

For additional information please visit the SRSP Bureaupedia page.

RICHMAN, DANIEL C (DO)(OGA)

From: RICHMAN, DANIEL C (DO)(OGA)
Sent: Tuesday, December 22, 2015 4:16 PM
To: [redacted](SECD)(CON)
Subject: RE: FD-772 --- UNCLASSIFIED

b6 1
b7C 1

Classification: UNCLASSIFIED
==========

I can confirm that I did this while doing personal travel. And I did submit an FD 772

Thx

Dan richman

From: [redacted](SECD)(CON)
Sent: Friday, December 18, 2015 2:14 PM
To: RICHMAN, DANIEL C (DO)(OGA)
Subject: FD-772 --- UNCLASSIFIED

b6 1
b7C 1

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 EPAS.

Thanks and have a nice day!

[redacted]

Security Specialist

Office of Security Operations

DO, FD, FLSD, INSD, IOD, OGC, OPE, RPO, WMDD

Work: [redacted]

Fax: [redacted]

FBIHQ Suite 1323

b6 1
b7C 1
b7E 3

==========
Classification: UNCLASSIFIED

==========
Classification: UNCLASSIFIED

[redacted] b7E 3

From: [redacted]
Sent: Tuesday, December 22, 2015 5:13 PM
To: RICHMAN, DANIEL C (DO)(OGA)
Subject: Enrollment in Online Course: Annual Standards of Ethical Conduct Training

Dear DANIEL RICHMAN,

Your enrollment in the Annual Standards of Ethical Conduct Training online course is confirmed.

The course will appear in the My Learning Plan section under the My Workspace tab until it is completed.

You may access the course by following the link below:

[redacted] b7E 3

If you have any questions regarding your enrollment in the online course, please contact the Virtual Academy for assistance.

Thank you,
Virtual Academy
Training Division

For Technical Issues: contact EOC Helpdesk, [redacted]

[redacted] (DO) (FBI) b6 1 b7C 1

From: [redacted] (DO) (FBI)
Sent: Wednesday, December 23, 2015 4:09 PM
To: RICHMAN, DANIEL C (DO)(OGA)
Subject: RE: Ethics Training --- UNCLASSIFIED

Classification: UNCLASSIFIED
==========

TRANSITORY RECORD

I sent it to your UNET account.

From: RICHMAN, DANIEL C (DO)(OGA)
Sent: Tuesday, December 22, 2015 5:51 PM
To: [redacted] (DO) (FBI) b6 1 b7C 1
Subject: RE: Ethics Training --- UNCLASSIFIED

Classification: UNCLASSIFIED
==========

TRANSITORY RECORD

Hi [redacted] I just accessed and watch The Squad at the NYO. But I'm having a problem downloading the certificate. Is there any way you can send it to me on 324mail so I can complete the certificate from home?

Thx

Dan richman

From: [redacted] (DO) (FBI) b6 1 b7C 1
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

==========
Classification: UNCLASSIFIED

==========
Classification: UNCLASSIFIED

EPAS

From:	EPAS
Sent:	Tuesday, January 12, 2016 5:16 PM
To:	RICHMAN, DANIEL C (DO) (OGA)
Subject:	SRSP Update: Thank you for submitting the FD-772b - Foreign Travel Debrief form

UNCLASSIFIED

This is an automated message from the Enterprise Process Automation System (EPAS). **Please do not reply to this message.**

Dear DANIEL RICHMAN,

Thank you for submitting the FD-772b - Foreign Travel Debrief form. You will be contacted by a Security Officer if any clarification is required. You may review the form by clicking here or by visiting your Items of Interest list in EPAS.

Ticket #: FD772b - 00089091

For additional information please visit the SRSP Bureaupedia page.

[redacted](NY)(INT)

b6 1
b7C 1

From: [redacted](NY)(INT)
Sent: Tuesday, January 12, 2016 6:05 PM
To: RICHMAN, DANIEL C (DO) (OGA)
Subject: Didn't get the email from you! --- UNCLASSIFIED

Classification: UNCLASSIFIED
==========

==========
Classification: UNCLASSIFIED

RICHMAN, DANIEL C (DO) (OGA)

From: RICHMAN, DANIEL C (DO) (OGA)
Sent: Tuesday, January 12, 2016 6:11 PM
To: [redacted](NY)(INT)
Subject: --- UNCLASSIFIED
Attachments: SEC-102 Foreign Travel Briefing Acknowledgement.pdf

b6 1
b7C 1

Classification: UNCLASSIFIED
==========

TRANSITORY RECORD

<<SEC-102 Foreign Travel Briefing Acknowledgement.pdf>> (U) (U)

==========
Classification: UNCLASSIFIED

SEC-102
V2.0 122015

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:
Daniel Richman	N/A
Assignment (Division and Unit/Office):	**Work Phone Number:**
DO	b6 4 b7C 4

Company or Agency (Contractor/Detailee/TFO only):
Columbia Law School

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

Daniel Richman
Printed Name

Date

Signature

ADMINISTRATIVE USE ONLY (TO BE COMPLETED BY SECURITY OFFICER)

Security Officer Administering FTB

Date SAB Administered

[redacted] (NY)(INT)

From: [redacted] (NY)(INT)
Sent: Wednesday, January 13, 2016 5:41 PM
To: RICHMAN, DANIEL C (DO) (OGA)
Subject: Copy of Foreign Travel Briefing Acknowledgement --- UNCLASSIFIED
Attachments: Foreign Travel Briefing Acknowledgement - [redacted].pdf

b6 1
b7C 1

Classification: UNCLASSIFIED
==========

Here you go!

<<Foreign Travel Briefing Acknowledgement - [redacted] pdf>>

==========
Classification: UNCLASSIFIED

==========
Classification: UNCLASSIFIED

SEC-102
V2.0 122015

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:
Daniel Richman	N/A
Assignment (Division and Unit/Office):	**Work Phone Number:**
DO	b6 4 b7C 4
Company or Agency (Contractor/Detailee/TFO only):	
Columbia Law School	

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

Daniel Richman — Printed Name

1/12/16 — Date

Signature

ADMINISTRATIVE USE ONLY (TO BE COMPLETED BY SECURITY OFFICER)

Security Officer Administering FTB

Date SAB Administered

[redacted] b7E 3

From: [redacted]
Sent: Sunday, January 17, 2016 9:45 AM
To: RICHMAN, DANIEL C (DO) (OGA)
Subject: Mandatory Training Assignment Deadline Approaching: Insider Threat and Media Contact Awareness
Importance: High

Dear DANIEL RICHMAN,

The deadline for a completing the following required training assignment is approaching:

Title: Insider Threat and Media Contact Awareness
Type: Online
Training Period: 10/6/2015 8:36 AM - 1/30/2016 11:59 PM

You must complete this assignment by 1/30/2016 11:59 PM. 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.

If you have any questions regarding this training assignment, please contact the Virtual Academy for assistance.

b7E 3

Thank you,
Virtual Academy
Training Division

For Technical Issues: contact EOC Helpdesk, [redacted]

[redacted] b7E 3

From: [redacted]
Sent: Sunday, February 07, 2016 3:38 AM
To: RICHMAN, DANIEL C (DO) (OGA)
Subject: Incomplete Mandatory Training Assignment: Insider Threat and Media Contact Awareness
Importance: High

Dear DANIEL RICHMAN,

You were assigned the following required training:

Title: Insider Threat and Media Contact Awareness

Type: Online

Training Period: 10/6/2015 8:36 AM - 1/30/2016 11:59 PM.

This assignment was not completed by the due date so you have a status of incomplete for this assignment's training period displayed on your Training Progress option under the My Learning tab.

If you have any questions, please contact the Virtual Academy for assistance.

Thank you,
Virtual Academy
Training Division

For Technical Issues: contact EOC Helpdesk [redacted] b7E 3

[redacted] b7E 3

From: [redacted]
Sent: Sunday, February 07, 2016 5:38 AM
To: RICHMAN, DANIEL C (DO) (OGA)
Subject: Incomplete Mandatory Training Assignment: Insider Threat and Media Contact Awareness
Importance: High

Dear DANIEL RICHMAN,

You were assigned the following required training:

Title: Insider Threat and Media Contact Awareness

Type: Online

Training Period: 10/6/2015 8:36 AM - 1/30/2016 11:59 PM.

This assignment was not completed by the due date so you have a status of incomplete for this assignment's training period displayed on your Training Progress option under the My Learning tab.

If you have any questions, please contact the Virtual Academy for assistance.

Thank you,
Virtual Academy
Training Division

For Technical Issues: contact EOC Helpdesk [redacted] b7E 3

[redacted] b7E 3

From: [redacted]
Sent: Wednesday, February 17, 2016 9:15 PM
To: RICHMAN, DANIEL C (DO) (OGA)
Subject: New Mandatory Training Assignment: Privacy: It's Every Employee's Business
Importance: High

Dear DANIEL RICHMAN,

You are required to complete the following mandatory training assignment by 5/17/2016 11:59 PM:

Title: Privacy: It's Every Employee's Business
Type: Online
Training Sponsor: FBI - Office of the General Counsel
Number of Training Hours: 1.5
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 5/17/2016 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 [redacted] 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.

[redacted] b7E 3

From: [redacted]
Sent: Thursday, February 25, 2016 8:38 PM
To: RICHMAN, DANIEL C (DO) (OGA)
Subject: New Mandatory Training Assignment: Marking Classified National Security Information 2016
Importance: High

Dear DANIEL RICHMAN,

You are required to complete the following mandatory training assignment by 6/30/2016 11:59 PM:

Title: Marking Classified National Security Information 2016
Type: Online
Training Sponsor: FBI - Security Division
Number of Training Hours: .5
Mandate Type: Policy - DOJ/Attorney General

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 6/30/2016 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 [redacted] 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.

[redacted] b7E 3

From: [redacted]
Sent: Tuesday, March 01, 2016 5:51 PM
To: RICHMAN, DANIEL C (DO) (OGA)
Subject: Interaction SD1124374/16 has been closed and a Customer Satisfaction Survey has been generated for you --- UNCLASSIFIED//~~FOUO~~

Classification: UNCLASSIFIED//~~FOUO~~
==========

ITB Service Manager - Survey Notification

Dear Sir/Madam,

[redacted] Interaction SD1124374/16 has been closed. b7E 7

Your feedback is important to us! Please use the following link to rate our service and provide any comments you may have regarding the service that you have received: Customer Satisfaction Survey

If you have any questions, please contact the Enterprise Operations Center (EOC) EOC Service Desk at [redacted] b7E 3

If you disagree with the solution, you may resubmit the interaction by clicking the following hyperlink: Interaction SD1124374/16

Interaction details are as follows, or you can click the following hyperlink to view the Interaction ticket details: SD1124374/16.

Title:	[redacted]
Interaction Number:	SD1124374/16
Primary Contact:	RICHMAN DANIEL CHARLES [redacted]
Service Recipient (If different from Primary Contact):	RICHMAN DANIEL CHARLES [redacted]
Affected CI:	[redacted]
Affected Service:	[redacted]
Closure Code:	
Closure Comments:	[redacted]
Area:	

b6 4
b7C 4
b7E 1

b7E 1, 7

Subarea:	
Impact:	
Urgency:	
Priority:	

b7E 1,7

Please do not reply to this one-way e-mail.

==========

Classification: UNCLASSIFIED//~~FOUO~~

[redacted] b7E 3

From: [redacted]
Sent: Wednesday, March 02, 2016 12:51 PM
To: RICHMAN, DANIEL C (DO) (OGA)
Subject: Interaction SD1125972/16 has been closed and a Customer Satisfaction Survey has been generated for you --- UNCLASSIFIED//~~FOUO~~

Classification: UNCLASSIFIED//~~FOUO~~

==========

ITB Service Manager - Survey Notification

Dear Sir/Madam,

[redacted] Interaction SD1125972/16 has been closed. b7E 7

Your feedback is important to us! Please use the following link to rate our service and provide any comments you may have regarding the service that you have received: Customer Satisfaction Survey

If you have any questions, please contact the Enterprise Operations Center (EOC) EOC Service Desk at [redacted] b7E 3

If you disagree with the solution, you may resubmit the interaction by clicking the following hyperlink: Interaction SD1125972/16

Interaction details are as follows, or you can click the following hyperlink to view the Interaction ticket details: SD1125972/16.

Title:	UNET PW RESET.
Interaction Number:	SD1125972/16
Primary Contact:	RICHMAN DANIEL CHARLES [redacted] b6 4 b7C 4
Service Recipient (If different from Primary Contact):	RICHMAN DANIEL CHARLES [redacted]
Affected CI:	
Affected Service:	b7E 7
Closure Code:	
Closure Comments:	

Area:	
Subarea:	
Impact:	
Urgency:	
Priority:	

b7E 7

Please do not reply to this one-way e-mail.

==========

Classification: UNCLASSIFIED//~~FOUO~~

[redacted] b7E 3

From: [redacted]
Sent: Wednesday, March 02, 2016 12:51 PM
To: RICHMAN, DANIEL C (DO) (OGA)
Subject: Interaction SD1125976/16 has been closed and a Customer Satisfaction Survey has been generated for you --- UNCLASSIFIED//~~FOUO~~

Classification: UNCLASSIFIED//~~FOUO~~
==========

ITB Service Manager - Survey Notification

Dear Sir/Madam,

[redacted] Interaction SD1125976/16 has been closed. b7E 7

Your feedback is important to us! Please use the following link to rate our service and provide any comments you may have regarding the service that you have received: Customer Satisfaction Survey

If you have any questions, please contact the Enterprise Operations Center (EOC) EOC Service Desk at [redacted] b7E 3

If you disagree with the solution, you may resubmit the interaction by clicking the following hyperlink: Interaction SD1125976/16

Interaction details are as follows, or you can click the following hyperlink to view the Interaction ticket details: SD1125976/16.

Title:	[redacted]
Interaction Number:	SD1125976/16
Primary Contact:	RICHMAN DANIEL CHARLES [redacted]
Service Recipient (If different from Primary Contact):	RICHMAN DANIEL CHARLES [redacted]
Affected CI:	[redacted]
Affected Service:	
Closure Code:	[redacted]
Closure Comments:	[redacted]
Area:	[redacted]

b6 4
b7C 4
b7E 1,7

Subarea:	
Impact:	
Urgency:	
Priority:	

b7E 1,7

Please do not reply to this one-way e-mail.

==========

Classification: UNCLASSIFIED/~~/FOUO~~

[redacted] b7E 3

From: [redacted]
Sent: Tuesday, March 15, 2016 2:37 AM
To: RICHMAN, DANIEL C (DO) (OGA)
Subject: New Mandatory Training Assignment: FBI Records Management: Records Management for All
Importance: High

Dear DANIEL RICHMAN,

You are required to complete the following mandatory training assignment by 6/14/2016 11:59 PM:

Title: FBI Records Management: Records Management for All
Type: Online
Training Sponsor: FBI - Records Management Division
Number of Training Hours: 1
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 6/14/2016 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 [redacted] 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.

[redacted] b7E 3

From: [redacted]
Sent: Tuesday, March 22, 2016 12:01 AM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: New Mandatory Training Assignment: Information Security (INFOSEC) Awareness
Importance: High

Dear DANIEL RICHMAN,

You are required to complete the following mandatory training assignment by 7/31/2016 11:59 PM:

Title: Information Security (INFOSEC) Awareness
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 7/31/2016 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 [redacted] 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.

[redacted] b7E 3

From: [redacted]
Sent: Tuesday, March 22, 2016 2:54 AM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: New Mandatory Training Assignment: Information Security (INFOSEC) Awareness
Importance: High

Dear DANIEL RICHMAN,

You are required to complete the following mandatory training assignment by 7/31/2016 11:59 PM:

Title: Information Security (INFOSEC) Awareness
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 7/31/2016 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 [redacted] 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.

[redacted] b7E 3

From: [redacted]
Sent: Wednesday, April 20, 2016 3:18 AM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: Mandatory Training Assignment Deadline Approaching: Privacy: It's Every Employee's Business
Importance: High

Dear DANIEL RICHMAN,

The deadline for a completing the following required training assignment is approaching:

Title: Privacy: It's Every Employee's Business
Type: Online
Training Period: 2/17/2016 8:40 AM - 5/17/2016 11:59 PM

You must complete this assignment by 5/17/2016 11:59 PM. 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.

If you have any questions regarding this training assignment, please contact the Virtual Academy for assistance. b7E 3

Thank you,
Virtual Academy
Training Division

For Technical Issues: contact EOC Helpdesk [redacted]

[redacted] b7E 3

From: [redacted]
Sent: Wednesday, May 11, 2016 4:28 AM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: Mandatory Training Assignment Deadline Approaching: Privacy: It's Every Employee's Business
Importance: High

Dear DANIEL RICHMAN,

The deadline for a completing the following required training assignment is approaching:

Title: Privacy: It's Every Employee's Business
Type: Online
Training Period: 2/17/2016 8:40 AM - 5/17/2016 11:59 PM

You must complete this assignment by 5/17/2016 11:59 PM. 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.

If you have any questions regarding this training assignment, please contact the Virtual Academy for assistance. b7E 3

Thank you,
Virtual Academy
Training Division

For Technical Issues: contact EOC Helpdesk, [redacted]

Mandatory Training Management

From:	Mandatory Training Management
Sent:	Friday, May 20, 2016 9:44 AM
To:	RICHMAN, DANIEL C. (DO) (OGA)
Subject:	Mandatory Training Assignment Deadline Approaching:

Dear DANIEL CHARLES RICHMAN,

The deadline for completing the following required training assignment is approaching:

Title: FBI Records Management: Records Management for All

Type: Web Based Training

You must complete this assignment by 6/14/2016. Please log into the Virtual Academy at [redacted] to complete this assignment. To find your required training list, locate My Training in the gray navigation bar at the top of the page and select My Training Plan from the drop-down menu. b7E 3

If you have any questions regarding this training assignment, please contact the Virtual Academy for assistance.

Thank you,

FBI Virtual Academy

virtualacademy@fbiacademy.edu

Mandatory Training Management

From:	Mandatory Training Management
Sent:	Friday, May 20, 2016 10:42 AM
To:	RICHMAN, DANIEL C. (DO) (OGA)
Subject:	Mandatory Training Assignment Deadline Approaching:

Dear DANIEL CHARLES RICHMAN,

The deadline for completing the following required training assignment is approaching:

Title: FBI Records Management: E-mail Record Marking Tool

Type: Web Based Training

You must complete this assignment by 6/16/2016. Please log into the Virtual Academy at [redacted] to complete this assignment. To find your required training list, locate My Training in the gray navigation bar at the top of the page and select My Training Plan from the drop-down menu. b7E 3

If you have any questions regarding this training assignment, please contact the Virtual Academy for assistance.

Thank you,

FBI Virtual Academy

virtualacademy@fbiacademy.edu

Mandatory Training Management

From:	Mandatory Training Management
Sent:	Friday, May 20, 2016 12:17 PM
To:	RICHMAN, DANIEL C. (DO) (OGA)
Subject:	Past-Due Training Assignment

Dear DANIEL CHARLES RICHMAN,

You were assigned the following required training:

Content Title: Privacy: It's Every Employee's Business

Content Type: Web Based Training

This assignment was not completed by the due date so you have a status of *Past Due* for this assignment's training period displayed on your My Training, Training Progress option under the My Workspace tab.

If you have any questions, please contact the Virtual Academy for assistance.

Thank You,

FBI Virtual Academy

virtualacademy@fbiacademy.edu

Mandatory Training Management

From: Mandatory Training Management
Sent: Wednesday, June 01, 2016 2:46 AM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: Mandatory Training Assignment Deadline Approaching:

Dear DANIEL CHARLES RICHMAN,

The deadline for completing the following required training assignment is approaching:

Title: Marking Classified National Security Information

Type: Web Based Training

You must complete this assignment by 6/30/2016. Please log into the Virtual Academy at [redacted] to complete this assignment. To find your required training list, locate My Training in the gray navigation bar at the top of the page and select My Training Plan from the drop-down menu. b7E 3

If you have any questions regarding this training assignment, please contact the Virtual Academy for assistance.

Thank you,

FBI Virtual Academy

virtualacademy@fbiacademy.edu

Mandatory Training Management

From:	Mandatory Training Management
Sent:	Tuesday, June 07, 2016 11:32 PM
To:	RICHMAN, DANIEL C. (DO) (OGA)
Subject:	Mandatory Training Assignment Deadline Approaching:

Dear DANIEL CHARLES RICHMAN,

The deadline for completing the following required training assignment is approaching:

Title: FBI Records Management: Records Management for All

Type: Web Based Training

You must complete this assignment by 6/14/2016. Please log into the Virtual Academy at [redacted] to complete this assignment. To find your required training list, locate My Training in the gray navigation bar at the top of the page and select My Training Plan from the drop-down menu. b7E 3

If you have any questions regarding this training assignment, please contact the Virtual Academy for assistance.

Thank you,

FBI Virtual Academy

virtualacademy@fbiacademy.edu

Mandatory Training Management

From:	Mandatory Training Management
Sent:	Thursday, June 09, 2016 11:25 PM
To:	RICHMAN, DANIEL C. (DO) (OGA)
Subject:	Mandatory Training Assignment Deadline Approaching:

Dear DANIEL CHARLES RICHMAN,

The deadline for completing the following required training assignment is approaching:

Title: FBI Records Management: E-mail Record Marking Tool

Type: Web Based Training

You must complete this assignment by 6/16/2016. Please log into the Virtual Academy at [redacted] to complete this assignment. To find your required training list, locate My Training in the gray navigation bar at the top of the page and select My Training Plan from the drop-down menu. b7E 3

If you have any questions regarding this training assignment, please contact the Virtual Academy for assistance.

Thank you,

FBI Virtual Academy

virtualacademy@fbiacademy.edu

[redacted] b7E 3

From: [redacted]
Sent: Tuesday, June 14, 2016 2:49 PM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: Interaction SD1316171/16 has been closed and a Customer Satisfaction Survey has been generated for you --- UNCLASSIFIED//~~FOUO~~

Classification: UNCLASSIFIED//~~FOUO~~

==========

ITB Service Manager - Survey Notification

Dear Sir/Madam,

[redacted] Interaction SD1316171/16 has been closed. b7E 7

Your feedback is important to us! Please use the following link to rate our service and provide any comments you may have regarding the service that you have received: Customer Satisfaction Survey

If you have any questions, please contact the Enterprise Operations Center (EOC) EOC Service Desk at [redacted] b7E 3

If you disagree with the solution, you may resubmit the interaction by clicking the following hyperlink: Interaction SD1316171/16

Interaction details are as follows, or you can click the following hyperlink to view the Interaction ticket details: SD1316171/16.

Title:	FBINET DOMAIN PW RESET.
Interaction Number:	SD1316171/16
Primary Contact:	RICHMAN DANIEL CHARLES [redacted] b6 4 b7C 4
Service Recipient (If different from Primary Contact):	RICHMAN DANIEL CHARLES [redacted]
Affected CI:	b7E 7
Affected Service:	
Closure Code:	
Closure Comments:	

Area:	
Subarea:	
Impact:	
Urgency:	
Priority:	

b7E 7

Please do not reply to this one-way e-mail.

==========

Classification: UNCLASSIFIED//~~FOUO~~

Mandatory Training Management

From:	Mandatory Training Management
Sent:	Tuesday, June 14, 2016 11:23 PM
To:	RICHMAN, DANIEL C. (DO) (OGA)
Subject:	Mandatory Training Assignment Deadline Approaching:

Dear DANIEL CHARLES RICHMAN,

The deadline for completing the following required training assignment is approaching:

Title: FBI Records Management: Records Management for All

Type: Web Based Training

You must complete this assignment by 6/14/2016. Please log into the Virtual Academy at [redacted] to complete this assignment. To find your required training list, locate My Training in the gray navigation bar at the top of the page and select My Training Plan from the drop-down menu. b7E 3

If you have any questions regarding this training assignment, please contact the Virtual Academy for assistance.

Thank you,

FBI Virtual Academy

virtualacademy@fbiacademy.edu

Mandatory Training Management

From:	Mandatory Training Management
Sent:	Wednesday, June 15, 2016 11:29 PM
To:	RICHMAN, DANIEL C. (DO) (OGA)
Subject:	Past-Due Training Assignment

Dear DANIEL CHARLES RICHMAN,

You were assigned the following required training:

Content Title: FBI Records Management: Records Management for All

Content Type: Web Based Training

This assignment was not completed by the due date so you have a status of *Past Due* for this assignment's training period displayed on your My Training, Training Progress option under the My Workspace tab.

If you have any questions, please contact the Virtual Academy for assistance.

Thank You,

FBI Virtual Academy

virtualacademy@fbiacademy.edu

Mandatory Training Management

From:	Mandatory Training Management
Sent:	Thursday, June 16, 2016 11:17 PM
To:	RICHMAN, DANIEL C. (DO) (OGA)
Subject:	Mandatory Training Assignment Deadline Approaching:

Dear DANIEL CHARLES RICHMAN,

The deadline for completing the following required training assignment is approaching:

Title: FBI Records Management: E-mail Record Marking Tool

Type: Web Based Training

You must complete this assignment by 6/16/2016. Please log into the Virtual Academy at [redacted] to complete this assignment. To find your required training list, locate My Training in the gray navigation bar at the top of the page and select My Training Plan from the drop-down menu. b7E 3

If you have any questions regarding this training assignment, please contact the Virtual Academy for assistance.

Thank you,

FBI Virtual Academy

virtualacademy@fbiacademy.edu

Mandatory Training Management

From: Mandatory Training Management
Sent: Friday, June 17, 2016 11:37 PM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: Past-Due Training Assignment

Dear DANIEL CHARLES RICHMAN,

You were assigned the following required training:

Content Title: FBI Records Management: E-mail Record Marking Tool

Content Type: Web Based Training

This assignment was not completed by the due date so you have a status of *Past Due* for this assignment's training period displayed on your My Training, Training Progress option under the My Workspace tab.

If you have any questions, please contact the Virtual Academy for assistance.

Thank You,

FBI Virtual Academy

virtualacademy@fbiacademy.edu

Mandatory Training Management

From:	Mandatory Training Management
Sent:	Friday, June 24, 2016 12:19 AM
To:	RICHMAN, DANIEL C. (DO) (OGA)
Subject:	Mandatory Training Assignment Deadline Approaching:

Dear DANIEL CHARLES RICHMAN,

The deadline for completing the following required training assignment is approaching:

Title: Marking Classified National Security Information

Type: Web Based Training

You must complete this assignment by 6/30/2016. Please log into the Virtual Academy at [redacted] to complete this assignment. To find your required training list, locate My Training in the gray navigation bar at the top of the page and select My Training Plan from the drop-down menu. b7E 3

If you have any questions regarding this training assignment, please contact the Virtual Academy for assistance.

Thank you,

FBI Virtual Academy

virtualacademy@fbiacademy.edu

Mandatory Training Management

From:	Mandatory Training Management
Sent:	Friday, July 01, 2016 12:17 AM
To:	RICHMAN, DANIEL C. (DO) (OGA)
Subject:	Mandatory Training Assignment Deadline Approaching:

Dear DANIEL CHARLES RICHMAN,

The deadline for completing the following required training assignment is approaching:

Title: Marking Classified National Security Information

Type: Web Based Training

You must complete this assignment by 6/30/2016. Please log into the Virtual Academy at [redacted] to complete this assignment. To find your required training list, locate My Training in the gray navigation bar at the top of the page and select My Training Plan from the drop-down menu. b7E 3

If you have any questions regarding this training assignment, please contact the Virtual Academy for assistance.

Thank you,

FBI Virtual Academy

virtualacademy@fbiacademy.edu

Mandatory Training Management

From: Mandatory Training Management
Sent: Saturday, July 02, 2016 2:34 AM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: Mandatory Training Assignment Deadline Approaching:

Dear DANIEL CHARLES RICHMAN,

The deadline for completing the following required training assignment is approaching:

Title: Information Security (INFOSEC) Awareness

Type: Web Based Training

You must complete this assignment by 7/31/2016. Please log into the Virtual Academy at [redacted] to complete this assignment. To find your required training list, locate My Training in the gray navigation bar at the top of the page and select My Training Plan from the drop-down menu. b7E 3

If you have any questions regarding this training assignment, please contact the Virtual Academy for assistance.

Thank you,

FBI Virtual Academy

virtualacademy@fbiacademy.edu

Mandatory Training Management

From:	Mandatory Training Management
Sent:	Saturday, July 02, 2016 9:48 AM
To:	RICHMAN, DANIEL C. (DO) (OGA)
Subject:	Past-Due Training Assignment

Dear DANIEL CHARLES RICHMAN,

You were assigned the following required training:

Content Title: Marking Classified National Security Information

Content Type: Web Based Training

This assignment was not completed by the due date so you have a status of *Past Due* for this assignment's training period displayed on your My Training, Training Progress option under the My Workspace tab.

If you have any questions, please contact the Virtual Academy for assistance.

Thank You,

FBI Virtual Academy

virtualacademy@fbiacademy.edu

Mandatory Training Management

From:	Mandatory Training Management
Sent:	Monday, July 25, 2016 2:40 AM
To:	RICHMAN, DANIEL C. (DO) (OGA)
Subject:	Mandatory Training Assignment Deadline Approaching:

Dear DANIEL CHARLES RICHMAN,

The deadline for completing the following required training assignment is approaching:

Title: Information Security (INFOSEC) Awareness

Type: Web Based Training

You must complete this assignment by 7/31/2016. Please log into the Virtual Academy at [redacted] to complete this assignment. To find your required training list, locate My Training in the gray navigation bar at the top of the page and select My Training Plan from the drop-down menu. b7E 3

If you have any questions regarding this training assignment, please contact the Virtual Academy for assistance.

Thank you,

FBI Virtual Academy

virtualacademy@fbiacademy.edu

Mandatory Training Management

From:	Mandatory Training Management
Sent:	Monday, August 01, 2016 12:19 AM
To:	RICHMAN, DANIEL C. (DO) (OGA)
Subject:	Mandatory Training Assignment Deadline Approaching:

Dear DANIEL CHARLES RICHMAN,

The deadline for completing the following required training assignment is approaching:

Title: Information Security (INFOSEC) Awareness

Type: Web Based Training

You must complete this assignment by 7/31/2016. Please log into the Virtual Academy at [redacted] to complete this assignment. To find your required training list, locate My Training in the gray navigation bar at the top of the page and select My Training Plan from the drop-down menu. b7E 3

If you have any questions regarding this training assignment, please contact the Virtual Academy for assistance.

Thank you,

FBI Virtual Academy

virtualacademy@fbiacademy.edu

Mandatory Training Management

From:	Mandatory Training Management
Sent:	Tuesday, August 02, 2016 12:47 AM
To:	RICHMAN, DANIEL C. (DO) (OGA)
Subject:	Past-Due Training Assignment

Dear DANIEL CHARLES RICHMAN,

You were assigned the following required training:

Content Title: Information Security (INFOSEC) Awareness

Content Type: Web Based Training

This assignment was not completed by the due date so you have a status of *Past Due* for this assignment's training period displayed on your My Training, Training Progress option under the My Workspace tab.

If you have any questions, please contact the Virtual Academy for assistance.

Thank You,

FBI Virtual Academy

virtualacademy@fbiacademy.edu

[redacted] b7E 3

From: [redacted]
Sent: Tuesday, August 30, 2016 9:55 AM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: FBINet Password Expiration Notification --- UNCLASSIFIED
Importance: High

Classification: UNCLASSIFIED
==========

FBINet Password Expiration Notice

Dear DANIEL RICHMAN,

b7E 1, 3

Your password on FBINet will expire in 14 day(s). Please change it as soon as possible to make sure your account does not get locked out.

[redacted]

*** Please do not respond to this email ***
Direct any questions or concerns regarding this issue to the EOC Help Desk at [redacted]

==========
Classification: UNCLASSIFIED

[redacted] b7E 3

From: [redacted]
Sent: Wednesday, August 31, 2016 9:52 AM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: FBINet Password Expiration Notification --- UNCLASSIFIED
Importance: High

Classification: UNCLASSIFIED
==========

FBINet Password Expiration Notice

Dear DANIEL RICHMAN, b7E 1, 3

Your password on FBINet will expire in 13 day(s). Please change it as soon as possible to make sure your account does not get locked out.

[redacted]

*** Please do not respond to this email ***
Direct any questions or concerns regarding this issue to the EOC Help Desk at [redacted]

==========
Classification: UNCLASSIFIED

[redacted] b7E 3

From: [redacted]
Sent: Thursday, September 01, 2016 9:55 AM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: FBINet Password Expiration Notification --- UNCLASSIFIED
Importance: High

Classification: UNCLASSIFIED
==========

FBINet Password Expiration Notice

Dear DANIEL RICHMAN,

Your password on FBINet will expire in 12 day(s). Please change it as soon as possible to make sure your account does not get locked out. b7E 1, 3

[redacted]

*** Please do not respond to this email ***
Direct any questions or concerns regarding this issue to the EOC Help Desk a[redacted]

==========
Classification: UNCLASSIFIED

[redacted] b7E 3

From: [redacted]
Sent: Friday, September 02, 2016 9:56 AM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: FBINet Password Expiration Notification --- UNCLASSIFIED
Importance: High

Classification: UNCLASSIFIED
==========

FBINet Password Expiration Notice

Dear DANIEL RICHMAN,

b7E 1, 3

Your password on FBINet will expire in 11 day(s). Please change it as soon as possible to make sure your account does not get locked out.

[redacted]

*** Please do not respond to this email ***
Direct any questions or concerns regarding this issue to the EOC Help Desk at [redacted]

==========
Classification: UNCLASSIFIED

[redacted] b7E 3

From: [redacted]
Sent: Saturday, September 03, 2016 9:55 AM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: FBINet Password Expiration Notification --- UNCLASSIFIED
Importance: High

Classification: UNCLASSIFIED
==========

FBINet Password Expiration Notice

Dear DANIEL RICHMAN,

Your password on FBINet will expire in 10 day(s). Please change it as soon as possible to make sure your account does not get locked out. b7E 1, 3

[redacted]

*** Please do not respond to this email ***
Direct any questions or concerns regarding this issue to the EOC Help Desk at [redacted]

==========
Classification: UNCLASSIFIED

[redacted] b7E 3

From: [redacted]
Sent: Sunday, September 04, 2016 9:43 AM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: FBINet Password Expiration Notification --- UNCLASSIFIED
Importance: High

Classification: UNCLASSIFIED
==========

FBINet Password Expiration Notice

Dear DANIEL RICHMAN,

Your password on FBINet will expire in nine day(s). Please change it as soon as possible to make sure your account does not get locked out. b7E 1, 3

[redacted]

*** Please do not respond to this email ***
Direct any questions or concerns regarding this issue to the EOC Help Desk a[redacted]

==========
Classification: UNCLASSIFIED

[redacted] b7E 3

From: [redacted]
Sent: Monday, September 05, 2016 9:54 AM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: FBINet Password Expiration Notification --- UNCLASSIFIED
Importance: High

Classification: UNCLASSIFIED
==========

FBINet Password Expiration Notice

Dear DANIEL RICHMAN,

Your password on FBINet will expire in eight day(s). Please change it as soon as possible to make sure your account does not get locked out. b7E 1, 3

[redacted]

*** Please do not respond to this email ***
Direct any questions or concerns regarding this issue to the EOC Help Desk at [redacted]

==========
Classification: UNCLASSIFIED

[redacted] b7E 3

From: [redacted]
Sent: Tuesday, September 06, 2016 10:03 AM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: FBINet Password Expiration Notification --- UNCLASSIFIED
Importance: High

Classification: UNCLASSIFIED
==========

FBINet Password Expiration Notice

Dear DANIEL RICHMAN,

Your password on FBINet will expire in seven day(s). Please change it as soon as possible to make sure your account does not get locked out. b7E 1, 3

[redacted]

*** Please do not respond to this email ***
Direct any questions or concerns regarding this issue to the EOC Help Desk at [redacted]

==========
Classification: UNCLASSIFIED

[redacted] b7E 3

From: [redacted]
Sent: Wednesday, September 07, 2016 10:21 AM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: FBINet Password Expiration Notification --- UNCLASSIFIED
Importance: High

Classification: UNCLASSIFIED
==========

FBINet Password Expiration Notice

Dear DANIEL RICHMAN,

Your password on FBINet will expire in six day(s). Please change it as soon as possible to make sure your account does not get locked out. b7E 1, 3

[redacted]

*** Please do not respond to this email ***
Direct any questions or concerns regarding this issue to the EOC Help Desk at [redacted]

==========
Classification: UNCLASSIFIED

[redacted] b7E 3

From: [redacted]
Sent: Thursday, September 08, 2016 9:17 AM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: FBINet Password Expiration Notification --- UNCLASSIFIED
Importance: High

Classification: UNCLASSIFIED

FBINet Password Expiration Notice

Dear DANIEL RICHMAN,

Your password on FBINet will expire in five day(s). Please change it as soon as possible to make sure your account does not get locked out. b7E 1, 3

[redacted]

*** Please do not respond to this email ***
Direct any questions or concerns regarding this issue to the EOC Help Desk at [redacted]

Classification: UNCLASSIFIED

[redacted] b7E 3

From: [redacted]
Sent: Friday, September 09, 2016 9:14 AM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: FBINet Password Expiration Notification --- UNCLASSIFIED
Importance: High

Classification: UNCLASSIFIED
==========

FBINet Password Expiration Notice

Dear DANIEL RICHMAN,

Your password on FBINet will expire in four day(s). Please change it as soon as possible to make sure your account does not get locked out. b7E 1, 3

[redacted]

*** Please do not respond to this email ***
Direct any questions or concerns regarding this issue to the EOC Help Desk at [redacted]

==========
Classification: UNCLASSIFIED

[redacted] b7E 3

From: [redacted]
Sent: Saturday, September 10, 2016 9:58 AM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: FBINet Password Expiration Notification --- UNCLASSIFIED
Importance: High

Classification: UNCLASSIFIED

FBINet Password Expiration Notice

Dear DANIEL RICHMAN,

Your password on FBINet will expire in three day(s). Please change it as soon as possible to make sure your account does not get locked out. b7E 1, 3

[redacted]

*** Please do not respond to this email ***
Direct any questions or concerns regarding this issue to the EOC Help Desk at [redacted]

Classification: UNCLASSIFIED

[redacted] b7E 3

From: [redacted]
Sent: Sunday, September 11, 2016 9:13 AM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: FBINet Password Expiration Notification --- UNCLASSIFIED
Importance: High

Classification: UNCLASSIFIED
==========

FBINet Password Expiration Notice

Dear DANIEL RICHMAN,

Your password on FBINet will expire in two day(s). Please change it as soon as possible to make sure your account does not get locked out. b7E 1, 3

[redacted]

*** Please do not respond to this email ***
Direct any questions or concerns regarding this issue to the EOC Help Desk a[redacted]

==========
Classification: UNCLASSIFIED

[redacted] b7E 3

From: [redacted]
Sent: Monday, September 12, 2016 9:16 AM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: FBINet Password Expiration Notification --- UNCLASSIFIED
Importance: High

Classification: UNCLASSIFIED

FBINet Password Expiration Notice

Dear DANIEL RICHMAN,

Your password on FBINet will expire in one day(s). Please change it as soon as possible to make sure your account does not get locked out. b7E 1, 3

[redacted]

*** Please do not respond to this email ***
Direct any questions or concerns regarding this issue to the EOC Help Desk at [redacted]

Classification: UNCLASSIFIED

[redacted] b7E 3

From: [redacted]
Sent: Wednesday, September 14, 2016 3:42 PM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: Interaction SD1444257/16 has been closed and a Customer Satisfaction Survey has been generated for you --- UNCLASSIFIED//~~FOUO~~

Classification: UNCLASSIFIED//~~FOUO~~
==========

ITB Service Manager - Survey Notification

Dear Sir/Madam,

[redacted] Interaction SD1444257/16 has been closed. b7E 7

Your feedback is important to us! Please use the following link to rate our service and provide any comments you may have regarding the service that you have received: Customer Satisfaction Survey

If you have any questions, please contact the Enterprise Operations Center (EOC) EOC Service Desk at [redacted] b7E 3

If you disagree with the solution, you may resubmit the interaction by clicking the following hyperlink: Interaction SD1444257/16

Interaction details are as follows, or you can click the following hyperlink to view the Interaction ticket details: SD1444257/16.

Title:	UNET PW UNLOCK.
Interaction Number:	SD1444257/16
Primary Contact:	RICHMAN DANIEL CHARLES [redacted] b6 4 b7C 4
Service Recipient (If different from Primary Contact):	RICHMAN DANIEL CHARLES [redacted]
Affected CI:	b7E 7
Affected Service:	
Closure Code:	
Closure Comments:	

Area:	
Subarea:	
Impact:	
Urgency:	
Priority:	

b7E 7

Please do not reply to this one-way e-mail.

==========

Classification: UNCLASSIFIED//~~FOUO~~

[redacted] b7E 3

From: [redacted]
Sent: Wednesday, September 14, 2016 3:42 PM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: Interaction SD1444257/16 has been updated --- UNCLASSIFIED//~~FOUO~~

Classification: UNCLASSIFIED//~~FOUO~~
==========

ITB Service Manager - Interaction Notification

Dear Sir/Madam,

Interaction SD1444257/16 has been updated.

Please click the following hyperlink to view the details or to update the ticket: Interaction SD1444257/16.

If you have any questions, please contact the Enterprise Operations Center:
EOC Service Desk
[redacted] b7E 3

Please do not reply to this one-way e-mail.

Interaction details are as follows:

Title:	UNET PW UNLOCK.
Primary Contact:	RICHMAN DANIEL CHARLES [redacted] b6 4 b7C 4
Service Recipient (If different from Primary Contact):	RICHMAN DANIEL CHARLES [redacted]
Affected CI:	
Affected Service:	b7E 7
Subservice:	
Subservice Type:	
Ticket Status:	
Network Enclave:	
Category:	
Area:	

Subarea:	
Impact:	
Urgency:	
Priority:	

b7E 7

Please do not reply to this one-way e-mail.

==========

Classification: UNCLASSIFIED//~~FOUO~~

Mandatory Training Management

From:	Mandatory Training Management
Sent:	Thursday, September 29, 2016 5:17 AM
To:	RICHMAN, DANIEL C. (DO) (OGA)
Subject:	Required Training Assignment Cancelled/Exempted

Dear DANIEL CHARLES RICHMAN,

The following training assignment has been cancelled therefor, you are no longer required to take it:

Title: No Fear

Type: Web Based Training

Assignment Date: 12/31/2016

Cancellation Date: 9/29/2016

You are no longer responsible for satisfying this required training assignment during this period and it has been removed from your Learning Plan.

If you have any questions, please contact the Virtual Academy for assistance.

Thank You,

FBI Virtual Academy

virtualacademy@fbiacademy.edu

Mandatory Training Management

From:	Mandatory Training Management
Sent:	Thursday, October 06, 2016 10:05 AM
To:	RICHMAN, DANIEL C. (DO) (OGA)
Subject:	New Training Assignment

Dear DANIEL CHARLES RICHMAN,

You are required to complete the following mandatory training assignment by 1/31/2017.

Title: Insider Threat and Media Contact Awareness

Type: Web Based Training

Training Sponsor: FBI - Inspection Division

Number Of Training Hours: 0.5

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 gray 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 before midnight (Eastern Time) on 1/31/2017; 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 Learning Plan. Please note, the moment you complete a WBT, it will show as complete under My Training, 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 [redacted] who will create a ticket and route it to the VA staff.

Thank You,

FBI Virtual Academy

virtualacademy@fbiacademy.edu

[redacted] b7E 3

From: [redacted]
Sent: Monday, December 12, 2016 10:09 AM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: FBINet Password Expiration Notification --- UNCLASSIFIED
Importance: High

Classification: UNCLASSIFIED
==========

FBINet Password Expiration Notice

Dear DANIEL RICHMAN,

Your password on FBINet will expire in 14 day(s). Please change it as soon as possible to make sure your account does not get locked out. b7E 1, 3

[redacted]

*** Please do not respond to this email ***
Direct any questions or concerns regarding this issue to the EOC Help Desk at [redacted]

==========
Classification: UNCLASSIFIED

[redacted] b7E 3

From: [redacted]
Sent: Tuesday, December 13, 2016 10:13 AM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: FBINet Password Expiration Notification --- UNCLASSIFIED
Importance: High

Classification: UNCLASSIFIED
==========

FBINet Password Expiration Notice

Dear DANIEL RICHMAN,

Your password on FBINet will expire in 13 day(s). Please change it as soon as possible to make sure your account does not get locked out. b7E 1, 3

[redacted]

*** Please do not respond to this email ***
Direct any questions or concerns regarding this issue to the EOC Help Desk at [redacted]

==========
Classification: UNCLASSIFIED

[redacted] b7E 3

From: [redacted]
Sent: Wednesday, December 14, 2016 9:17 AM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: FBINet Password Expiration Notification --- UNCLASSIFIED
Importance: High

Classification: UNCLASSIFIED
==========

FBINet Password Expiration Notice

Dear DANIEL RICHMAN,

Your password on FBINet will expire in 12 day(s). Please change it as soon as possible to make sure your account does not get locked out. b7E 1, 3

[redacted]

*** Please do not respond to this email ***
Direct any questions or concerns regarding this issue to the EOC Help Desk at [redacted]

==========
Classification: UNCLASSIFIED

[redacted] b7E 3

From: [redacted]
Sent: Thursday, December 15, 2016 9:17 AM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: FBINet Password Expiration Notification --- UNCLASSIFIED
Importance: High

Classification: UNCLASSIFIED
==========

FBINet Password Expiration Notice

Dear DANIEL RICHMAN,

Your password on FBINet will expire in 11 day(s). Please change it as soon as possible to make sure your account does not get locked out. b7E 1, 3

[redacted]

*** Please do not respond to this email ***
Direct any questions or concerns regarding this issue to the EOC Help Desk at [redacted]

==========
Classification: UNCLASSIFIED

[redacted] b7E 3

From: [redacted]
Sent: Friday, December 16, 2016 9:16 AM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: FBINet Password Expiration Notification --- UNCLASSIFIED
Importance: High

Classification: UNCLASSIFIED
==========

FBINet Password Expiration Notice

Dear DANIEL RICHMAN,

Your password on FBINet will expire in 10 day(s). Please change it as soon as possible to make sure your account does not get locked out. b7E 1, 3

[redacted]

*** Please do not respond to this email ***
Direct any questions or concerns regarding this issue to the EOC Help Desk at [redacted]

==========
Classification: UNCLASSIFIED

[redacted] b7E 3

From: [redacted]
Sent: Saturday, December 17, 2016 9:12 AM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: FBINet Password Expiration Notification --- UNCLASSIFIED
Importance: High

Classification: UNCLASSIFIED
==========

FBINet Password Expiration Notice

Dear DANIEL RICHMAN,

Your password on FBINet will expire in nine day(s). Please change it as soon as possible to make sure your account does not get locked out. b7E 1, 3

[redacted]

*** Please do not respond to this email ***
Direct any questions or concerns regarding this issue to the EOC Help Desk at [redacted]

==========
Classification: UNCLASSIFIED

[redacted] b7E 3

From: [redacted]
Sent: Sunday, December 18, 2016 10:01 AM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: FBINet Password Expiration Notification --- UNCLASSIFIED
Importance: High

Classification: UNCLASSIFIED
==========

FBINet Password Expiration Notice

Dear DANIEL RICHMAN,

Your password on FBINet will expire in eight day(s). Please change it as soon as possible to make sure your account does not get locked out. b7E 1, 3

[redacted]

*** Please do not respond to this email ***
Direct any questions or concerns regarding this issue to the EOC Help Desk at [redacted]

==========
Classification: UNCLASSIFIED

[redacted] b7E 3

From: [redacted]
Sent: Monday, December 19, 2016 10:02 AM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: FBINet Password Expiration Notification --- UNCLASSIFIED
Importance: High

Classification: UNCLASSIFIED
==========

FBINet Password Expiration Notice

Dear DANIEL RICHMAN,

Your password on FBINet will expire in seven day(s). Please change it as soon as possible to make sure your account does not get locked out. b7E 1, 3

[redacted]

*** Please do not respond to this email ***
Direct any questions or concerns regarding this issue to the EOC Help Desk at [redacted]

==========
Classification: UNCLASSIFIED

[redacted] b7E 3

From: [redacted]
Sent: Tuesday, December 20, 2016 10:24 AM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: FBINet Password Expiration Notification --- UNCLASSIFIED
Importance: High

Classification: UNCLASSIFIED
==========

FBINet Password Expiration Notice

Dear DANIEL RICHMAN,

Your password on FBINet will expire in six day(s). Please change it as soon as possible to make sure your account does not get locked out. b7E 1, 3

[redacted]

*** Please do not respond to this email ***
Direct any questions or concerns regarding this issue to the EOC Help Desk at [redacted]

==========
Classification: UNCLASSIFIED

[redacted] b7E 3

From: [redacted]
Sent: Wednesday, December 21, 2016 10:01 AM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: FBINet Password Expiration Notification --- UNCLASSIFIED
Importance: High

Classification: UNCLASSIFIED
==========

FBINet Password Expiration Notice

Dear DANIEL RICHMAN,

Your password on FBINet will expire in five day(s). Please change it as soon as possible to make sure your account does not get locked out. b7E 1, 3

[redacted]

*** Please do not respond to this email ***
Direct any questions or concerns regarding this issue to the EOC Help Desk at [redacted]

==========
Classification: UNCLASSIFIED

[redacted] b7E 3

From: [redacted]
Sent: Thursday, December 22, 2016 9:13 AM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: FBINet Password Expiration Notification --- UNCLASSIFIED
Importance: High

Classification: UNCLASSIFIED

FBINet Password Expiration Notice

Dear DANIEL RICHMAN,

Your password on FBINet will expire in four day(s). Please change it as soon as possible to make sure your account does not get locked out. b7E 1, 3

[redacted]

*** Please do not respond to this email ***
Direct any questions or concerns regarding this issue to the EOC Help Desk at [redacted]

Classification: UNCLASSIFIED

[redacted] b7E 3

From: [redacted]
Sent: Friday, December 23, 2016 10:05 AM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: FBINet Password Expiration Notification --- UNCLASSIFIED
Importance: High

Classification: UNCLASSIFIED
==========

FBINet Password Expiration Notice

Dear DANIEL RICHMAN,

Your password on FBINet will expire in three day(s). Please change it as soon as possible to make sure your account does not get locked out. b7E 1, 3

[redacted]

*** Please do not respond to this email ***
Direct any questions or concerns regarding this issue to the EOC Help Desk at [redacted]

==========
Classification: UNCLASSIFIED

[redacted] b7E 3

From: [redacted]
Sent: Saturday, December 24, 2016 9:42 AM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: FBINet Password Expiration Notification --- UNCLASSIFIED
Importance: High

Classification: UNCLASSIFIED
==========

FBINet Password Expiration Notice

Dear DANIEL RICHMAN,

Your password on FBINet will expire in two day(s). Please change it as soon as possible to make sure your account does not get locked out. b7E 1, 3

[redacted]

*** Please do not respond to this email ***
Direct any questions or concerns regarding this issue to the EOC Help Desk at [redacted]

==========
Classification: UNCLASSIFIED

[redacted] b7E 3

From: [redacted]
Sent: Sunday, December 25, 2016 9:52 AM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: FBINet Password Expiration Notification --- UNCLASSIFIED
Importance: High

Classification: UNCLASSIFIED

FBINet Password Expiration Notice

Dear DANIEL RICHMAN,

Your password on FBINet will expire in one day(s). Please change it as soon as possible to make sure your account does not get locked out. b7E 1, 3

[redacted]

*** Please do not respond to this email ***
Direct any questions or concerns regarding this issue to the EOC Help Desk at [redacted]

Classification: UNCLASSIFIED

Mandatory Training Management

From:	Mandatory Training Management
Sent:	Sunday, January 01, 2017 5:13 PM
To:	RICHMAN, DANIEL C. (DO) (OGA)
Subject:	Mandatory Training Assignment Deadline Approaching:

Dear DANIEL CHARLES RICHMAN,

The deadline for completing the following required training assignment is approaching:

Title: Insider Threat and Media Contact Awareness

Type: Web Based Training

You must complete this assignment before midnight (Eastern Time) on 1/31/2017. Please log into the Virtual Academy at [redacted] to complete this assignment. To find your required training list, locate My Training in the gray navigation bar at the top of the page and select My Training Plan from the drop-down menu. b7E 3

If you have any questions regarding this training assignment, please contact the Virtual Academy for assistance.

Thank you,

FBI Virtual Academy

virtualacademy@fbiacademy.edu

[redacted] b7E 3

From: [redacted]
Sent: Wednesday, January 11, 2017 11:53 AM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: Interaction SD1014671/17 has been opened --- UNCLASSIFIED//~~FOUO~~

Classification: UNCLASSIFIED//~~FOUO~~

ITB Service Manager - Interaction Notification

Dear Sir/Madam,

Interaction SD1014671/17 has been opened.

Please click the following hyperlink to view the details or to update the ticket: Interaction SD 1014671/17

If you have any questions, please contact the Enterprise Operations Center:
EOC Service Desk
[redacted] b7E 3

Please do not reply to this one-way e-mail.

Interaction details are as follows:

Title:	Desktop Issues
Primary Contact:	RICHMAN DANIEL CHARLES [redacted]
Service Recipient (If different from Primary Contact):	RICHMAN DANIEL CHARLES [redacted]
Affected CI:	[redacted]
Affected Service:	
Subservice:	
Subservice Type:	
Network Enclave:	[redacted]
Category:	
Area:	
Subarea:	

b6 4
b7C 4
b7E 1, 7

Impact:	
Urgency:	
Priority:	

Please do not reply to this one-way e-mail.

==========

Classification: UNCLASSIFIED//~~FOUO~~

[redacted] b7E 3

From: [redacted]
Sent: Wednesday, January 11, 2017 11:57 AM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: Interaction SD1014591/17 has been closed and a Customer Satisfaction Survey has been generated for you --- UNCLASSIFIED//~~FOUO~~

Classification: UNCLASSIFIED//~~FOUO~~

==========

ITB Service Manager - Survey Notification

Dear Sir/Madam,

[redacted] Interaction SD1014591/17 has been closed. b7E 7

Your feedback is important to us! Please use the following link to rate our service and provide any comments you may have regarding the service that you have received: Customer Satisfaction Survey

If you have any questions, please contact the Enterprise Operations Center (EOC) EOC Service Desk at [redacted] b7E 3

If you disagree with the solution, you may resubmit the interaction by clicking the following hyperlink: Interaction SD1014591/17

Interaction details are as follows, or you can click the following hyperlink to view the Interaction ticket details: SD1014591/17.

Title:	FBINET DOMAIN PW RESET.
Interaction Number:	SD1014591/17
Primary Contact:	RICHMAN DANIEL CHARLES [redacted] b6 4 b7C 4
Service Recipient (If different from Primary Contact):	
Affected CI:	b7E 7
Affected Service:	
Closure Code:	
Closure Comments:	

Area:	
Subarea:	
Impact:	
Urgency:	
Priority:	

b7E 7

Please do not reply to this one-way e-mail.

==========

Classification: UNCLASSIFIED//~~FOUO~~

[redacted] b7E 3

From: [redacted]
Sent: Wednesday, January 11, 2017 12:15 PM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: Enrollment in Online Course: Insider Threat and Media Contact Awareness

Dear DANIEL RICHMAN,

Your enrollment in the Insider Threat and Media Contact Awareness online course is confirmed.

The course will appear in the My Learning Plan section under the My Workspace tab until it is completed.

You may access the course by following the link below:

[redacted] b7E 3

If you have any questions regarding your enrollment in the online course, please contact the Virtual Academy for assistance.

Thank you,
Virtual Academy
Training Division

For Technical issues: contact EOC Helpdesk, [redacted]

RICHMAN, DANIEL C. (DO) (OGA)

From: RICHMAN, DANIEL C. (DO) (OGA)
Sent: Wednesday, January 11, 2017 12:31 PM
To: [redacted] (NY) (FBI)
Subject: FW: Interaction SD1014671/17 has been opened --- UNCLASSIFIED//~~FOUO~~

b6 1
b7C 1

Classification: UNCLASSIFIED//~~FOUO~~
==========

From: [redacted]
Sent: Wednesday, January 11, 2017 11:53 AM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: Interaction SD1014671/17 has been opened --- UNCLASSIFIED//~~FOUO~~

b7E 3

Classification: UNCLASSIFIED//~~FOUO~~
==========

ITB Service Manager - Interaction Notification

Dear Sir/Madam,

Interaction SD1014671/17 has been opened.

Please click the following hyperlink to view the details or to update the ticket: Interaction SD1014671/17

If you have any questions, please contact the Enterprise Operations Center:
EOC Service Desk
[redacted]

Please do not reply to this one-way e-mail.

b6 4
b7C 4
b7E 1, 3, 7

Interaction details are as follows:

Title:	Desktop Issues
Primary Contact:	RICHMAN DANIEL CHARLES [redacted]
Service Recipient (If different from Primary Contact):	RICHMAN DANIEL CHARLES ([redacted]
Affected CI:	[redacted]
Affected Service:	
Subservice:	
Subservice Type:	

Network Enclave:	
Category:	
Area:	
Subarea:	
Impact:	
Urgency:	
Priority:	

Please do not reply to this one-way e-mail.

==========

Classification: UNCLASSIFIED//~~FOUO~~

==========

Classification: UNCLASSIFIED//~~FOUO~~

[redacted] b7E 3

From: [redacted]
Sent: Tuesday, January 17, 2017 3:46 PM
To: RICHMAN, DANIEL C. (DO) (OGA)
Subject: Incident IM1009610/17 has been closed and a Customer Satisfaction Survey has been generated for you --- UNCLASSIFIED//~~FOUO~~

Classification: UNCLASSIFIED//~~FOUO~~
==========

ITB Service Manager - Survey Notification

Dear Sir/Madam,

[redacted] Incident IM1009610/17 has been closed. b7E 7

Your feedback is important to us! Please use the following link to rate our service and provide any comments you may have regarding the service that you have received: Customer Satisfaction Survey

If you have any questions, please contact the Enterprise Operations Center (EOC) EOC Service Desk at [redacted] b7E 3

Incident details are as follows:

Title:	Windows Password Reset for FBINET [redacted]
Incident Number:	IM1009610/17
Original Interaction (if applicable):	
Primary Contact:	[redacted]
Service Recipient (If different from Primary Contact):	RICHMAN DANIEL CHARLES [redacted]
Affected CI:	
Affected Service:	
Closure Code:	
Closure Comments:	
Assignment Group:	[redacted]

b6 1, 4
b7C 1, 4
b7E 3, 7

Assignee:		
Area:		
Subarea:		
Impact:		
Urgency:		
Priority:		

b6 1
b7C 1
b7E 7

Please do not reply to this one-way e-mail.

==========

Classification: UNCLASSIFIED//~~FOUO~~

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	:	INDICTMENT
- v. -	:	16 Cr.
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.		

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, Unite 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

Form No. USA-33s-274 (Ed. 9-25-58)

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.

Daniel Charles Richman

From: Daniel Charles Richman
Sent: Saturday, February 04, 2017 6:05 PM
To: [redacted](DO) (OGA)
Cc: [redacted](DO) (FBI); Richman, Daniel C. (DO) (OGA); Kelley, Patrick W. (DO) (FBI); [redacted](DO) (FBI)
Subject: Re: Professor Richman re U.S. v. Percoco

b6 1
b7C 1
b7E 3

I'm ever so grateful for the speed and thoroughness with which you all are looking into this. Thanks so much
dr

On Sat, Feb 4, 2017 at 6:03 PM, [redacted](DO) (OGA) <[redacted]> wrote:

Thank you [redacted] I think a quick conversation Monday afternoon might be helpful, if there is a time that suits you.

.

-------- Original message --------
From: [redacted] (DO) (FBI)" <[redacted]>
Date: 2/4/17 3:21 PM (GMT-05:00)
To: [redacted](DO) (OGA)" [redacted] "Richman, Daniel C. (DO) (OGA)" [redacted]
Cc: "Kelley, Patrick W. (DO) (FBI)" <[redacted](DO) (FBI)" [redacted]
Subject: Professor Richman re U.S. v. Percoco

b6 1, 4
b7C 1, 4
b7E 3

[redacted] good afternoon. By all means, we can discuss at your convenience, including today if you happen to see this message. My contacts are also below. I'm in the office now and foreseeably a bit longer, and also will have my Bureau mobile. If you prefer, I can also continue to correspond via UNET email.

I talked with Prof. Richman last night, who was planning to call and apprise you; so I thought best to add him here, too. I've also copied my boss OIC AD Pat Kelley, who as you may know is the FBI's Deputy Designated Agency Ethics Official (DDAEO), and ethics attorney [redacted] who has been assisting on this matter, as well as communicating with Prof. Richman. [redacted] and I discussed this matter with Pat late last Thursday.

b6 1
b7C 1

The gist is that while there appears to be no 18 U.S.C. §§ 203 or 205 concerns, since Prof. Richman has not worked more than 60 days as a Special Government Employee (SGE) for the FBI in the last 365 days, there is still the issue of "outside employment" which means any form of employment involving "personal services," whether or not for compensation. The DOJ Supplemental Regulations (5 C.F.R. § 3801.106) restricts Department employees, including SGEs, from engaging in outside employment that, per Subsection (b)(1) involves: (i) the practice of law, unless uncompensated and in the nature of community

service or on behalf of yourself, your parents, spouse or children; (ii) any criminal or habeas corpus matter, be it Federal, State, or local; or, (iii) litigation, investigations, grants or other matters in which the Department of Justice is or represents a party, witness, litigant, investigator or grant-maker. Professor Richman's role as "part of the joint defense team" (per the Engagement Letter he provided us) in the case of *U.S. v. Percoco*, involves the practice of law, a criminal matter, and litigation in which the DOJ is a party; per the attached indictment.

Although the DOJ/JMD/DEO summary of the SGE ethics rules (https://www.justice.gov/jmd/ summary-government-ethics-rules-special-government-employees) states: "[t]hese prohibitions may be waived by the Deputy Attorney General and generally are waived in the case of a special government employee ..." -- at this time we do not have a waiver. Moreover, it is not necessarily a given that a waiver would be granted for this particular matter. To assist all parties with this determination, we have contacted the NY field office for any additional information on the FBI's interests in this case. Meanwhile, we have recommended that Prof. Richman not be involved with the defense team until we can better determine whether a waiver will or will not be granted. We should know more, hopefully definitively, by the end of next week.

Please let us know if you have any questions, or if you would like to meet to discuss further by phone or in person. Thank you.

[redacted]

-----Original Message-----
From: [redacted] (DO) (OGA) b6 1 b7C 1
Sent: Friday, February 03, 2017 6:23 PM b7E 3
To: [redacted] (DO) (FBI) [redacted]
Subject: Re:

[redacted]

Your message below was forwarded to me by Jim Rybicki to follow up. Could we set up a time for a quick phone call to get me up to speed on Dan Richman's status early next week sometime?

Thanks.

[redacted]
Special Counsel to the Director
Federal Bureau of Investigation

From: [redacted] (DO) (FBI) b6 1 b7C 1
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)

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

[redacted]
Chief, Ethics and Integrity Unit (EIU)
Office of Integrity and Compliance (OIC)
Desk: [redacted] Mobile: [redacted]

Spam
Not spam
Forget previous vote

--
Daniel Richman
Paul J. Kellner Professor of Law,
Columbia Law School
office [redacted] b6 4 b7C 4
cellphone [redacted]
You can download my papers at http://ssrn.com/author=937729

Daniel Charles Richman

From: Daniel Charles Richman
Sent: Saturday, June 18, 2016 4:17 PM
To: Rybicki, James E. (DO) (FBI)
Subject: Re: homicide spike law review essay
Attachments: Rosenfeld on homicides.pdf

Lovely seeing you. Now I want to solidify our talks on that Colum L Rev, piece. I won't bother explaining why the CLR would love a piece from the D -- anything on the general topic would do [redacted]

[redacted]

b5 1
b6 1,2
b7C 1,2

I'm happy to help on this and to make the process painless. My instinct is that [redacted] (I'm attaching the Rosenfeld paper that DOJ just released.) [redacted]

d

On Mon, May 16, 2016 at 4:15 PM, Daniel Charles Richman [redacted] wrote:

> Hi Jim R -- I've had some discussions with the Dir about writing something short for a Columbia Law Review "mini-symposium" on the homicide spike. (Yes, I suggested the idea to the Law Rev people.) He sounded interested and gave me the go-head to send a formal invite to you. So one is attached. As I told him, I'd be happy to help him and/or others write this. Happy to give you whatever further info you'd like
>
> thx
> dan r
>
> --
> 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

--
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

U.S. Department of Justice
Office of Justice Programs
National Institute of Justice

National Institute of Justice

Documenting and Explaining the 2015 Homicide Rise: Research Directions

Richard Rosenfeld*
University of Missouri – St. Louis

June 2016

*Dr. Rosenfeld prepared this paper with support from the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice, under contract number 2010F_10097 (CSR, Incorporated). The opinions, findings, and conclusions or recommendations expressed in this publication are those of the authors and do not necessarily represent those of the Department of Justice.

NCJ 249895

U.S. Department of Justice
Office of Justice Programs
810 Seventh St. N.W.
Washington, DC 20531

Loretta E. Lynch
Attorney General

Karol V. Mason
Assistant Attorney General

Nancy Rodriguez, Ph.D.
Director, National Institute of Justice

This and other publications and products of the National Institute of Justice can be found at:

National Institute of Justice
Strengthen Science • Advance Justice
http://www.nij.gov

Office of Justice Programs
Innovation • Partnerships • Safer Neighborhoods
http://www.ojp.usdoj.gov

The National Institute of Justice is the research, development and evaluation agency of the U.S. Department of Justice. NIJ's mission is to advance scientific research, development and evaluation to enhance the administration of justice and public safety.

The National Institute of Justice is a component of the Office of Justice Programs, which also includes the Bureau of Justice Assistance; the Bureau of Justice Statistics; the Office for Victims of Crime; the Office of Juvenile Justice and Delinquency Prevention; and the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The debate over the size, scope and causes of the homicide increase in 2015 has been largely free of systematic evidence. This paper documents the scale of the homicide increase for a sample of 56 large U.S. cities. It then examines three plausible explanations of the homicide rise: an expansion of urban drug markets fueled by the heroin epidemic, reductions in incarceration resulting in a growing number of released prisoners in the nation's cities, and a "Ferguson effect" resulting from widely publicized incidents of police use of deadly force against minority citizens. The paper concludes with a call for the more frequent and timely release of crime information to address crime problems as they arise.

The homicide increase in the nation's large cities was real and nearly unprecedented. It was also heavily concentrated in a few cities with large African-American populations. Empirical explanations of the homicide increase must await future research based on year-end crime data for 2015. Several empirical indicators for assessing the explanations under consideration here are discussed. For example, if the homicide increase resulted from an expansion in urban drug markets, we should observe larger increases in drug-related homicides than those committed under other circumstances. If returning prisoners fueled the homicide increase, that should be reflected in growing numbers of homicides committed by parolees.

It will be more difficult to empirically evaluate the so-called Ferguson effect on crime increases, depending on the version of this phenomenon under consideration. The dominant interpretation of the Ferguson effect is that criticism of the police stemming from widely publicized and controversial incidents of the use of force against minority citizens caused the police to disengage from vigorous enforcement activities. Another version of the Ferguson effect, however, switches the focus from changes in police behavior to the longstanding grievances and discontent with policing in African-American communities. In this interpretation, when activated by controversial incidents of police use of force, chronic discontent erupts into violence.

The de-policing interpretation of the Ferguson effect can be evaluated with data on arrests and other forms of self-initiated activity by the police. De-policing should be reflected in declining arrest rates in cities experiencing homicide increases. Tracing the pathways from chronic levels of discontent to an escalation in homicide will ultimately require ethnographic studies in minority communities that reveal, for example, whether offenders believe they can engage in crime without fear that residents will contact the police or cooperate in police investigations. Such studies could also disclose other linkages between discontent, police use of force and criminal violence.

In summary, the following research questions for documenting and explaining the 2015 homicide rise, at a minimum, should be pursued when the requisite data become available:

- How large and widespread was the homicide increase in 2015? Did other crimes also increase?

- What conditions drove the homicide increase? Candidate explanations must account for the timing as well as the magnitude and scope of the increase.
- What role, if any, did the expansion of drug markets play in the 2015 homicide increase? Was there a relative increase in drug arrests and drug-related homicides?
- Did declining imprisonment rates contribute to the 2015 homicide rise? Was the increase greater in cities with more returning prisoners and among parolees?
- What role did the Ferguson effect play in the homicide rise? If de-policing contributed to the increase, arrest rates should have declined in cities experiencing the largest homicide increases. An open question is how to evaluate the role, if any, of community discontent with the police. Ethnographic studies, among other methods, should be high on the list of research approaches to identify the mechanisms linking police legitimacy and escalating levels of violence.

Researchers would have been in a better position to begin addressing the 2015 homicide rise, with evidence rather than speculation, if timely crime data had been available as the increase was occurring. We would have known whether the homicide rise was confined to large cities, whether other crimes were also increasing, and whether arrest rates were falling. The debate over the homicide increase would have been better informed. Technical impediments to the monthly release of crime data no longer exist. A large and worrisome increase in homicide should be the catalyst to finally bring the nation's crime monitoring system into the 21st century.

INTRODUCTION

Early in 2015, the local press in several U.S. cities reported that the decades-long crime decline had been reversed by a sizable increase in homicide. Then, late in the summer, the *New York Times* broke the story nationwide (Davey and Smith 2015). Shortly after the *Times* account appeared, Attorney General Loretta Lynch called big city mayors and police chiefs to a meeting in Washington, D.C., to discuss the homicide rise (Byrne 2015). It was there that FBI Director James Comey first publicly speculated that the increase may have been driven by widely publicized reports of police use of force that resulted in de-policing. Director Comey repeated the claim a few days later in a speech at the University of Chicago, where he called attention to a "chill wind" blowing through the nation's police departments. He also pointed out, however, that he did not have the evidence necessary to confirm de-policing or any other explanation of the homicide rise (Schmit and Apuzzo 2015).

A lively debate in the press soon erupted over the size of the putative homicide increase and its causes. On one side were commentators who argued that the increase was real and caused by widespread public criticism of the police, which had made police officers hesitant to engage in the proactive policing strategies that reduce crime (Mac Donald 2015).[1] On the other side were skeptics who argued that the homicide rise had been overblown and, whatever its magnitude, did not result from a "Ferguson effect" on vigorous policing (Bialik 2015; Coates 2015; Friedman, Fortier, and Cullen 2015).

Notably absent from the conflicting accounts of the 2015 homicide rise was comprehensive evidence needed to evaluate the two issues that framed the debate: (1) Did homicide rates increase and, if so, how large and widespread was the upturn? and (2) Was the increase caused by hesitancy on the part of police to carry out their crime-fighting mission? This paper is organized accordingly.

I begin by documenting the homicide increase in 2015 with data on year-end homicide rates in 56 U.S. cities.[2] I then present three plausible explanations of the homicide rise: expanding urban drug markets, declining imprisonment rates, and the so-called Ferguson effect on policing. Only the latter explanation has received significant attention in the debate over the homicide increase, but prior research has tied crime rate changes to the violence surrounding urban drug markets and to prison expansion (e.g., Blumstein 1995; Levitt 1996; Rosenfeld 2011a). In addition, there are at least two ways in which the Ferguson effect may have unfolded. The dominant interpretation is that the publicity surrounding recent controversial police killings resulted in de-policing. A second equally plausible explanation is that, regardless of their effect on police behavior, the police killings in Ferguson and elsewhere activated longstanding grievances in minority communities concerning the police and the criminal justice system as a whole, resulting

[1] Mac Donald later attributed the homicide increase, in part, to statements made by President Obama that she believed were unduly critical of the police (Mac Donald 2016).

[2] I am grateful to Max Ehrenfreund of *The Washington Post* and Darrel W. Stephens of the Major Cities Chiefs Police Association for providing the crime data used in this study.

in a "legitimacy crisis" that spurred crime increases. Researchers have also attributed homicide increases to declining institutional legitimacy (LaFree 1998; Roth 2009).

I present several empirical indicators that can be used to evaluate the alternative explanations for the 2015 homicide rise. Unfortunately, the evidence needed to carry out the pertinent research is unavailable as of this writing, and will not be available until September or October of 2016 when the FBI releases its Uniform Crime Reports (UCR) for yearend 2015. In the final section of the paper, I argue that it should not be necessary, well into the 21st century, to wait nine months after the collection year to learn whether crime rates are increasing and gain some insight into the underlying causes. The press and advocacy organizations have done due diligence in compiling crime data from local police departments, but these sporadic and necessarily incomplete efforts are no substitute for the timely release of comprehensive crime and arrest statistics by the responsible federal agencies. Had the official crime data been released on a monthly basis during 2015, the debate over the homicide rise might have produced less heat and more light.

My focus is on homicide for two reasons. First, with few exceptions (e.g., Friedman, Fortier, and Cullen 2015), the public debate has largely turned on whether and why homicide rates may have increased during the past year. Second, homicide is the most serious and reliably measured crime type for which trend data are available. None of the arguments in the debate over the homicide rise, however, including the explanations examined here, is limited to homicide. A Ferguson effect, expanding drug markets or declining imprisonment rates might have been expected to lead to increases in other violent crimes or in property crime. The first order of business for future research on the 2015 homicide increase is to extend the range of offenses under consideration beyond homicide.[3]

DOCUMENTING THE INCREASE

The data used to determine the size and scope of the homicide increase in 2015 are from the police departments in 56 large U. S. cities (see fn. 2). The cities are listed in the Appendix. With the exception of Salt Lake City, Utah (population 190,884), the population of each city exceeded 250,000 in 2014. The 56-city sample, therefore, constitutes the bulk of cities in the UCR's Group I category of cities with populations greater than 250,000. The sample accounted for fully 92 percent or 4,873 of the 5,305 homicides in the Group I cities in 2014.[4]

In addition, as shown in Figure 1, the average homicide rates in the 56-city sample and the UCR Group I cities have trended together for the past two decades. The correlation (r) between the two trends is an impressive .96. Both series declined through the end of the

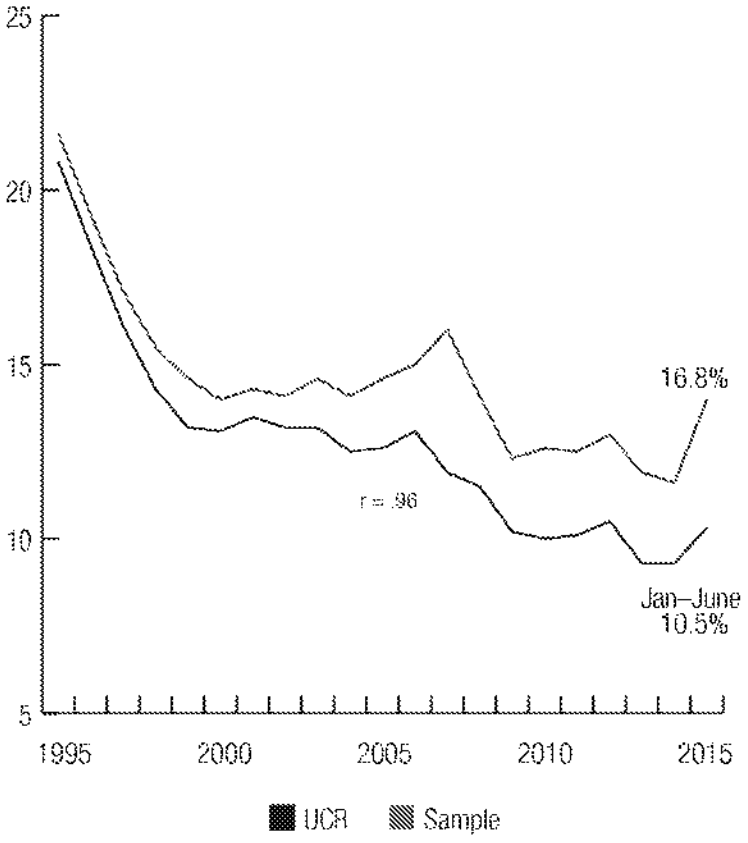
[3] A good start is a study by Pyrooz et al. (2016) that examined changes in each of the FBI's Part I violent and property crimes in relation to a possible Ferguson effect.

[4] See the 2014 UCR at https://www.fbi.gov/about-us/cjis/ucr/crime-in-the-u.s/2014/crime-in-the-u.s.-2014.

1990s, flattened for a few years, rose slightly through 2007, and fell again through 2009. Another slight dip followed until 2015, when both series exhibited a notable increase.

The 56-city sample used in this study is clearly a reasonable proxy for the 70-80 cities that typically constitute the UCR Group I cities with populations over 250,000. At the same time, the results of this study are limited to those cities and cannot be generalized to smaller cities, towns and rural areas, where average homicide rates are lower. With that limitation in mind, we observe that the homicide rate in the sample rose by 16.8 percent over the previous year. According to preliminary UCR figures, the homicide rate in the Group I cities increased by 10.5 percent during the first six months of 2015 over the same period in 2014.[5] Depending on the reliability of the homicide data obtained directly from police departments, a best guess is that the year-end 2015 homicide rate for the Group I cities will be close to the 16.8-percent rise over 2014 observed in the sample. The question now is whether an increase of that magnitude merits the attention it has received from pundits, advocates and federal officials.

Figure 1. Change in Homicide Rates for 56-City Sample and UCR Group I Cities Over 250,000 Population, 1995-2015



National attention to homicide increases in U.S. cities is not new, even during the period of the crime drop since the early 1990s. A recent example is the National Violent Crime Summit hosted by the Police Executive Research Forum

[5] Computed from data presented in https://www.fbi.gov/about-us/cjis/ucr/crime-in-the-u.s/2015/preliminary-semiannual-uniform-crime-report-januaryjune-2015/tables/table-1. The 2015 six-month preliminary UCR figures for smaller cities also reveal sizable increases over the previous year. For example, homicides in cities with populations between 50,000 and 99,000 went up by 8.9 percent.

(PERF) in Washington during August of 2006 to discuss rising violent crime[6] rates across the nation. PERF issued a report, provocatively titled *A Gathering Storm — Violent Crime in America*, that highlighted crime increases in a sample of 55 cities. According to the report, "For a growing number of cities across the United States, violent crime is accelerating at an alarming pace" (Police Executive Research Forum 2006; Somers 2006). The Department of Justice initiated an investigation of crime changes in selected cities, but never publicly issued a report summarizing the results (Rosenfeld 2007).

To gain perspective on the significance of the 2015 homicide increase, it is useful to compare it with the increases featured in the PERF report. Between 2004 and 2006, national violent crime rates rose by 3.5 percent and homicide rates increased by 5.4 percent. The comparable increases for Group I cities were .4 percent and 4.8 percent, respectively. Violent crime and homicide rates then dropped in 2007.[7] These homicide increases are not trivial but they are considerably smaller than those recorded for 2015, and they were relatively short lived. If increases of this magnitude garnered the attention of public officials, including the Attorney General (Somers 2006), in 2006, it is not surprising that the double-digit percentage increase in big-city homicide registered in 2015 would also spark the interest of public officials and the press.

Was the homicide increase in large cities during 2015 "statistically significant"? A study by Pyrooz et al. (2016) examined crime rates in 81 large cities 12 months before and 12 months after the killing of Michael Brown by a police officer in Ferguson, Missouri, on August 9, 2014. They concluded that the difference in homicide trends between the two periods was not statistically significant, although they did find a significant increase in robbery after the Ferguson incident. By comparison, the difference between the 2015 and 2014 homicide rates for the 56-city sample in the current study is just significant at the conventional 5 percent threshold in a one-tailed test ($p = .05$, $t = 1.66$).

A closer look at the results of the Pyrooz et al. study, however, reveals a somewhat different conclusion. Table 2 in that study reports a coefficient on the post-Ferguson trend in homicide of .015 and a standard error of .009, which yields a t-statistic of 1.67, nearly identical to that in the current study. Given the differences between the two studies in sample size, sample composition and estimation methods, it is difficult to directly compare the results. Moreover, tests of statistical significance are technically unwarranted because neither sample is a random draw from a population. Nonetheless, it seems reasonable to conclude that the homicide increases revealed in both studies are at least roughly comparable.

Pyrooz et al. (2016) did acknowledge that homicide had increased in "selected cities" during the period they investigated and called attention to the elevated variance in city homicide rates after the Ferguson incident. The results of the current study are similar. Figure 2 (see page 9) displays the percentage change between 2014 and 2015 in homicides for the 56-city sample. There is marked variation in these one-year changes. Forty cities experienced homicide increases and 16 saw declines or, in one case, no

[6] Violent crimes include homicide, rape, robbery and aggravated assault.
[7] See https://www.fbi.gov/about-us/cjis/ucr/ucr.

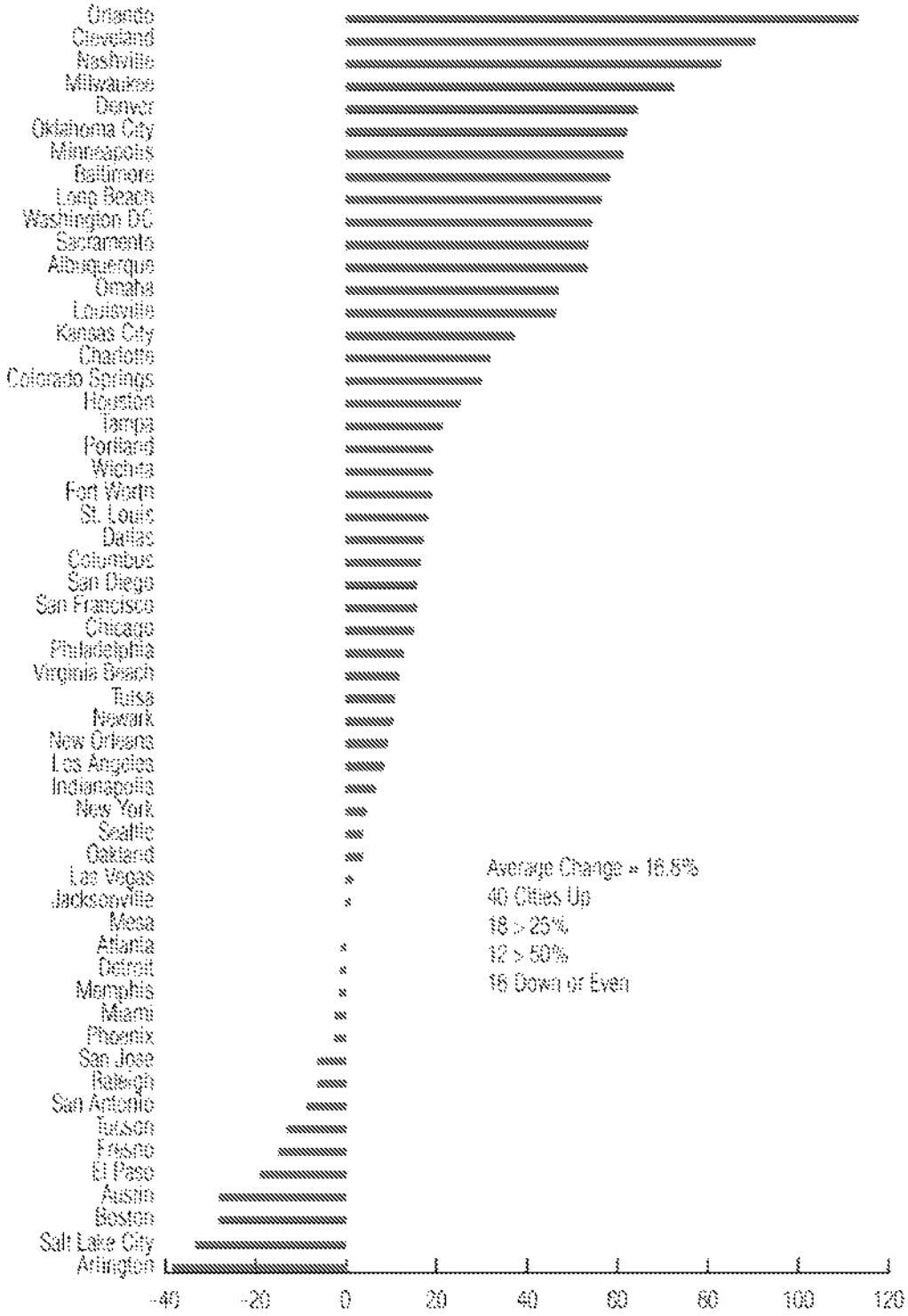
change. Homicides in 18 of the cities increased by more than 25 percent; the increase exceeded 50 percent in 12 cities. The skewed distribution of the homicide changes indicates that a relatively small number of cities accounted for most of the increase in the sample. In fact, just 10 cities accounted for two-thirds of the total homicide increase between 2014 and 2015, as shown in table 1.

Table 1 displays the 10 cities that contributed the largest number of homicides to the total increase in 2015. Together, the increases in these cities constituted 66.7 percent of the total increase in the 56-city sample. Had homicides not risen in these cities, it is likely that the homicide increase of 2015 would have generated far less attention and controversy. The remainder of this section focuses on these "top ten" contributors to the homicide rise in large U.S. cities.

Table 1: Ten Cities With Largest Absolute Homicide Increases, 2014-2015

City	Absolute increase	% increase	Cum % of total increase
Baltimore	127	56.5	15.6
Chicago	61	16.0	22.9
Houston	61	25.2	30.3
Milwaukee	61	72.6	37.8
Cleveland	57	90.5	44.7
Washington DC	57	54.3	51.8
Nashville	34	32.9	55.6
Philadelphia	32	12.8	59.7
Kansas City	29	37.2	63.2
St. Louis	29	18.2	66.7

Figure 2: Percentage Change in Homicide in 56 Cities, 2014-2015



THE TOP TEN

The top ten cities not only produced two-thirds of the big-city homicide increase in 2015, they also experienced a far larger percentage increase than the sample as a whole. The percentage increases in the top ten ranged from 90.5 percent in Cleveland to 12.9 percent in Philadelphia. The average homicide increase over 2014 in the top ten was 33.3 percent, compared with a 16.8-percent rise for the sample as a whole. One-year increases of this magnitude in the nation's large cities, although not unknown, are very rare. Cities in the top ten had experienced one-year percentage increases in homicide that exceeded their increase in 2015 on only 15 occasions since 1985. The increase in 2015 was greater than 95 percent of the yearly increases these cities had experienced during the previous three decades.[8] If not unprecedented, then, the 33.3-percent homicide rise in the top ten cities certainly deserves further scrutiny.[9]

The top ten cities differ from other large cities in other ways as well. As shown in Figure 3 (see page 11), with an average population of roughly one million, the top ten cities are somewhat larger than the others in the 56-city sample.[10] They also have somewhat higher poverty rates (24.6 percent versus 20.8 percent). The largest difference between the top ten and other cities in the sample, however, is their race/ethnic composition. The top ten have larger black populations and smaller Hispanic populations than the other cities. The relative size of the black population in the top ten is double that in the other cities (40.8 percent versus 19.9 percent). By contrast, Hispanics make up just 15.2 percent of the population in the top ten compared with 26.4 percent of the population of the remaining cities in the sample. As we move to a consideration of explanations for the homicide rise in 2015, these race/ethnic differences merit prominent attention.

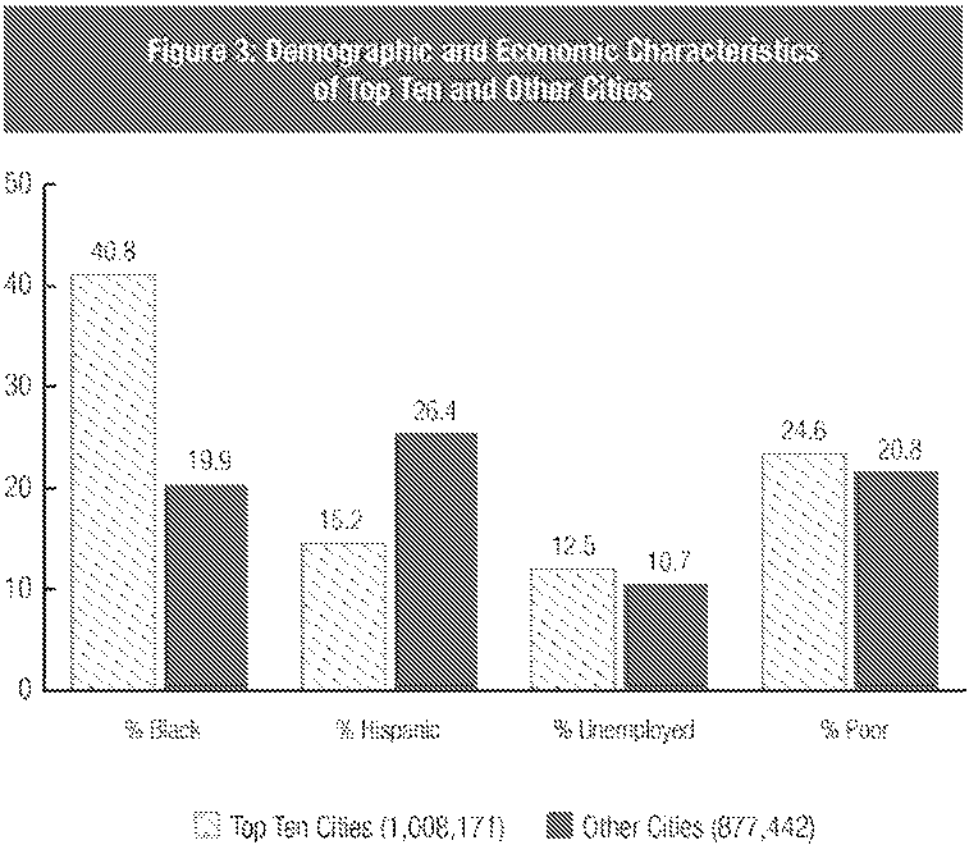
In summary, the homicide rise in 2015 in the nation's large cities was real and, while not unprecedented, comparatively large. Whether the increase extended beyond the largest cities remains unknown, although preliminary UCR data for the first six months of 2015 reveal sizable increases in smaller cities as well (see fn. 5). Homicides in the 56-city sample used in this study increased by 16.8 percent over 2014. Ten cities accounted for two-thirds of this increase, and together they experienced a 33.3-percent jump in homicide. These cities have considerably larger black populations and smaller Hispanic populations than the other cities in the sample. We now turn to three plausible explanations of the homicide rise: the expansion of urban drug markets, falling imprisonment rates, and the effects of widely publicized and controversial incidents of the use of force by the police against minority citizens.

---

[8] The 2015 percentage increase in four of the cities (Cleveland, Washington, Milwaukee and Baltimore) was greater than the increase they experienced during any year since 1985. The 15 yearly homicide increases that exceeded the percentage increase in 2015 were concentrated in the remaining six of the top ten cities and constituted just 5.0 percent of the 300 possible yearly increases during the 30-year period (10 cities x 30 years).

[9] The 33.3-percent rise in homicides in the top ten cities is statistically significant in a one-tailed test ($p = .04$; $t = 1.99$).

[10] The data shown in Figure 3 are from the 2010-2014 combined files of the American Community Survey (www.census.gov/programs-surveys/acs/)



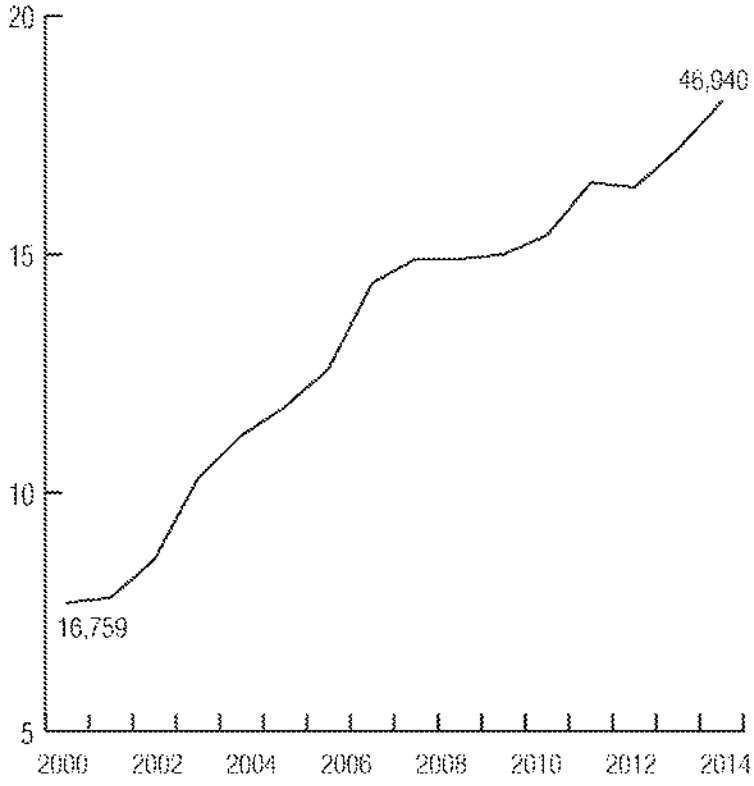
EXPLAINING THE INCREASE

The study of crime trends is as old as criminology itself. A large body of contemporary research literature is devoted to explaining the causes and correlates of changing crime rates (Blumstein and Wallman 2006; Rosenfeld 2011a). The current task, however, is not to explain a long- or even short-run trend in crime rates, but rather a *trend reversal* in the nation's large cities. Some of the explanatory factors that have been emphasized in the crime trends literature are poor candidates for explaining the homicide rise of 2015. Shifts in age composition or the consequences of exposure to lead, for example, unfold gradually over time and cannot explain why homicide rates would suddenly increase after falling for over two decades. The same is true of economic conditions, except for the relatively abrupt changes in income and employment that occur during a recession. The last recession in the United States, however, ended at least five years before the current upturn in homicide (see www.nber.org/cycles/main.html). Some evidence suggests that a drop in consumer confidence contributed to the increase in violent crime in 2005 and 2006 (Rosenfeld and Oliver 2008). Consumer confidence, however, rose from 2014 to

2015.[11] Crime increases also tend to correspond with rising inflation rates (Rosenfeld and Levin 2016), but U.S. inflation rates fell from 2011 through the end of 2015.[12]

It is reasonable to assume that whatever factors lay behind the 2015 homicide rise should themselves have exhibited comparably abrupt changes at the same time or shortly before. Among the explanatory factors featured in research on crime trends, the three that are examined here appear better able than others, at least in principle, to explain the recent homicide increase. We begin by considering whether the comparatively sudden uptick in homicide in large cities might have been spurred by a recent expansion in urban drug markets. The discussion then turns to the possible role of recent changes in imprisonment rates and, finally, to the Ferguson effect, in both its de-policing and "legitimacy" versions. Throughout the discussion, several empirical indicators are described that can be used to evaluate the contribution of these factors to the homicide increase, once the requisite data become available.

Figure 4. Drug-Related Deaths per 100,000 Population Age 15 and Over, 1999-2014



Source: Rudd et al. (2016)

DRUG MARKETS

The United States is in the midst of a major drug epidemic. An important indicator of rising drug use and abuse is the death rate from drug overdose. Figure 4 displays the trend in drug overdose deaths from 1999 to 2014. The overdose death rate more than doubled over the period. In 2014, more persons died from drug overdose than during any previous year on record (Rudd et al. 2016). The increase in drug deaths, in turn, was driven largely by the growth in deaths related to the non-

[11] The University of Michigan's Index of Consumer Sentiment rose from a value of 84.1 in 2014 to 92.9 in 2015 (http://www.sca.isr.umich.edu/tables.html). See Rosenfeld and Fornango (2007) for a study of crime trends and consumer sentiment.

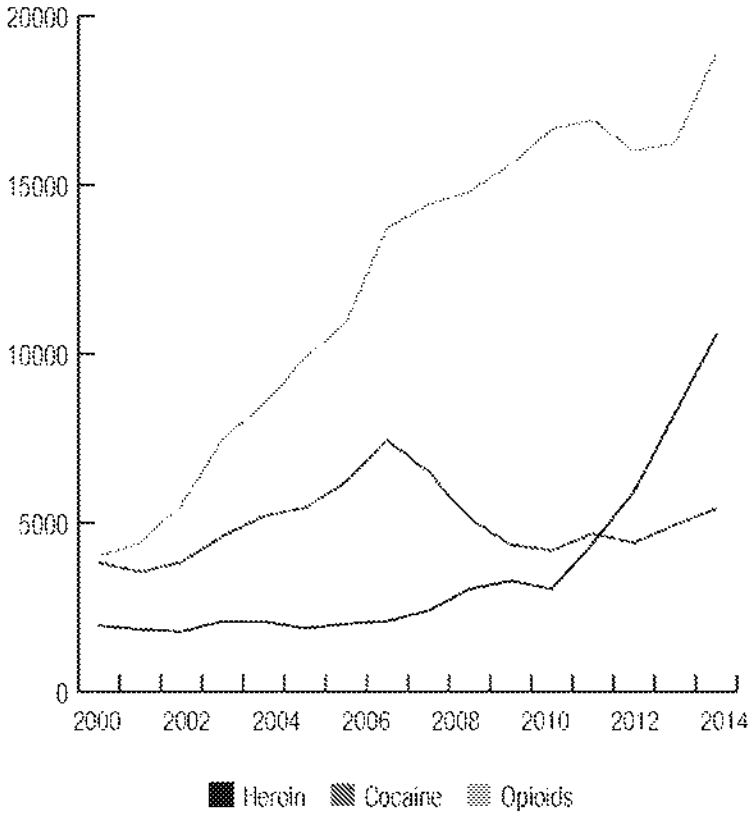
[12] See http://www.usinflationcalculator.com/inflation/historical-inflation-rates/.

medical use of opioid analgesics (e.g., Oxycontin, Vicodin) and heroin, as shown in Figure 5. By 2014, opioid and heroin deaths accounted for 61.0 percent of all drug overdose deaths in the United States (Rudd et al. 2016). Cocaine overdose contributed an additional 5,415 drug deaths in 2014, but the number of cocaine deaths peaked in 2006. Beginning in 2012, the number of heroin overdose deaths overtook the number of cocaine deaths; by 2014, the number of heroin deaths was nearly twice as large (see Figure 5).

As more users enter the market for illicit drugs, the opportunities and incentives for drug sellers also expand. Disputes among sellers over access to customers, and between sellers and buyers over price, purity and other terms of trade, often end in violence in illicit markets where participants have no legal means to resolve disputes (Reuter 2010). In an influential paper, Blumstein (1995) linked youth homicide increases to the emergence and spread of the crack cocaine markets in U.S. cities during the 1980s and early 1990s. As the demand for crack grew, young sellers were recruited into the markets because of their reduced legal liability. They carried guns to protect themselves from rivals, customers and street robbers. As the violence connected to the crack markets escalated, other youth acquired guns to protect themselves from an increasingly dangerous inner-city environment. A classic arms race ensued and youth firearm homicide rates rose (see also Blumstein and Rosenfeld 1998).

Subsequent research has confirmed the "Blumstein hypothesis" linking homicide and the diffusion of guns to the expansion of urban drug markets (e.g., Cork 1999; Messner et al. 2005; Ousey and Lee 2002). The question is whether similar dynamics were at play in the homicide rise of 2015.

Figure 5. Number of Drug Deaths by Drug Type, 1999-2014



Source: Rudd et al. (2016)

There are reasons, and some evidence, for and against this hypothesis. Urban drug markets are, or at least were, violent locales. As more buyers and sellers come into contact in these "stateless" locations, homicide rates should be expected to rise. But some evidence suggests that changes in illicit drug market transactions, such as the use of cell phones to connect with customers and effective law enforcement initiatives to shut down open air street markets, have reduced drug market violence (see Zimring 2011). In addition, the population groups fueling the growing demand for heroin differ from the largely inner-city African-American consumers of crack cocaine during the initial years of the crack era. As shown in Table 2, heroin use rates among non-Hispanic whites more

Table 2: Heroin Use Rates[a] by Demographic and Behavioral Characteristics, 2002-2013

	2002-04	2005-07	2008-10	2011-13	% Change
Total	1.6	1.8	2.3	2.6	62.5%
Sex					
Male	2.4	2.6	3.3	3.6	50%
Female	0.8	1.0	1.3	1.6	100.0%
Age					
12-17	1.8	1.3	1.4	1.6	-11.1%
18-25	3.5	4.3	5.3	7.3	108.6%
26 and over	1.2	1.3	1.9	1.9	58.3%
Race-Ethnicity					
Non-Hisp. White	1.4	1.8	2.6	3.0	114.3%
Other	2.0	2.2	1.9	1.7	-15.0%
Residence					
Large City[b]	1.8	2.0	2.4	3.0	66.7%
Other	1.4	1.5	2.3	2.1	50.0%
Substance Use[c]					
Opioids	17.6	25.1	34.0	42.4	138.2%
Cocaine	48.9	57.6	68.3	91.6	87.1%

a Per 1,000 persons age 12 and over.
b Core Based Statistical Area 1 million population
c Past year non-medical use
Source: Jones et al. (2015)

than doubled between 2002 and 2013, while heroin use actually fell somewhat among other race and ethnic groups (see Jones et al. 2015). Prior research has shown that, during the crack era, the link between expanding drug markets and homicide was strongest in cities with high levels of economic disadvantage and racial segregation (Ousey and Lee 2002). Evidence that the current heroin epidemic has been confined to the white population also may be one reason why it has been defined largely as a public health challenge rather than a criminal justice problem (Cohen 2015).

But the major reason to be skeptical of the view that the expansion of the heroin markets led to the homicide increase of 2015 is that the heroin epidemic took off several years before the homicide rise. Heroin overdose deaths were essentially unchanged between 1999 and 2006. They rose gradually over the next few years and then increased sharply beginning in 2011 (see Figure 5). It is not obvious why the increase in homicide would lag at least five years behind the explosive growth in the demand for heroin, if the expansion of urban drug markets spurred the homicide rise.

Whether the homicide rise was produced by drug market expansion or other factors is ultimately an empirical question for which we do not yet have answers. Strong conclusions will require ethnographic studies of contemporary drug markets, like those written about the crack era, that take a close look at the ways in which they may, or may not, give rise to the violence associated with the crack markets a generation ago (Bourgois 2003; Contreras 2013). In the meantime, however, several empirical indicators can be used to gauge whether the recent expansion of drug markets was implicated in the homicide increase of 2015.

The most obvious indicator for assessing a rise in drug-related crime is the drug arrest rate. Drug arrests reflect enforcement policy and do not necessarily correspond with changes in drug law violations. Prior research, however, has revealed a close relationship between drug arrest rates and other indicators of drug use, such as hospital admissions for drug overdose (Rosenfeld and Decker 1999). Expanding drug markets should produce increases in arrests for both drug sales and possession. Arrests for drug abuse violations actually fell nationwide between 2011 and 2014, when the heroin epidemic was underway, but the aggregate data combine arrests for all drug types, including marijuana.[13] Researchers can query local police departments for data that partition drug arrests by drug type. Comparably detailed data for large cities will be available when the 2015 UCR files are archived.

A more sensitive indicator of the possible role of drug market expansion in the 2015 homicide increase is the fraction of homicides that are drug related. Most big city police departments code homicides by circumstance, including whether the killing was related to drug use or a drug transaction. The FBI's Supplementary Homicide Reports also classify homicides by drug circumstance. Obviously, such classifications require considerable discretion on the part of crime analysts, but we should expect to see a rise in the proportion of drug-related homicides if expanding drug markets were a major contributor to the homicide increase.

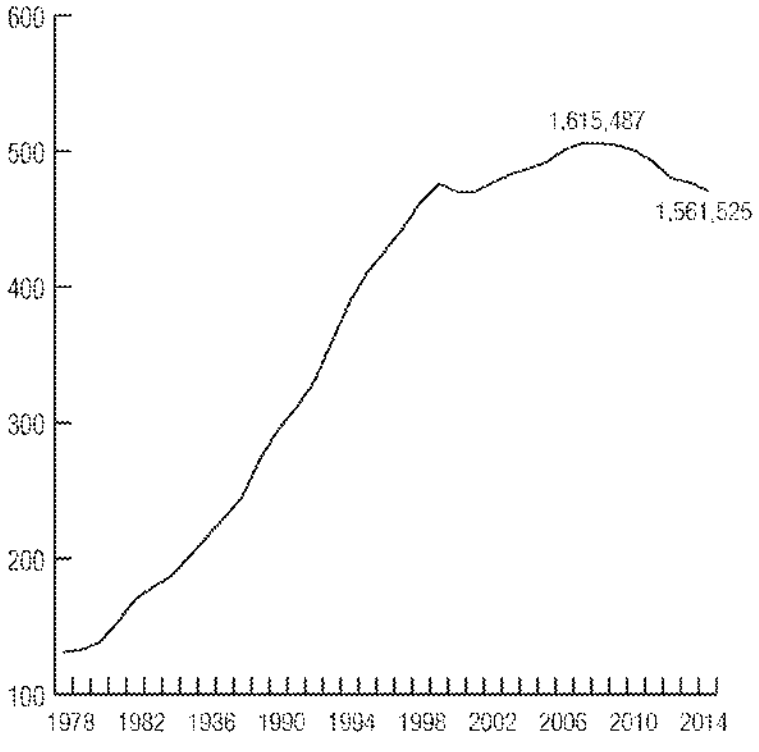
[13] See http://www.bjs.gov/index.cfm?ty=datool&surl=/arrests/index.cfm.

IMPRISONMENT

After rising continuously for several decades, the number of state and federal prisoners in the United States peaked in 2009 and began to decline modestly, as shown in Figure 6 (for source data, see http://www.bjs.gov/index.cfm?ty=nps). In 2014, 1.56 million persons were serving time in prison, down from the peak of 1.62 million in 2009. Rising imprisonment rates are associated with declining crime rates, although debate exists regarding the strength and policy implications of the relationship, as shown by the recent National Research Council report, *The Growth of Incarceration in the United States: Exploring Causes and Consequences* (Travis, Western, and Redburn 2014). Falling imprisonment rates might then trigger crime increases, assuming the relationship between imprisonment and crime is symmetrical. Did the growing number of ex-prisoners returning home contribute to the 2015 homicide increase?

As with the drug market hypothesis, there are reasons for and against assuming that declining imprisonment was a major contributor to the 2015 homicide rise. Ex-prisoners have high recidivism rates; the most recent data indicate that two-thirds will be arrested within three years after release (Cooper, Durose, and Snyder 2014). The arrest rates of released prisoners are far greater than those of general population groups of the same age and race (Rosenfeld, Wallman, and Fornango 2005). As more released prisoners re-enter the population, other things equal, crime rates should rise. But all else is rarely equal, if for no other reason than some number of persons will be entering prison at the same time others are released. The crimes committed by the latter should be discounted by the crimes the former would have committed had they remained free. A reasonably accurate indicator of the net

Figure 6: U.S. Imprisonment Rate per 100,000 Population, 1978-2014



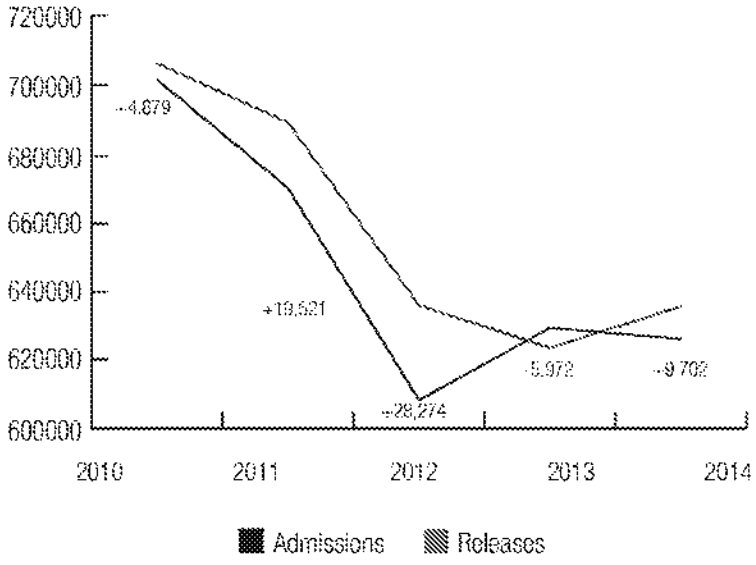
Source: Bureau of Justice Statistics

contribution of imprisonment to crime, therefore, is the number of persons released from prison minus the number entering prison during a given period. Figure 7 displays these figures for the period 2010 to 2014.

With the exception of 2013, prison releases exceeded prison entries during the five-year period shown in Figure 7. But the net increase in returning prisoners varied considerably, from fewer than 5,000 in 2010 to more than 28,000 in 2012. The large net increase in ex-prisoners in 2012 may have contributed to the homicide rise three years later, but the time lag requires additional explanation. The results of a recent study are generally supportive of a time lag between imprisonment rates and crime rates. Rosenfeld and Levin (2016) found that imprisonment rates have nonsignificant effects on crime rates in the short run but significant effects that unfold over several years. That study, however, focused on robbery and property crime rates; it is unknown whether similar results exist for homicide.

Future research on the role of imprisonment in the 2015 homicide rise must address the variation in prison releases and admissions across states and cities (see http://www.bjs.gov/index.cfm?ty=nps). Three instructive empirical indicators for assessing the contribution of imprisonment to the homicide increase are (1) the net change in the number of prisoners released from and entering prison, (2) the number of persons on parole and (3) the fraction of homicides committed by persons on parole.

Figure 7: Prison Releases and Admissions, 2010-2014



Source: Bureau of Justice Statistics

The first two indicators essentially depict the flow and stock, respectively, of ex-prisoners in the jurisdiction. Published data on parolees at the state level are available from the Bureau of Justice Statistics' (BJS's) yearly probation and parole surveys.[14] County-level data from the surveys would have to be obtained under special arrangement with BJS or directly from state corrections departments. The third indicator provides evidence of

[14] See http://www.bjs.gov/index.cfm?ty=tp&tid=1521. The surveys, of course, do not include ex-prisoners who have "maxed out" their sentences and are not under community supervision.

change over time in the involvement in homicide, both as offenders and victims, of ex-prisoners under community supervision. If ex-prisoners contributed significantly to the homicide increase, researchers should observe a corresponding increase in the homicide rate of persons on parole and in the proportion of homicides committed by parolees in those cities exhibiting large increases in homicide. These data will have to be compiled from the records of local law enforcement agencies.

FERGUSON EFFECT

What has become known as the "Ferguson effect" on the homicide increase, as noted, is subject to considerable controversy and evidence-free rhetoric. The term is also unfortunate, because it does not only apply to the police killing in Ferguson and because its precise meaning is unclear. The dominant de-policing interpretation is that highly publicized incidents of police use of deadly force against minority citizens, including but not limited to the Ferguson incident, caused police officers to disengage from their duties, particularly proactive tactics that prevent crime. Interestingly, however, that is not the interpretation of the individual who evidently coined the term. Sam Dotson, Chief of the St. Louis Metropolitan Police Department, used the term in an interview with a reporter in November of 2014, three months after Michael Brown was killed. "It's the Ferguson effect," Dotson said. "I see it not only on the law enforcement side, but the criminal element is feeling empowered by the environment" (Byers 2014).

It is important to emphasize both arguments Chief Dotson advanced in the interview.[15] He stated that the police in St. Louis were redeployed from their normal and more proactive responsibilities to address protest activities and civil disorder in Ferguson and elsewhere in the St. Louis area during the months immediately following Brown's death. As conditions returned to normal, so did police activity. For example, arrest rates returned to pre-Ferguson levels after decreasing during the late summer and fall of 2014.

In the view of the St. Louis police chief, changes in police deployment patterns did result in crime increases in St. Louis in the immediate aftermath of the Ferguson incident. But he does not believe that his officers engaged in de-policing in the conventional sense of a work slowdown or reluctance to engage in vigorous, proactive enforcement. That is where the second point becomes relevant. The Ferguson effect, in his view, was not simply a matter of altered police behavior. Criminals, according to Chief Dotson, became "empowered" by the police killing in Ferguson and ensuing protests and civil unrest. The question then becomes how such feelings and beliefs might have triggered a homicide increase that persisted at least another year after Ferguson.

Intentionally or not, the St. Louis police chief invoked an important strain of sociological and criminological thinking in his explanation of the Ferguson effect: the idea that violence escalates when individuals and communities are alienated from the legitimate means of social control. When persons do not trust the police to act on their behalf and to treat them fairly and with respect, they lose confidence in the formal apparatus of social

[15] The discussion in this section is based on Byers (2014) and personal communication with Chief Dotson.

control and become more likely to take matters into their own hands. Interpersonal disputes are settled informally and often violently. Honor codes develop that encourage people to respond with violence to threats and disrespect (Anderson 1999). Predatory violence increases because offenders believe victims and witnesses will not contact the police. Individuals engage in "self-help" and entire communities become "stateless" social locations (Black 1983, 2010).

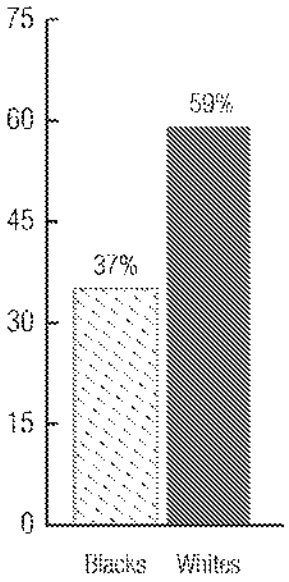
Randolph Roth (2009) has distinguished the proximate and ultimate causes of historical changes in U.S. homicide rates. Proximate causes refer to conditions that criminologists typically point to as risk factors for violence (e.g., economic disadvantage, firearm carrying, drug and alcohol use). Ultimate causes are the more or less widespread popular beliefs that government and the legal system are legitimate and worthy of respect, and that government officials can be trusted. When the perceived legitimacy of government and trust in officials erode, according to Roth, homicide rates increase. Such historical periods include the years immediately preceding the American Revolution and the Civil War. Both Roth (2009) and Gary LaFree (1998) have attributed the rise in homicide during the 1960s and 1970s to the declining legitimacy of U.S. political institutions.

The police are the front line of government in disadvantaged urban communities. Following Roth (2009), the ultimate cause of violence in these communities is lack of confidence in the police. When the police are called to respond to a crime, they arrive at the scene late or not at all. They do not follow up with vigorous and thorough investigation, even of the most serious crimes (Leovy 2015). They harass innocent youth. And, too often, they use force unnecessarily and indiscriminately. What matters is not the factual accuracy of these beliefs in every instance; what matters is that they can metastasize into a pronounced "legal cynicism," especially in disadvantaged African-American communities (Sampson and Bartusch 1998). When people believe the procedures of formal social control are unjust, they are less likely to obey the law (Tyler 2006).

If this complex of "feelings and beliefs," in Roth's (2009) terms, is the ultimate cause of escalations in homicide, the more proximate cause could be widely publicized incidents of police use of force that seem to confirm the validity of the underlying belief system. Lack of confidence in the police among African-Americans predates the recent police killings in Ferguson, Cleveland, New York and elsewhere. But it is likely to be activated by such incidents, transforming longstanding latent grievances into an acute legitimacy crisis. If that led to the 2015 homicide increase, we should expect at least four empirical conditions to hold: (1) the increase should be concentrated in cities with large African-American populations, (2) the timing of the increase should correspond closely to controversial incidents of police use of force against African-Americans, (3) confidence in the police should be substantially lower among African-Americans than other groups and (4) the homicide increase should be greater among African-Americans than other groups.

The available evidence supports the first two expectations. We have seen that 10 cities with relatively large African-American populations accounted for two-thirds of the

Figure 8: Percentage of Adults With "a Great Deal/ Quite a Lot" of Confidence in the Police (2011-2014)

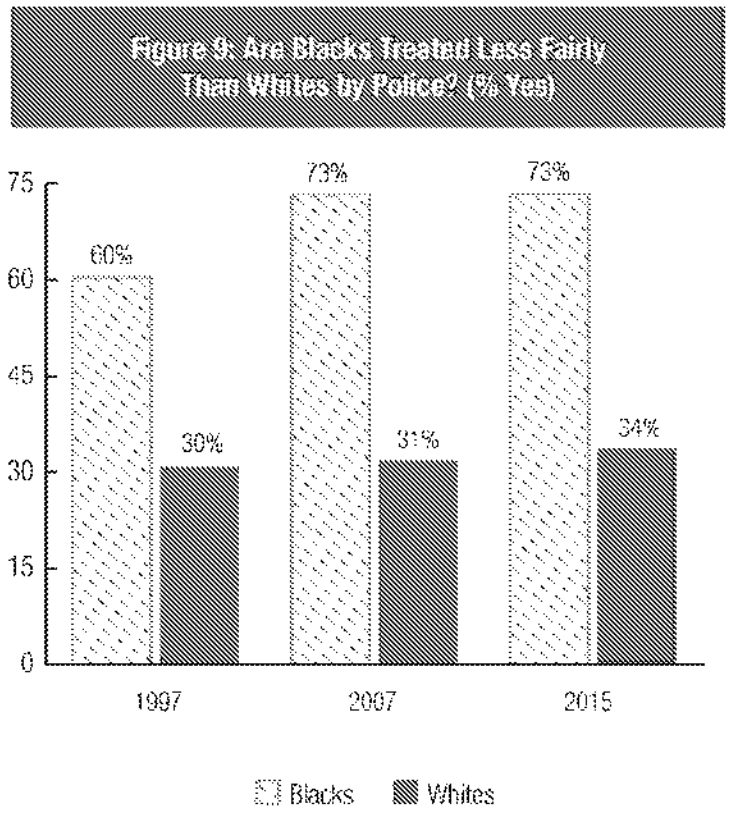


Source: Gallup Poll

big-city homicide increase in 2015 (see Table 1 and Figure 3). Further, the homicide increase occurred in the immediate aftermath of controversial police use-of-force incidents. The timing of the increase provides stronger support for the Ferguson effect explanation, in either of its versions, than for explanations attributing the homicide rise to expanding drug markets or declining imprisonment. Neither hypothesis can easily account for the sheer abruptness of the increase in 2015 or, in the case of the drug market explanation, for why homicide rates did not begin to rise several years earlier. At the same time, researchers must be open to the possibility that the homicide increase predated the Ferguson events, at least in some cities (Rosenfeld 2015).

There is ample evidence in support of the third expectation regarding African-Americans' lack of confidence in the police. As shown in Figure 8, just 37 percent of blacks compared with 59 percent of whites expressed "a great deal" or "quite a lot" of confidence in the police in Gallup surveys conducted between 2011 and 2014.[16] The sizable racial gap in attitudes toward the police is not the result of Ferguson or other recent events. For example, in 1997, 60 percent of blacks compared with 30 percent of whites answered "yes" when asked in Gallup surveys whether the police treat blacks less fairly than whites, as shown in Figure 9 (see page 21). The racial difference in responses to this item increased over the next 10 years. Interestingly, the racial gap did not change appreciably between 2007 and 2015, the year after the Ferguson incident and other controversial episodes of police use of deadly force against African-Americans. Finally, the difference between blacks and whites in attitudes toward the police extends to the justice system as a whole, as shown in Figure 10 (see page 22). Fully two-thirds of black respondents and just a quarter of whites told Gallup in 2013 they believe the justice system is biased against blacks. After Ferguson in 2015, the percentage of blacks who believe the justice system is biased increased to 74 percent, although the comparable increase among whites was larger, rising to 42 percent.

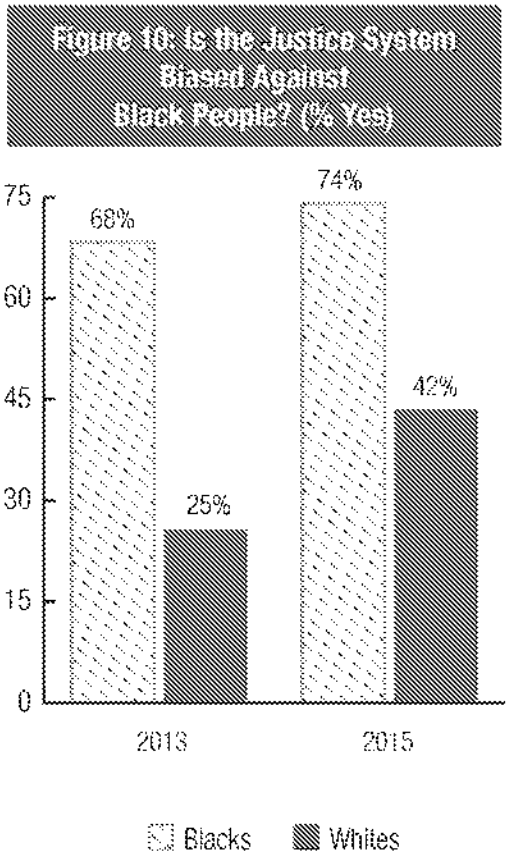
[16] For source data for Figures 8-10, see http://www.gallup.com/poll/175088/gallup-review-black-white-attitudes-toward-police.aspx.



Source: Gallup Poll

There is little question that blacks and whites differ greatly in their confidence in the police, belief that the police treat blacks less fairly than whites, and belief that the justice system is racially biased. The racial gap in attitudes toward the police is not a recent development. Tensions between the police and the black community triggered the urban civil disorders of the 1960s (Report of the National Commission on Civil Disorders 1968). Lack of confidence in the police represents a smoldering reservoir of discontent among African-Americans that is ignited by heavily publicized episodes of police use of force — the ultimate and proximate causes, respectively, of the escalation of violence. This hypothesis regarding the recent homicide rise merits close scrutiny by researchers, along with the alternative version of the Ferguson effect that attributes the homicide increase to de-policing. Finally, if the legitimacy crisis explanation is correct, we should observe larger increases in homicide among African-Americans than whites or other groups. Further, the increases should be concentrated in the disadvantaged black communities of large cities where legal cynicism is most pronounced (Sampson and Bartusch 1998).

It will be easier to empirically evaluate the de-policing hypothesis than the legitimacy crisis explanation of the 2015 homicide increase. If de-policing was the operative mechanism, we should observe larger drops in arrests and other self-initiated police activities in cities that experienced the greatest homicide increases. The arrest data are readily available from the UCR, or will be when the 2015 UCR data are released in the fall of 2016. Data on pedestrian and traffic stops, building checks, and other self-initiated police activity will have to be obtained from local police departments. It should be noted, however, that the de-policing hypothesis presupposes a very large effect of policing on crime, large enough to explain homicide increases from de-policing of 50 percent or more in some cities. Effect sizes of that magnitude far surpass those revealed in research on the most effective policing strategies to prevent crime (Braga, Papachristos, and Hureau 2014).



Source: Gallup Poll

Testing the hypothesis that a police legitimacy crisis caused the homicide increase will be more difficult. The four empirical expectations discussed above are necessary but not sufficient conditions to rule out other explanations. The key question that must be answered concerns the mechanisms that translate community discontent with the police into escalating levels of violence. Very little is known about this hypothesized relationship. Does widespread discontent lead offenders to believe they can commit crime with impunity? That seems to be what the St. Louis police chief meant when he said criminals became "empowered" by the Ferguson events. Is community discontent with the police fertile soil for "stop snitching" campaigns? Even more basic criminological questions are at issue. Was the homicide increase fueled primarily by offenders and victims with extensive criminal records or did the violence spread beyond the already criminally involved population? In other words, was the increase spurred by a growing prevalence of criminal violence or by a heightened incidence of violence among active offenders?

The latter question might be addressed with data from ongoing longitudinal studies of delinquency and crime (e.g., Berg et al. 2016; Loeber and Farrington 2011). To determine whether discontent with the police reduced the willingness of African-Americans to report crimes to the police, police reporting rates by race can be accessed from the National Crime Victimization Survey when BJS releases the 2015 data and the results can be compared with those for previous years and across differing community types. The best and perhaps only way to address other questions pertaining to the hypothesized police legitimacy crisis is through ethnographic research in African-American communities that seeks to disclose how chronic discontent with the police may be activated by controversial incidents of police use of force and, in turn, may lead to a rise in violence.

In summary, there are several empirical indicators and methods to evaluate alternative explanations of the 2015 homicide rise. It may turn out that the three considered here, as well as others yet to be proposed, are not competing hypotheses so much as interacting components of a broader explanation. For example, we might expect offenders to feel

especially "empowered," not only in the context of community discontent and anger, but when they also believe, correctly or not, that the police have backed off as a result. Homicide increases owing to a Ferguson effect might have been greater in cities with expanding drug markets and a larger pool of recently released prisoners than elsewhere. The necessary research will take time to carry out and must await the release of key empirical indicators.

TOWARD A 21ST CENTURY CRIME INFORMATION SYSTEM

At several points in this discussion, reference has been made to the need to wait for the release of data needed to document and explain the recent homicide increase. The FBI's UCR data cannot answer all of the empirical questions raised here, but they can be used to address some important ones, such as whether arrest rates fell in the large cities registering homicide increases or, indeed, whether the homicide increase extended beyond the large cities. FBI Director Comey has pointed to the importance of the data his agency compiles for understanding and responding to the homicide rise, noting that "without more reliable data, the task of identifying trends and remedies to fix them is far more challenging. . . . [I]t's important, because it gives us the full picture of what's happening" (Schmit and Apuzzo 2015).

Imagine how the public debate over the homicide rise might have differed had the FBI released monthly UCR data one or two months after the collection period. We would have known whether other crimes in addition to homicide were increasing. We would know whether smaller cities were experiencing crime increases. We would not have had to rely on newspaper reporters and policy advocates to gather data from small and nonrepresentative samples. Assuming the Supplementary Homicide Reports data were not far behind, researchers would have had some indication of whether drug-related homicides were on the rise. The debate over de-policing could have been informed by comparative data on arrest rates. Better and timelier data would not have ended the debate, but they would have placed it on sounder empirical footing.

There are no longer technical impediments to timely release of the nation's crime and arrest data by the FBI. That is largely because the national UCR program no longer compiles data directly from the 18,000 law enforcement agencies in the country. Rather, most of the data are compiled, checked and submitted by state UCR programs.[17] Many of the state programs submit the data on a monthly basis and those that do not can be encouraged to do so. Even if the FBI was able to release timely data for just five percent of the nation's law enforcement agencies, roughly 900 jurisdictions, that would constitute a much larger number of cases than currently available. Researchers could then construct reasonably representative samples from those data that would be far more useful than the

[17] According to the UCR Data Quality Guidelines: "For the most part, agencies submit monthly crime reports, using uniform offense definitions, to a centralized repository within their state. The state UCR Program then forwards the data to the FBI's UCR Program" (www.fbi.gov/about-us/cjis/ucr/data-quality-guidelines-new/#_ftn2).

samples of a few dozen cities that journalists and policy advocates have been able to stitch together.

The dissemination of timelier crime data that are useful for addressing crime problems as they arise would require that the FBI return to a practice it abandoned more than 80 years ago. During the 1930s, the FBI released crime data on a monthly basis (Rosenfeld 2011b). Admittedly, there were fewer law enforcement agencies in the 1930s, but the data were entered in pen and ink or on manual typewriters and then sent by the local post office to Washington. If the FBI could release monthly data under those conditions, surely it can do so in an age of electronic data transfer when local police departments routinely post recent crime information on their public websites.

Fortunately, the FBI is now working closely with BJS to modernize the nation's police-based crime data infrastructure.[18] A high priority in this cooperative effort should be to disseminate crime and arrest data on a schedule that makes the data useful for addressing emerging crime problems. Otherwise, we can be certain that the press and advocacy organizations will attempt to fill the information void with data of uncertain reliability — the very problem to which FBI Director Comey has directed attention in his comments on the recent crime rise. The nearly unprecedented homicide increase of 2015 should be all that is necessary to finally move the nation's crime monitoring system into the 21st century.

[18] See, e.g., http://www.bjs.gov/content/pub/pdf/NCS-X_FBI_BJS%20Joint_Statement.pdf.

APPENDIX: CITY SAMPLE

New York City	Columbus	Las Vegas	Raleigh
Los Angeles	Fort Worth	Louisville	Miami
Chicago	Charlotte	Milwaukee	Oakland
Houston	Detroit	Albuquerque	Minneapolis
Philadelphia	El Paso	Tucson	Tulsa
Phoenix	Seattle	Fresno	Cleveland
San Antonio	Denver	Sacramento	Wichita
San Diego	Washington DC	Long Beach	St. Louis
Dallas	Memphis	Kansas City	New Orleans
San Jose	Boston	Mesa	Arlington
Austin	Nashville	Atlanta	Tampa
Jacksonville	Baltimore	Virginia Beach	Newark
San Francisco	Oklahoma City	Omaha	Orlando
Indianapolis	Portland	Colorado Springs	Salt Lake City

City Sample (N = 58)

REFERENCES

Anderson, Elijah. 1999. *Code of the Street: Decency, Violence, and the Moral Life of the Inner City*. New York: Norton.

Berg, Mark, Eric Baumer, Richard Rosenfeld, and Rolf Loeber. Forthcoming. Dissecting the prevalence and incidence of offending during the crime decline of the 1990s. *Journal of Quantitative Criminology*.

Bialik, Carl. 2015. Scare headlines exaggerated the U.S. crime wave. *FiveThirtyEight* (September 11). http://fivethirtyeight.com/features/scare-headlines-exaggerated-the-u-s-crime-wave/. Retrieved February 29, 2016.

Black, Donald. 1983. Crime as social control. *American Sociological Review* 48: 34-45.

Black, Donald. 2010. *The Behavior of Law*. Special ed. United Kingdom: Emerald Group.

Blumstein, Alfred. 1995. Youth violence, guns, and the illicit drug industry. *Journal of Criminal Law and Criminology* 86: 10-36.

Blumstein, Alfred, and Richard Rosenfeld. 1998. Explaining recent trends in US homicide rates. *Journal of Criminal Law and Criminology* 88: 1175-1216.

Blumstein, Alfred, and Joel Wallman, eds. 2006. *The Crime Drop in America,* revised ed. New York: Cambridge University Press.

Bourgois, Philippe. 2003. *In Search of Respect: Selling Crack in El Barrio,* second ed. New York: Cambridge University Press.

Braga, Anthony A., Andrew V. Papachristos, and David M. Hureau. 2014. The effects of hot spots policing on crime: An updated systematic review and meta-analysis. *Justice Quarterly* 31: 633-663.

Byers, Christine. 2014. Crime up after Ferguson and more police needed, top St. Louis area chiefs say. *St. Louis Post-Dispatch* (November 15). http://www.stltoday.com/news/local/crime-and-courts/crime-up-after-ferguson-and-more-police-needed-top-st/article_04d9f99f-9a9a-51bc-a231-1707a57b50d6.html. Retrieved March 11, 2016.

Byrne, John. 2015. Emanuel blames Chicago crime uptick on officers second-guessing themselves. *Chicago Tribune* (October 13). http://www.chicagotribune.com/news/local/politics/ct-emanuel-fetal-police-met-20151012-story.html. Retrieved February 29, 2016.

Coates, Ta-Nehisi. 2015. There is no Ferguson effect. *Atlantic* (September 1). http://www.theatlantic.com/notes/2015/09/there-is-no-ferguson-effect/403132/. Retrieved February 29, 2016.

Cohen, Andrew. 2015. How white users made heroin a public-health problem. *Atlantic* (August 12). http://www.theatlantic.com/politics/archive/2015/08/crack-heroin-and-race/401015/. Retrieved March 8, 2016.

Contreras, Randol. 2013. *The Stickup Kids: Race, Drugs, Violence, and the American Dream*. Berkeley, CA: University of California Press.

Cooper, Alexia D., Matthew R. Durose, and Howard N. Snyder. 2014. Recidivism of Prisoners Released in 30 States in 2005: Patterns from 2005 to 2010. Washington, DC: U.S. Department of Justice, Bureau of Justice Statistics. http://www.bjs.gov/index.cfm?ty=pbdetail&iid=4986. Retrieved March 9, 2016.

Cork, Dan. 1999. Examining space–time interaction in city-level homicide data: Crack markets and the diffusion of guns among youth. *Journal of Quantitative Criminology* 15: 379-406.

Davey, Monica, and Mitch Smith. 2015. Murder rates rising sharply in many U.S. cities. *New York Times* (August 15). http://www.nytimes.com/2015/09/01/us/murder-rates-rising-sharply-in-many-us-cities.html?_r=1. Retrieved February 29, 2016.

Friedman, Matthew, Nicole Fortier, and James Cullen. 2015. *Crime in 2015: A Preliminary Analysis*. New York: New York University School of Law, Brennan Center for Justice (November 18). http://www.brennancenter.org/publication/crime-2015-preliminary-analysis. Retrieved February 29, 2016.

Jones, Christopher M., Joseph Logan, R. Matthew Gladden, and Michele K. Bohm. 2015. Vital signs: Demographic and substance use trends among heroin users – United States, 2002-2013. *Morbidity and Mortality Weekly Report* 64: 719-725.

LaFree, Gary. 1998. *Losing Legitimacy: Street Crime and the Decline of Social Institutions in the United States*. Boulder, CO: Westview.

Leovy, Jill. 2015. *Ghettoside*. New York: Spiegel & Grau.

Levitt, Steven D. 1996. The effect of prison population size on crime rates: Evidence from prison overcrowding litigation. *Quarterly Journal of Economics* 111: 319-351.

Loeber, Rolf, and David P. Farrington. 2011. *Young Homicide Offenders and Victims*. New York: Springer.

Mac Donald, Heather. 2015. Trying to hide the rise of violent crime. *Wall Street Journal* (December 25). http://www.wsj.com/articles/trying-to-hide-the-rise-of-violent-crime-1451066997. Retrieved February 29, 2016.

Mac Donald, Heather. 2016. Obama's assault on the police. *Commentary* (February 17). https://www.commentarymagazine.com/articles/obamas-assault-police/. Retrieved February 29, 2016.

Messner, Steven F., Glenn D. Deane, Luc Anselin, and Benjamin Pearson-Nelson. 2005. Locating the vanguard in rising and falling homicide rates across U.S. cities. *Criminology* 43: 661-696.

Ousey, Graham, and Matthew R. Lee. 2002. Examining the conditional nature of the illicit drug market-homicide relationship: A partial test of the theory of contingent causation. *Criminology* 40: 73-102.

Police Executive Research Forum. 2006. *A Gathering Storm—Violent Crime in America*. http://www.policeforum.org/assets/docs/Critical_Issues_Series/a%20gathering%20storm%20-%20violent%20crime%20in%20america%202006.pdf. Retrieved March 1, 2016.

Pyrooz, David C., Scott H. Decker, Scott E. Wolfe, and John A. Shjarback. 2016. Was there a Ferguson effect on crime rates in large U.S. cities? *Journal of Criminal Justice* 46: 1-8.

Report of the National Commission on Civil Disorders, Kerner Commission. 1968. Washington, DC: U.S. Government Printing Office.

Reuter, Peter, ed. 2010. *Understanding the Demand for Illegal Drugs*. Washington, DC: National Academies Press.

Rosenfeld, Richard. 2007. Transfer the Uniform Crime Reporting Program from the FBI to the Bureau of Justice Statistics. *Criminology and Public Policy* 6: 825-834.

Rosenfeld, Richard. 2011a. Changing crime rates. In *Crime and Public Policy,* edited by James Q. Wilson and Joan Petersilia. New York: Oxford University Press.

Rosenfeld, Richard. 2011b. The big picture: 2010 Presidential Address to the American Society of Criminology. *Criminology* 49: 1-26.

Rosenfeld, Richard. 2015. *Was there a 'Ferguson effect' on crime in St. Louis?* Sentencing Project Policy Brief. Washington, DC: Sentencing Project. http://sentencingproject.org/wp-content/uploads/2015/09/Ferguson-Effect.pdf.

Rosenfeld, Richard, and Scott H. Decker. 1999. Are arrest statistics a valid measure of illicit drug use? *Justice Quarterly* 16: 685-699.

[redacted] (DO) (OGA)

From: [redacted] (DO) (OGA) b6 1 b7C 1
Sent: Saturday, February 04, 2017 6:04 PM
To: Rybicki, James E. (DO) (FBI)
Subject: Fwd: Professor Richman re U.S. v. Percoco
Attachments: US v Percoco et al Indictment - Foreperson Signed (1).pdf

Just FYI that I'm following up.

-------- Original message --------
From: [redacted] (DO) (FBI)" [redacted] b6 1, 4 b7C 1, 4 b7E 3
Date: 2/4/17 3:21 PM (GMT-05:00)
To: [redacted] (DO) (OGA)" [redacted] "Richman, Daniel C. (DO) (OGA)" [redacted]
Cc: "Kelley, Patrick W. (DO) (FBI)" [redacted] (DO) (FBI)" [redacted]
Subject: Professor Richman re U.S. v. Percoco

[redacted] good afternoon. By all means, we can discuss at your convenience, including today if you happen to see this message. My contacts are also below. I'm in the office now and foreseeably a bit longer, and also will have my Bureau mobile. If you prefer, I can also continue to correspond via UNET email.

I talked with Prof. Richman last night, who was planning to call and apprise you; so I thought best to add him here, too. I've also copied my boss OIC AD Pat Kelley, who as you may know is the FBI's Deputy Designated Agency Ethics Official (DDAEO), and ethics attorney [redacted] who has been assisting on this matter, as well as communicating with Prof. Richman. [redacted] and I discussed this matter with Pat late last Thursday. b6 1 b7C 1

The gist is that while there appears to be no 18 U.S.C. §§ 203 or 205 concerns, since Prof. Richman has not worked more than 60 days as a Special Government Employee (SGE) for the FBI in the last 365 days, there is still the issue of "outside employment" which means any form of employment involving "personal services," whether or not for compensation. The DOJ Supplemental Regulations (5 C.F.R. § 3801.106) restricts Department employees, including SGEs, from engaging in outside employment that, per Subsection (b)(1) involves: (i) the practice of law, unless uncompensated and in the nature of community service or on behalf of yourself, your parents, spouse or children; (ii) any criminal or habeas corpus matter, be it Federal, State, or local; or, (iii) litigation, investigations, grants or other matters in which the Department of Justice is or represents a party, witness, litigant, investigator or grant-maker. Professor Richman's role as "part of the joint defense team" (per the Engagement Letter he provided us) in the case of *U.S. v. Percoco*, involves the practice of law, a criminal matter, and litigation in which the DOJ is a party; per the attached indictment.

Although the DOJ/JMD/DEO summary of the SGE ethics rules (https://www.justice.gov/jmd/summary-government-ethics-rules-special-government-employees) states: "[t]hese prohibitions may be waived by the Deputy Attorney General and generally are waived in the case of a special government employee ..." --

at this time we do not have a waiver. Moreover, it is not necessarily a given that a waiver would be granted for this particular matter. To assist all parties with this determination, we have contacted the NY field office for any additional information on the FBI's interests in this case. Meanwhile, we have recommended that Prof. Richman not be involved with the defense team until we can better determine whether a waiver will or will not be granted. We should know more, hopefully definitively, by the end of next week.

b6 1
b7C 1

Please let us know if you have any questions, or if you would like to meet to discuss further by phone or in person. Thank you.

[redacted]

-----Original Message-----
From: [redacted] (DO) (OGA)
Sent: Friday, February 03, 2017 6:23 PM
To: [redacted] (DO) (FBI) [redacted]
Subject: Re:

b6 1
b7C 1
b7E 3

[redacted]

Your message below was forwarded to me by Jim Rybicki to follow up. Could we set up a time for a quick phone call to get me up to speed on Dan Richman's status early next week sometime?

Thanks.

[redacted]
Special Counsel to the Director
Federal Bureau of Investigation

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

[redacted] (DO) (FBI)

b6 1
b7C 1

From: [redacted] (DO) (FBI)
Sent: Friday, February 03, 2017 5:56 PM
To: [redacted] (DO) (FBI)
Cc: Kelley, Patrick W. (DO) (FBI)
Subject: FW: Professor Richman's contact(s)
Attachments: United States v. Percoco et al - Sealed complaint (2).pdf

[redacted] fyi. I talked with Prof. Richman. He confirmed that he had not worked more than 60 days in the last 365 day period. He did mention his work consists primarily of answering emails, and recalled reading where that was not considered a work day. However, even if it was, he was confident that it was still less than 60 days. So with 203/205 removed, he understood the remaining issue is the DOJ sup reg 5 C.F.R. § 3801.106. I explained that even if he practiced law without compensation (pro bono) there is still the "criminal matter." I let him know we have contacted the NY CDC for assistance in helping us determine any FBI role/interest, and if so its extent. We also discussed the FBI's DDAEO role, DEO/DAEO and the DAG waiver, in relation to any FBI or Department interests in the case. Finally, I advised (and consulted with Pat to confirm) ... that Prof. Richman not take any actions on behalf of the defense for one week, as by next Friday we should have the requisite information to know whether a waiver would be supported.

b6 1
b7C 1

So for now, I think we're good and nothing more needs to be done regarding any follow-up email to Prof. Richman, who was going to apprise the Director's Special Counsel. Meanwhile, I let Prof. Richman know not to hesitate to contact either you or me with any further questions.

[redacted]

P.S. Thanks, again, for your work identifying, researching, and briefing this matter.

From: Daniel Charles Richman [mailto:[redacted]
Sent: Friday, February 03, 2017 5:22 PM
To: [redacted] (DO) (FBI) [redacted]
Subject: Re: Professor Richman's contact(s)

here's the complaint
thx again for your help and have a lovely weekend
d

b6 1, 4
b7C 1, 4
b7E 3

On Fri, Feb 3, 2017 at 3:24 PM, [redacted] (DO) (FBI) <[redacted]> wrote:

> Prof Richman: Dan, thank you for the reply. Yes, 4:30 good for me. I'm here in the office until 6pm if you're not able to talk right then. You're also welcome to call me at any time on my work cell; listed below.
>
> [redacted]
>
> ----- Original Message-----
> From: Richman, Daniel C. (DO) (OGA)
> Sent: Friday, February 03, 2017 12:51 PM
> To: [redacted] (DO) (FBI) <[redacted]>; Rybicki, James E. (DO) (FBI)

[redacted]

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

b6 1, 4
b7C 1, 4
b7E 3

Subject: Re: Professor Richman's contact(s)

Hi [redacted] Thanks for reaching out. Would you be free to talk at 4:30 today? (I have an awful faculty mtg most of the afternoon). More generally, a quick way to reach me is my school email [redacted] or my cell [redacted] or my office [redacted] thx dan r

---

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)

b6 1
b7C 1

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.

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

[redacted]

Chief, Ethics and Integrity Unit (EIU)
Office of Integrity and Compliance (OIC)
Desk: [redacted] Mobile: [redacted]

--
BEGIN-ANTISPAM-VOTING-LINKS

Teach Email if this mail (ID 01SEknXnD) is spam:

Spam: https://antispam.law.columbia.edu/canit/b.php?i=01SEknXnD&m=e3cbf031da39&t=20170203&c=s

Not spam: https://antispam.law.columbia.edu/canit/b.php?i=01SEknXnD&m=e3cbf031da39&t=20170203&c=n

Forget vote: https://antispam.law.columbia.edu/canit/b.php?i=01SEknXnD&m=e3cbf031da39&t=20170203&c=f

---

END-ANTISPAM-VOTING-LINKS

--
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

Approved: _____
JANIS ECHENBERG/ROBERT BOONE/DAVID ZHOU/MATTHEW PODOLSKY
Assistant United States Attorneys

Before: THE HONORABLE GABRIEL W. GORENSTEIN
United States Magistrate Judge
Southern District of New York

16 MAG 6005

UNITED STATES OF AMERICA	SEALED COMPLAINT
- v. -	Violations of 18 U.S.C. §§ 666, 1001, 1349, 1951, and 2
JOSEPH PERCOCO, a/k/a "Herb,"	
ALAIN KALOYEROS, a/k/a "Dr. K,"	
PETER GALBRAITH KELLY, JR., a/k/a "Braith,"	COUNTY OF OFFENSE: NEW YORK
STEVEN AIELLO,	
JOSEPH GERARDI,	
LOUIS CIMINELLI,	
MICHAEL LAIPPLE, and	
KEVIN SCHULER,	
Defendants.	

SOUTHERN DISTRICT OF NEW YORK, ss.:

DELEASSA PENLAND, being duly sworn, deposes and says that she is a Criminal Investigator with the United States Attorney's Office for the Southern District of New York ("USAO"), and charges as follows:

COUNT ONE

(Conspiracy to Commit Extortion Under Color of Official Right)

1. 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, 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, Section 1951.

2. It was a part and an object of the conspiracy that JOSEPH PERCOCO, a/k/a "Herb," the defendant, and others known and unknown, willfully and knowingly, would and did obstruct, delay, and affect commerce and the movement of articles and commodities in commerce by extortion as that term is defined in Title 18, United States Code, Section 1951, to wit, PERCOCO, who was a senior official in the Office of the Governor of New York State (the "State"), and others known and unknown, would and did cause companies with business before the State 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 TWO

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

3. 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, willfully and knowingly, would and did obstruct, delay, and affect commerce and the movement of articles and commodities in commerce by extortion as that term is defined in Title 18, United States Code, Section 1951, to wit, PERCOCO used his official State position and power and authority within the Office of the Governor to cause an energy company seeking benefits and business from the State (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 THREE

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

4. 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, willfully and knowingly, would and did obstruct, delay, and affect commerce and the movement of articles and commodities in commerce by extortion as that term is defined in Title 18, United States Code, Section 1951, to wit, PERCOCO

used his official State position and power and authority within the Office of the Governor to cause a Syracuse-based real estate developer seeking benefits and business from the State (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 FOUR

(Conspiracy to Commit Honest Services Fraud)

5. 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, 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.

6. 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, 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 return for bribes paid, at the direction of KELLY, AIELLO, and GERARDI, by the Energy Company and the Syracuse Developer.

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

COUNT FIVE

(Solicitation of Bribes and Gratuities – The Energy Company)

7. 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 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 and 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, PERCOCO, in his capacity as a senior official in the Office of the Governor, solicited and accepted cash and things of value from the Energy Company intending for PERCOCO to be influenced and rewarded.

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

COUNT SIX

(Solicitation of Bribes and Gratuities – The Syracuse Developer)

8. 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 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 and 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, PERCOCO, in his capacity as a senior official in the Office of the Governor, solicited and accepted cash and things

of value from the Syracuse Developer intending for PERCOCO to be influenced and rewarded.

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

COUNT SEVEN

(Payments of Bribes and Gratuities - The Energy Company)

9. 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 an organization of a State government, and an agency thereof, in connection with business, transactions, and series of transactions of such organization, government, and 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, KELLY offered and gave bribes to JOSEPH PERCOCO, a/k/a "Herb," the defendant, in order for PERCOCO to influence regulatory approvals and funding related to the development of a power plant in Orange County, New York, and take other official action to benefit the Energy Company.

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

COUNT EIGHT

(Payments of Bribes and Gratuities - The Syracuse Developer)

10. 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 an organization of a State government, and an agency thereof, in connection with business, transactions, and series of transactions of such organization, government, and 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 offered and gave bribes to JOSEPH PERCOCO, a/k/a "Herb," the defendant, in order for PERCOCO to promote the Syracuse Developer's development projects in the State and take other official action to benefit the Syracuse Developer.

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

COUNT NINE

(Wire Fraud Conspiracy - The Preferred Developer RFPs)

11. 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.

12. 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, and SCHULER, and their co-conspirators, devised a scheme to defraud Fort Schuyler Management Corporation ("Fort Schuyler"), a State-funded entity charged with awarding 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, they secretly tailored the requests for proposals ("RFPs") for those contracts so that companies that were owned,

controlled, and managed by AIELLO, GERARDI, CIMINELLI, LAIPPLE, and SCHULER were guaranteed to win the contracts.

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

COUNT TEN

(Payments of Bribes and Gratuities - The Syracuse Developer RFP)

13. 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 an organization of a State government, and an agency thereof, in connection with business, transactions, and series of transactions of such organization, government, and 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 offered and gave bribes and gratuities to a representative of a New York State university and foundation in order to obtain a development contract.

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

COUNT ELEVEN

(Payments of Bribes and Gratuities - The Buffalo Developer RFP)

14. 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 an organization of a State government, and an agency thereof, in connection with business, transactions, and series of transactions of such organization, government, and 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 offered and gave bribes and gratuities to a representative of a New York State university and foundation in order to obtain a development contract.

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

COUNT TWELVE

(False Statements to Federal Officers)

15. 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, legislative, and judicial branches 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, 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).)

The bases for deponent's knowledge and for the foregoing charges are, in part, as follows:

16. I am a Criminal Investigator with the USAO, and I have been personally involved in the investigation of this matter, which has been handled by Special Agents of the Federal Bureau of Investigation, Buffalo Field Office ("FBI") and Criminal Investigators in the USAO. I have been employed by the USAO since 2015, prior to which I was a Revenue Agent with the Internal Revenue Service for more than twelve years. I and other members of the investigative team have experience in fraud and political corruption investigations and techniques associated with such investigations, including executing search warrants, financial analysis, and working with informants.

17. This affidavit is based in part upon my own observations, my conversations with other law enforcement agents and others, my

examination of documents and reports by others, my interviews of witnesses, and my training and experience. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of the investigation. Where the contents of documents, including emails, and the actions, statements and conversations of others are reported herein, they are reported in substance and in part, except where specifically indicated otherwise. For ease of reference, I have included a table of contents below.

TABLE OF CONTENTS

I. OVERVIEW

18. The charges in this Complaint stem from two overlapping criminal schemes involving bribery, corruption, and fraud in the award of hundreds of millions of dollars in State contracts and other official State benefits.

19. The first scheme (the "PERCOCO Bribery Scheme") involves efforts by JOSEPH PERCOCO, a/k/a "Herb," the defendant, who served as the Executive Deputy Secretary to the Governor of the State between in or about January 2012 and mid-2014, and again in or about 2015, to abuse his official position and extensive influence within the Executive Branch by seeking and accepting bribe payments from executives at companies that were seeking benefits and business from the State in exchange for use of PERCOCO's official authority and influence to benefit those companies. In part to disguise the nature and source of the bribe payments, bribes to PERCOCO were funneled in certain instances through a third-party intermediary and in other instances through bank accounts and a shell company set up by Todd Howe ("Howe"), a consultant who had been retained by the bribe-paying companies to help them obtain official State favors, and who is now cooperating with the Government.

20. More specifically, between 2012 and 2016, Howe arranged for more than $315,000 in bribe payments to JOSEPH PERCOCO, a/k/a "Herb," the defendant, and PERCOCO's wife, funded by two clients of Howe that were seeking substantial official State benefits at the time the payments were solicited and made: an energy company (the "Energy Company") and a Syracuse-based real estate developer (the "Syracuse Developer"). PETER GALBRAITH KELLY, JR., a/k/a "Braith," the defendant, oversaw external affairs and government relations for the Energy Company. KELLY arranged for PERCOCO and PERCOCO's wife to receive more than $287,000 in bribe payments from the Energy Company in exchange for PERCOCO's official assistance for the Energy Company on an as-needed basis, including helping the Energy Company obtain a State contract estimated to be worth $100 million, that would help finance a $900 million power plant in Wawayanda, New York, and assisting the Energy Company with obtaining millions of dollars in energy credits for a power plant it was building in New Jersey. STEVEN AIELLO and JOSEPH GERARDI, the defendants, were the President and the General Counsel, respectively, of the Syracuse Developer. AIELLO and GERARDI arranged for PERCOCO to receive approximately $35,000 in bribe payments in exchange for PERCOCO's official

assistance for the Syracuse Developer on an as-needed basis, including assisting the Syracuse Developer in reversing a costly decision of a State economic development agency, influencing the State to release payments owed to the Syracuse Developer, and obtaining a raise for AIELLO's son, a New York State employee who worked for PERCOCO.

21. The second scheme (the "Buffalo Billion Fraud and Bribery Scheme") involves bribery, corruption, and fraud in the award of contracts under the Governor's "Buffalo Billion" initiative and similar programs. In that scheme, executives at two companies, one of which was the Syracuse Developer, conspired with ALAIN KALOYEROS, a/k/a "Dr. K," the defendant, and Howe to deceive Fort Schuyler, a State-funded entity charged with awarding State contracts worth hundreds of millions of dollars, by secretly rigging the bidding process so that the contracts would be awarded to those two companies.

22. More specifically, ALAIN KALOYEROS, a/k/a "Dr. K," the defendant, who oversaw the application process for many of the State grants awarded under the Buffalo Billion and similar programs, retained Howe to assist with developing the projects and identifying developers for those projects. Howe in turn solicited and received bribe and gratuity payments from (a) the Syracuse Developer, run by, among others, STEVEN AIELLO and JOSEPH GERARDI, the defendants, who were seeking State development grants for projects in Syracuse, New York, and (b) a Buffalo-based developer (the "Buffalo Developer"), run by, among others, LOUIS CIMINELLI, MICHAEL LAIPPLE, and KEVIN SCHULER, the defendants, that was seeking State development grants for projects in Buffalo, New York. In exchange for the bribe payments to Howe, Howe worked with KALOYEROS to deceive Fort Schuyler by secretly tailoring the required qualifications for those development deals so that the Syracuse Developer and the Buffalo Developer would be awarded the contracts, in Syracuse and Buffalo respectively, without any meaningful competition.

II. RELEVANT INDIVIDUALS AND ENTITIES

A. New York State Government and the Office of the Governor

23. According to public sources and information provided by the Governor's Office, I know the following: 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." The Executive Chamber includes the following officials, among others: Executive Deputy Secretary, which is the position that was held by JOSEPH PERCOCO, a/k/a "Herb," the defendant, as described below; Secretary to the Governor; and Director of State Operations. The Secretary to the Governor is in charge of the Executive Chamber's overall management. The Director of State Operations oversees the day-to-day functioning of State government, including overseeing and providing direction to many of the State agencies. Within the Executive Chamber there are also various Deputy and Assistant Secretaries organized by subject area, who are the primary liaisons with their respective State agencies, and report up to the Director of State Operations.

24. I know from publicly available federal and State government documents and public reports that, in each year relevant to this Complaint, the government of the State received funds from the federal government in excess of $10,000 per year.

B. *CNSE and Fort Schuyler*

25. Based on public information and interviews with, among others, individuals associated with the College of Nanoscale Science and Engineering ("CNSE") and its affiliated entities, I learned the following:

a. CNSE is a public institution of higher education that is 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"), of which CNSE is now a part. Because CNSE became part of SUNY Poly during the time period relevant to this Complaint, unless otherwise specified, I refer to both CNSE and SUNY Poly as "CNSE" in this Complaint. SUNY Poly is part of the State University of New York, which is a public, State-supported organization.

b. The head of CNSE and SUNY Poly at all times relevant to this Complaint was ALAIN KALOYEROS, a/k/a "Dr. K," the defendant. Under his leadership, CNSE, and later SUNY Poly, focused on developing partnerships with private companies to create large development and construction projects. When the Governor's Buffalo Billion initiative was announced in 2012, CNSE created projects in

Buffalo and Syracuse, New York, in order to take advantage of new State funds committed to development in upstate New York.

c. In or around 2009, CNSE created Fort Schuyler as an affiliated non-profit real estate corporation to partner with private companies on CNSE's behalf to carry out its development projects. As relevant here, Fort Schuyler manages development and construction projects associated with CNSE in Buffalo and Syracuse, New York. Fort Schuyler is governed by a Board of Directors, which, among other things, is charged with selecting private companies to partner with Fort Schuyler in CNSE-related development projects, including Buffalo Billion-related projects in Buffalo and similar development projects in Syracuse, among other places. Certain public funding for CNSE goes through the Research Foundation for the State University of New York (the "Research Foundation"), which employed many individuals associated with CNSE and Fort Schuyler, including ALAIN KALOYEROS, a/k/a "Dr. K," the defendant, and Howe (as a retained consultant), during the times relevant to this Complaint. During each year relevant to this Complaint, the Research Foundation received more than $10,000 in federal funding.

C. *JOSEPH PERCOCO*

26. Based on my review of documents both publicly available and obtained during this investigation, including electronic communications to and from JOSEPH PERCOCO, a/k/a "Herb," the defendant, and my interviews with Howe as well as several individuals who worked at the Governor's Office at the relevant times, I learned that:

a. In or around 1992, PERCOCO joined the Office of the then-Governor of New York (the "Former Governor") as an intern. PERCOCO later worked for the current Governor (the son of the Former Governor) when the Governor was Attorney General. In or about January 2011, PERCOCO was appointed to be the Executive Deputy Secretary to the Governor, and remained one of the Governor's closest advisors during the Governor's first and second terms. The position of Executive Deputy Secretary is a high-ranking, senior, and influential part of the Governor's Executive staff. PERCOCO 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's role included serving as a primary "gatekeeper" of opportunities to speak or meet with the Governor,

overseeing logistics of the Governor's events and travel, supervising appointments and administrative matters for the Executive Chamber, and playing the principal role in organizing support for the Governor's initiatives among lawmakers, labor leaders, and other constituencies. During all times relevant to this Complaint, 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 his official duties. PERCOCO also maintained a very close, personal relationship with the Governor and the Former Governor, exhibited by the Governor's public reference to PERCOCO as the Former Governor's "third son."

b. On or about April 21, 2014, PERCOCO officially left New York State employment to serve as campaign manager for the Governor's reelection campaign, and returned to State service on or about December 8, 2014. PERCOCO permanently left his position as Executive Deputy Secretary in or about January 2016, and is currently an executive in the private sector.

c. According to multiple witnesses interviewed in this investigation, as well as PERCOCO's email communications at the relevant time, although PERCOCO was not on the State payroll between at least on or about April 22, 2014 and December 7, 2014, while he was the manager of the Governor's reelection campaign, PERCOCO nevertheless continued to function in a senior advisory and supervisory role with regard to the Governor's Office during that time period, and continued to be involved in the hiring of staff and the coordination of the Governor's official events and priorities, among other things, and to travel with the Governor on official business. In addition, PERCOCO represented to others that he intended to return to State service, including by stating on a mortgage application submitted on or about August 7, 2014, that he was "guaranteed a position with [the Governor] after the November election."

D. *ALAIN KALOYEROS*

27. I have learned from emails, financial records, publicly available information, and witness interviews, including interviews with Howe and executives of CNSE and its affiliated entities, that:

a. ALAIN KALOYEROS, a/k/a "Dr. K," the defendant, currently serves as the President of SUNY Poly. Prior to CNSE's merger into SUNY Poly, KALOYEROS served as Senior Vice President and Chief Executive Officer of CNSE.

b. At all relevant times, KALOYEROS served as a member of the Board of Directors of Fort Schuyler. Fort Schuyler's officers also were hired by KALOYEROS and relied on staffing from the Research Foundation, and KALOYEROS supervised and controlled Fort Schuyler's day-to-day operations.

E. *Todd Howe*

28. I know from witness interviews, including interviews with Howe, and the review of emails, financial records and publicly available information that:

a. Howe has held several public positions, including as a strategic advisor to the Governor when the Governor was United States Secretary of Housing and Urban Development, and as a senior aide to the Former Governor when the Former Governor was Governor of New York. I also know that Howe has known JOSEPH PERCOCO, a/k/a "Herb," the defendant, since PERCOCO was a college student, when Howe hired PERCOCO to work for the Former Governor.

b. During all times relevant to this Complaint, Howe was the president and primary employee of a government relations and lobbying firm (the "Government Relations Firm") located in Washington, DC, that was a subsidiary of a law firm located in Albany, New York (the "Law Firm"). The co-chair of the Law Firm controlled the finances of the Government Relations Firm, including Howe's salary and bonuses, and approved all retention agreements for new clients of the Government Relations Firm. Also during all times relevant to this Complaint, Howe was retained by several clients, most, if not all, of which retained Howe for his contacts with State officials, and for which Howe provided assistance with obtaining or facilitating business before the State. Howe's clients included the Energy Company, the Syracuse Developer, and the Buffalo Developer.

c. During all times relevant to this Complaint, Howe was also retained as a consultant to CNSE. In his role as a consultant for CNSE, Howe maintained an office and parking space at CNSE, served

as a close advisor to ALAIN KALOYEROS, a/k/a "Dr. K," the defendant, acted as an agent of CNSE with respect to, among other things, CNSE's development projects, including large, state-funded development projects in Syracuse and Buffalo, New York, and served as CNSE's primary liaison to the Governor and the Governor's senior staff.

d. In or around June 2016, Howe began meeting with the Government and cooperating with the Government's investigation. In those meetings, Howe admitted to his role in the illegal schemes set forth herein as well as other crimes. In or about September 2016, Howe pleaded guilty pursuant to a cooperation agreement with the Government to several federal crimes, including conspiracies to commit honest services fraud, extortion under color of official right, bribery, and wire fraud, substantive extortion and wire fraud offenses, and tax fraud. The information provided by Howe has been corroborated by contemporaneous documents, including emails, and by the statements of other witnesses.

F. PETER GALBRAITH KELLY and the Energy Company

29. I have learned from my review of emails, financial records, publicly available information, and witness interviews, including interviews with Howe and with employees of the Energy Company, that:

a. The Energy Company is a privately-owned electric power generation development and asset management company that, according to its website, focuses on a clean energy strategy utilizing natural gas and wind-powered generation. Since in or about 2008, the Energy Company has been working to develop a $900 million power plant (the "Power Plant") in Wawayanda, New York, currently under construction. As set forth in more detail below, the development process for the Power Plant involved numerous State approvals.

b. Since in or about 2008, PETER GALBRAITH KELLY, JR., a/k/a "Braith," the defendant, has been the Senior Vice President of External Affairs at the Energy Company. In that role, which he continues to hold, he oversees public relations and governmental affairs for the Energy Company, in particular as it relates to the building of new power plants across the United States.

G. STEVEN AIELLO, JOSEPH GERARDI, and the Syracuse Developer

30. I have learned from emails, financial records, publicly available information, and witness interviews, including interviews with Howe, that:

a. The Syracuse Developer is a large real estate development firm located in Syracuse, New York that, through various corporate affiliates, builds, owns, and manages real estate in and around New York State. Prior to 2013, the Syracuse Developer's business focused primarily on private development opportunities, including strip malls and supermarkets. Beginning in or about 2013, the Syracuse Developer began obtaining a significant portion of its business from State-funded construction contracts. Specifically, in or around December 2013, the Syracuse Developer was awarded a contract with Fort Schuyler to serve as the preferred developer for projects of CNSE to be created in Syracuse, New York. This award permitted the Syracuse Developer to be chosen for CNSE 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 in Syracuse, New York, associated with CNSE, and in or around October 2015, the Syracuse Developer received a contract worth approximately $90 million to build a manufacturing plant in Syracuse, New York, associated with CNSE.

b. STEVEN AIELLO, the defendant, is a founder of the Syracuse Developer and has been its President since in or about 1998. Among other responsibilities, AIELLO serves as the company's general manager, focusing on business development, negotiating real estate contracts and handling tenant negotiations.

c. JOSEPH GERARDI, the defendant, is a founder of the Syracuse Developer and its General Counsel since in or about 1998. Among other responsibilities, GERARDI is responsible for, among other things, public permitting and negotiating company contracts.

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

31. I have learned from emails, financial records, publicly available information, and witness interviews, including interviews with Howe, that:

a. The Buffalo Developer is a large Buffalo-based construction and development company that provides, among other things, construction management and general contracting services. As relevant to this Complaint, in or around January 2014, the Buffalo Developer was named by Fort Schuyler as a preferred developer for projects of CNSE to be created in Buffalo, New York. This award permitted the Buffalo Developer to be chosen for CNSE 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, associated with CNSE. That contract ultimately expanded to be worth approximately $750 million.

b. LOUIS CIMINELLI, the defendant, is the Chairman and CEO of the Buffalo Developer, and served in that role at all times relevant to this Complaint. In that role, CIMINELLI directs the Buffalo Developer's long-term strategy and develops strategic partnerships in the State and elsewhere.

c. MICHAEL LAIPPLE, the defendant, is the President of a division of the Buffalo Developer that focuses, among other things, on initiatives involving public-private infrastructure projects, and served in that role at all times relevant to this Complaint. In this role, LAIPPLE works on, among other things, developing partnerships between the Buffalo Developer and public entities for large-scale developments.

d. KEVIN SCHULER, the defendant, is a Senior Vice President for the Buffalo Developer, and served in that role at all times relevant to this Complaint. SCHULER is responsible for, among other things, the Buffalo Developer's external communications, government affairs, and community and media relations.

III. THE PERCOCO BRIBERY SCHEME

A. *The Energy Company Paid Bribes to PERCOCO in Exchange for Official Actions by PERCOCO*

32. As set forth in detail below, based on my review of emails, documents obtained in course of this investigation, and financial records, and interviews with, among others, Howe and current and former State employees and employees of the Energy Company, I believe that JOSEPH PERCOCO, a/k/a "Herb," and PETER GALBRAITH KELLY, JR., a/k/a "Braith," the defendants, and Howe engaged in a multi-year bribery scheme whereby KELLY caused the Energy Company to make secret payments to PERCOCO through PERCOCO's wife in exchange for PERCOCO's official assistance to the Energy Company. The evidence shows that: (a) State action was critical to the Energy Company's business; (b) starting as early as 2010, KELLY provided personal benefits to PERCOCO in an effort to cultivate access to PERCOCO; (c) in response to KELLY's requests for official assistance, PERCOCO requested that the Energy Company hire his wife; (d) in or around the end of 2012, KELLY caused the Energy Company to create a position for PERCOCO's wife; and (e) in exchange for various personal benefits from KELLY as well as payments of approximately $90,000 per year ($7,500 per month) from the Energy Company to PERCOCO and his wife, PERCOCO agreed to use his official position and influence, and did in fact use his official position and influence, to help the Energy Company with specific State matters as the opportunities arose. Among other things, PERCOCO agreed to use his official position and influence to assist the Energy Company's efforts to obtain (i) a valuable agreement from the State allowing the Energy Company to buy lower-cost emissions credits in New York for a power plant proposed to be built in New Jersey (the "Reciprocity Agreement") and (ii) a lucrative long-term power purchase agreement with the State guaranteeing a buyer for the power to be produced at a power plant proposed to be built in New York (the "PPA").

33. Furthermore, as explained in detail below, based on my review of emails, documents obtained in course of this investigation, and financial records and interviews of, among others, Howe and current and former State employees, I believe that JOSEPH PERCOCO, a/k/a "Herb," the defendant, and Howe continued to extort monetary payments from PETER GALBRAITH KELLY, JR., a/k/a "Braith," the defendant, and the Energy Company even after it became clear to PERCOCO and Howe in or around the end of 2013 that the State would not award

a PPA to the Energy Company. PERCOCO and Howe did not inform KELLY that they understood from State officials that the Energy Company would not be receiving a PPA. To the contrary, PERCOCO continued to promise official actions and influence related to the PPA in order to ensure that KELLY and the Energy Company continued to employ and pay PERCOCO's wife.

i. State Action Was Critical to the Energy Company

34. Based on my review of emails, Energy Company documents, and public information, I learned that the Energy Company's business has depended significantly on its success in obtaining State regulatory approvals, contracts, and agreements. For example, the Energy Company's Power Plant project, budgeted to cost approximately $900 million, required numerous State regulatory approvals, including from the Department of Public Service ("DPS"), Department of Environmental Conservation ("DEC") and Department of Transportation ("DOT"). Beginning at least in or about mid-2010, the Energy Company was seeking to obtain a PPA, under which the State would purchase virtually all power produced by the Power Plant for up to 15 years, guaranteeing a significant and long-term stream of income for the Power Plant. Based on internal Energy Company projections, obtaining a PPA was worth at least approximately $100 million to the Energy Company, and would significantly assist the Energy Company in obtaining financing for the project. In or around 2012, the Energy Company began actively seeking to apply for and obtain a PPA offered through DPS and the New York Power Authority ("NYPA").

35. Based on my review of emails, Energy Company documents, and public information, and on interviews with, among others, Howe and employees of the Energy Company, I learned the following:

a. As of mid-2010, the Energy Company had retained the Law Firm and Howe to provide consulting advice with respect to regulatory approvals related to the Energy Company's Power Plant project. Pursuant to its arrangement with Howe, the Energy Company made regular payments to the Law Firm, a portion of which were paid to Howe through the Government Relations Firm, the D.C.-based lobbying firm associated with the Albany Law Firm. In or about that time, however, PETER GALBRAITH KELLY, JR., a/k/a "Braith," the defendant, sought to have the Energy Company make additional payments directly to Howe. Howe understood, based on his conversations with KELLY, that KELLY wanted to make additional payments to Howe in order to increase

KELLY's access to the Governor (who was expected to be elected in the coming months) and certain of the Governor's advisors, including JOSEPH PERCOCO, a/k/a "Herb," the defendant, in order to secure a PPA for the Energy Company. In consultation with KELLY, Howe set up a limited liability company ("Howe's LLC") that had no business purpose other than to conceal the source and receipt of payments made to or through Howe. Howe then used his LLC to conceal from his principal employer, the Government Relations Firm, additional payments made to Howe from the Energy Company.

b. Between August 2010 and April 2015, the Energy Company paid Howe's LLC approximately $474,000. Because Howe accepted these payments outside of his employment agreement with the Government Relations Firm, KELLY agreed with Howe not to tell anyone at the Government Relations Firm or the Law Firm about the additional payments to Howe's LLC. During that same period, the Energy Company paid the Government Relations Firm approximately $332,062.

36. Based on my review of emails, Energy Company documents, and public information, and on interviews with, among others, Howe, State officials, and employees of the Energy Company, I learned that PETER GALBRAITH KELLY, JR., a/k/a "Braith," the defendant, understood that JOSEPH PERCOCO, a/k/a "Herb," the defendant, and an individual who worked closely with PERCOCO in the Executive Chamber from 2011 through in or around June 2014, in the position of State Operations Director (referred to herein as the "Former State Operations Director"), had the ability to influence the development of the Power Plant given their senior roles with respect to the Governor, and their respective roles overseeing State operations and the functioning of key agencies such as DEC, DOT, DPS and NYPA, and liaising with labor unions. Ultimately, and as set out in greater detail below, KELLY sought to have PERCOCO use his official position and influence with respect to at least the following State decisions and actions:

a. As early as 2010, Howe began to seek PERCOCO's assistance in influencing the Former State Operations Director with respect to the Power Plant, most specifically by asking PERCOCO to advise the Former State Operations Director that the Power Plant was supported by labor unions and to advocate for the closing of a nuclear power plant located in Westchester County, New York (the "Nuclear Power Plant"). Based on my review of publicly available documents and my interviews of witnesses, including employees of the Energy Company, the importance of the Power Plant to the State depended,

at least in part, on whether the Nuclear Power Plant was going to be shut down.

b. Beginning in or about 2011, after the Governor's election, KELLY sought information and assistance regarding the process through which the Energy Company could apply for a long-term PPA, something the Energy Company believed would be of great economic benefit because it would guarantee a steady and significant stream of income for the Power Plant and assist the Energy Company in securing financing to build the Power Plant.

c. In or about early 2012, the Governor announced in his State of the State address the creation of an "Energy Highway Initiative," which included the appointment of an interagency task force to focus on increasing New York's energy generation and transmission capacity. In connection with this initiative, in or about April 2012, NYPA issued a request for information (the "Energy RFI"), seeking information on potential energy generation projects. On or about May 30, 2012, the Energy Company submitted a response to the Energy RFI, highlighting its efforts to build the Power Plant.

d. In or about April 2013, NYPA issued a request for proposals for energy transmission projects and for the construction of new power plants. NYPA further offered a PPA to any selected new power plant. On or about May 20, 2013, the Energy Company filed its response seeking the PPA.

e. In or around August 2013, the Energy Company sought a valuable agreement between a New Jersey state agency and the New York State DEC (the "Reciprocity Agreement") which would allow the Energy Company to purchase emissions credits -- which are required to offset certain types of pollution created by power plants -- in New York in connection with a power plant being built by the Energy Company in New Jersey. The absence of a Reciprocity Agreement would have made it difficult, if not impossible, for the Energy Company to construct the New Jersey power plant.

ii. KELLY Began Providing Personal Benefits to PERCOCO

37. Based on my review of emails between and among PETER GALBRAITH KELLY, JR., a/k/a "Braith," and JOSEPH PERCOCO, a/k/a "Herb," the defendants, and Howe, and Energy Company expense records, I know that KELLY began to offer and provide certain benefits to JOSEPH

PERCOCO, a/k/a "Herb," the defendant, in late 2010 and 2011, in an effort to ingratiate himself to PERCOCO. Examples of these interactions include the following:

a. In or around August 2010, KELLY took PERCOCO, Howe and others on a weekend fishing trip in Montauk, New York, paid for by the Energy Company. In connection with the trip, KELLY submitted a reimbursement request for approximately $2,748 in "business development" expenses connected to the Power Plant, which did not reflect that PERCOCO was on the fishing trip.

b. On or about October 27, 2010, KELLY arranged, at PERCOCO's request, for the Energy Company to donate a private jet to transport the Governor and his staff to campaign events later that same week.

c. KELLY took PERCOCO and Howe to a $279 lunch at a steak restaurant in Manhattan, on or about December 23, 2010, just a few days before the Governor took office for the first time, and charged the meal to the Energy Company, under a billing code for the Power Plant.

d. On or about February 4, 2011, KELLY invited PERCOCO fishing again and stated in an email, "just know whenever YOU need me I'm in."[1]

---

[1] To the extent emails to or from PERCOCO are referenced herein, the emails were sent to or from PERCOCO's personal email address, and not his New York State email address, and, as is true with all documents referenced herein, were obtained pursuant to judicially authorized search warrants, in response to grand jury subpoenas to third parties, or through voluntary disclosures from third parties. Based on my review of policies and advisory opinions issued by the State Office of Information Technology Services and State Committee on Open Government, I learned that State employees are not to use personal email addresses to conduct State business unless explicitly authorized, and that emails received or sent by a State official in his or her capacity as an official are records subject to disclosure pursuant to the New York Freedom of Information Law regardless of whether those emails are sent or received from an official or personal

38. Based on emails and interviews with, among others, Howe, I know that, by at least the spring of 2011, PETER GALBRAITH KELLY, JR., a/k/a "Braith," the defendant, was actively seeking the assistance of JOSEPH PERCOCO, a/k/a "Herb," the defendant, with obtaining State support for the development of the Power Plant, and PERCOCO began to use his influence to assist the development of the Power Plant.

a. On or about May 16, 2011, Howe reported to KELLY that PERCOCO is "all over" the Power Plant project and wanted to set up a meeting with the Former State Operations Director to discuss the project. Howe further reported to KELLY that there was "No opinion yet . . . JP doing something with this though." KELLY responded, "I got an email from Joe as well saying just that." Based on my conversations with Howe, I understand that the "opinion" referred to in this email is the opinion of senior members of the Governor's staff, including the Former State Operations Director, with respect to supporting the development of the Power Plant.

b. On or about June 5, 2011, the Former State Operations Director sent an email from his personal email address to Howe that stated that the "project" -- *i.e.*, the development of the Power Plant -- faced a lot of challenges, including the need for a PPA, low energy prices given a "supply glut in NY State," and stiff competition from other potential projects. That same day, Howe wrote to PERCOCO that he had spoken to the Former State Operations Director regarding the Energy Company and that the Former State Operations Director was "good but need u now."

c. On or about June 7, 2011, Howe advised KELLY by email that Howe had arranged a meeting for KELLY with the Former State Operations Director on or about June 9, 2011. In an email on the same day as the meeting, June 9, 2011, Howe stated to PERCOCO: "Herb, do the right thing with Braith..this goes south herb, you will have to

---

email address. Nonetheless, I am aware of media reports of State employees using personal email addresses to avoid disclosure of records under the New York Freedom of Information Law.

clean out the 'herb cave' downstairs at the estate as I'll have to move in!!!"[2] I understand that, in this email, Howe is reminding PERCOCO what a financially important client the Energy Company was to Howe. PERCOCO responded, "U got it herb. Thx."

d. On the day of the meeting, on or about June 9, 2011, Howe instructed KELLY to "go see Percoco after [Former State Operations Director] meeting [. . .] Wait if necessary." KELLY replied, "I'll sleep in the streets of NYC waiting for JP if I need to." Howe has explained that "JP" is PERCOCO.

iii. PERCOCO Sought to Have His Wife Hired by the Energy Company

39. As set forth above, in or around May 2012, the Energy Company responded to the Energy RFI with a submission that sought to convince State officials of the Power Plant's importance to energy generation in the State. Based on emails and financial records of JOSEPH PERCOCO, a/k/a "Herb," the defendant, and my conversations with Howe, I know that at or around the same time, PERCOCO was facing significant financial difficulties and was struggling to pay his bills. In or about July 2012, PERCOCO and his wife purchased a home in Westchester County, New York, for approximately $800,000. In or about September 2012, PERCOCO's wife took a one-year unpaid leave of absence from her job as a public school teacher in a New York City school, which she resigned from the following year. Based on my review of financial analysis conducted by the FBI, which reviewed financial records pertaining to the PERCOCOs, I learned that after PERCOCO's wife left her job in September 2012, the PERCOCOs' average monthly income decreased from approximately $12,714 to approximately $8,594. At that time, their monthly expenses, which totaled at least approximately $20,000 per month, far exceeded their income, and their

---

[2] Based on my review of emails in this investigation, and the interview of witnesses, including Howe, I learned that "Herb" is a name PERCOCO, Howe, the Former State Operations Director, and at least one other government official have used as a term of endearment to refer to each other since in or around the time that the Former Governor was in office. Separately, I also learned that Howe and others often referred to KELLY as "Braith," short for KELLY's middle name, GALBRAITH.

savings was close to being depleted. Between in or about May and October 2012, PERCOCO attempted -- unsuccessfully -- to assist his wife in obtaining a substitute teaching job near their new home in Westchester County.

40. Based on my review of emails and my discussion with Howe, I learned that in the spring of 2012 -- at or around the same time the Energy Company submitted its response to the Energy RFI -- JOSEPH PERCOCO, a/k/a "Herb," the defendant, asked PETER GALBRAITH KELLY, JR., a/k/a "Braith," the defendant, to have the Energy Company hire his (PERCOCO's) wife. Indeed, according to Howe, from in or about the spring of 2012 until in or about November 2012, PERCOCO continually pressured Howe and KELLY to provide PERCOCO's wife a job with the Energy Company. My review of emails during this time period confirms and corroborates the pressure brought to bear by PERCOCO. For example:

a. On or about May 31, 2012, after KELLY sought "feedback" from Howe on the Energy Company's proposed response to the Energy RFI, Howe wrote to KELLY, "Spoke to Joe. He's calling you possibly tomorrow on wife issue." Howe further noted, in the same email, that he had spoken to the Former State Operations Director, who "said 87 [Energy RFI responses] came in." I know from publicly available information that the State received approximately 85 responses to the Energy RFI, including the response from the Energy Company.

b. On or about September 11, 2012, PERCOCO wrote an email to Howe stating, "Herb: Nail down that issue. Happy to have dinner or meet with you guys anytime! Thanks." According to Howe, "nail down that issue," referred to finding a job for PERCOCO's wife. Howe forwarded the email to KELLY, and stated: "Braith need to talk."

c. On or about September 18, 2012, Howe wrote an email to KELLY suggesting a dinner for Howe, "jp," (*i.e.*, PERCOCO) and KELLY the following week. In the same email chain, Howe suggested KELLY and Howe talk the next day, "Need to try and hammer something out for jp. Wants you and I to try and identify something he wants to try and stay removed if possible if u know what I mean." Howe understood that PERCOCO wanted to "stay removed" because it was improper for PERCOCO to be asking KELLY for a job for his wife given the work PERCOCO had done and was doing to advocate for the Power

Plant. Howe further understood that PERCOCO did not want others to know that he was asking the Energy Company for a job for his wife.

d. Based on my review of emails, KELLY's business expense records and cellular phone records noting the location of calls made by Howe and PERCOCO, and discussions with Howe, I learned that, on or about September 26, 2012, PERCOCO, KELLY, and Howe had dinner at a restaurant in Danbury, Connecticut. According to Howe, during dinner, PERCOCO, KELLY and Howe discussed, among other things, the Energy Company hiring PERCOCO's wife and the Energy Company obtaining a PPA. KELLY agreed at this dinner that he would work on finding a job at the Energy Company for PERCOCO's wife. KELLY charged this dinner, which cost approximately $386.00, to the Energy Company's budget for the Power Plant, according to a reimbursement request from KELLY that was approved by the Energy Company. The reimbursement request further noted that the meal was with Howe, but made no reference to PERCOCO.

41. Based on my interview of the then-President of the Energy Company ("Executive-1"), I learned that, in or about October 2012, PETER GALBRAITH KELLY, JR., a/k/a "Braith," the defendant, met with Executive-1 and the then-CEO of the Energy Company to advise them that KELLY wanted to hire the wife of JOSEPH PERCOCO, a/k/a "Herb," the defendant, to work on a community education project that KELLY was planning to develop. Executive-1 and the then-CEO expressed concern about hiring the wife of a senior member of the Governor's staff while the Energy Company was seeking extensive regulatory review of its Power Plant before State agencies, and directed KELLY to obtain an ethics opinion or approval from the Governor's Office before proceeding. KELLY later advised them that he had obtained, in sum and substance, an ethics opinion from the Governor's Office approving the Energy Company's hiring of PERCOCO's wife. Based on my review of documents provided by the Governor's Office and the Energy Company, and interviews of Executive-1 and attorneys for the Executive Chamber, I learned that no such ethics opinion was ever provided to the Energy Company and there is no evidence to suggest that one was ever sought or prepared.

42. Emails in or around the fall of 2012 reflect continued pressure by JOSEPH PERCOCO, a/k/a "Herb," the defendant, to finalize the hiring of his wife by the Energy Company. For example, on or about November 12, 2012, PERCOCO wrote to Howe stating, "Herb: need to pull the trigger here. things getting bad. What do you think about this

Thursday at my house?" Howe has explained that he understood "things getting bad" to refer to PERCOCO's financial situation at the time.

a. In a follow-up email, Howe confirmed, "Fat boy locked and loaded.. 7Thursday night at the estate." PERCOCO replied, "is he bringing the check?? LOL." Based on my interviews of Howe and my review of emails in this investigation, I know that Howe and PERCOCO often referred to KELLY as "Fat Man," or "Fat Boy." Howe later wrote, "herb -- need 7500 boxes of zitti!!" PERCOCO responded, "yes 7500/month is her old salary."[3]

b. Howe has explained that "zitti" or "ziti" was a code word he and PERCOCO used for money, which PERCOCO came up with based on the use of the term in the television show "The Sopranos."

iv. KELLY Caused the Energy Company to Make Payments to PERCOCO's Wife

43. As set forth herein, I believe, based on emails, documents obtained in the course of this investigation, financial records, and interviews with, among others, Howe and employees of the Energy Company, that in or about November 2012, JOSEPH PERCOCO, a/k/a "Herb," and PETER GALBRAITH KELLY, JR., a/k/a "Braith," the defendants, reached an agreement under which the Energy Company would employ and make payments to PERCOCO's wife and, in exchange, PERCOCO agreed to use, and did in fact use, his official position and influence to assist the Energy Company with State actions as opportunities arose. To carry out his end of this agreement, KELLY (a) caused the Energy Company to create a previously non-existent job for PERCOCO's wife; (b) ran payments to the PERCOCOs of approximately $7,500 per month through a consultant who worked for the Energy Company ("Consultant-1") in order to disguise the source of the payments, and also took additional steps to conceal PERCOCO's wife's employment at the Energy Company; (c) paid PERCOCO's wife a much higher salary than warranted by her limited work; and (d) falsely told his superiors at the Energy Company (on two occasions) that PERCOCO had obtained an ethics opinion from the Governor's Office approving of PERCOCO's

---

3 Based on my review of Department of Education records, PERCOCO's wife annual salary during the 2011-2012 school year was approximately $75,796.

wife's employment with the Energy Company. Moreover, when recently questioned by federal agents about his arrangement with PERCOCO, KELLY made false statements about the purpose of making payments through Consultant-1 in an apparent effort to conceal the criminal nature of his conduct. For his part, PERCOCO further concealed the criminal scheme by failing to include the Energy Company as the source of payments on his State-mandated financial disclosure forms.

44. Evidence of the nature of the job created for the wife of JOSEPH PERCOCO, a/k/a "Herb," the defendant, and of the efforts of PETER GALBRAITH KELLY, JR., a/k/a "Braith," the defendant, and PERCOCO to conceal the payments made by the Energy Company includes the following:

a. Based on my review of emails, documents obtained in the course of this investigation, financial records, and interviews with, among others, Howe and employees of the Energy Company, I know that, in or around fall 2012, after KELLY learned that PERCOCO wanted to find a job for his wife, KELLY and others he supervised began developing an education program targeted at fourth grade students located in and around a power plant the Energy Company was building in New Jersey (the "Education Program"). Based on an interview of Executive-1, I learned that this was the first time the Energy Company developed an education program for elementary school students in connection with the development of one of its power plants, and that Executive-1 was not aware of any particular issue, either during mid to late 2012 or at or around the New Jersey location, that necessitated such a program.

b. Based on my review of financial records and interviews with employees of the Energy Company, I know that the Energy Company began making monthly payments of approximately $7,500 to the wife of PERCOCO on or about December 18, 2012. On or about December 6, 2012, Howe advised PERCOCO that the payments would begin shortly: "Herb. with bk in dc. Ziti gets cleared on 15 th When all the boxes are signed arrives in ur mailbox 2 or 3 days later." Howe has explained that "bk" refers to KELLY.

c. Based on my review of emails, documents obtained in the course of this investigation, financial records, and interviews with, among others, Howe, and employees of the Energy Company, I

believe that PERCOCO and KELLY deliberately tried to conceal the fact that the Energy Company was the source of these payments, as follows:

i. Throughout PERCOCO's wife's tenure with the Education Program, the Energy Company used Consultant-1 as a pass-through for its monthly payments to PERCOCO's wife. Between December 2012 and January 2016, PERCOCO's wife received a monthly check of approximately $7,500 from Consultant-1. During each of these months, shortly before each payment to PERCOCO's wife, Consultant-1 received a payment from the Energy Company to cover the amount to be paid to PERCOCO's wife.

ii. Based on interviews with Consultant-1 and other employees of the Energy Company, I learned that Consultant-1 did not hire or supervise PERCOCO's wife. Consultant-1 stated that, in or about fall 2012, he was told by KELLY that payments to PERCOCO's wife would be made through Consultant-1. KELLY provided two reasons for this payment structure: (i) it purportedly was more convenient for billing purposes; and (ii) there would be negative "optics" of hiring the wife of a senior official in State government while the Energy Company had business before the State.

iii. Based on an interview with an external affairs manager at the Energy Company (the "External Affairs Manager"), who has worked for KELLY since in or about 2010, I learned that, based on conversations the External Affairs Manager had with KELLY and others in the External Affairs team, the External Affairs Manager purposefully kept PERCOCO's wife's last name out of brochures for the Education Program, directed PERCOCO's wife to refer to herself by her first name when in classrooms, and purposefully kept PERCOCO's wife out of any pictures used to promote the program.

d. Based on my review of emails and interviews with employees of the Energy Company, I believe that the hours worked by PERCOCO's wife did not come close to justifying the $7,500 per month salary she was receiving. Between in or around December 2012 and April 2014, during which time the Education Program was being developed, PERCOCO's wife worked no more than 15 hours per month assisting with the development of the curriculum and participating in calls. Once PERCOCO's wife began teaching in classrooms in or around April 2014, she worked approximately 16 to 25 hours per month during the school year, primarily teaching partial-day courses to fourth graders once

or occasionally twice per week. During the summer, when school was not in session, PERCOCO's wife worked approximately ten hours per month, and sometimes as little as two to three hours per month, on special projects assigned by the External Affairs Manager. PERCOCO's wife was paid $7,500 per month regardless of the number of hours she worked, and was paid approximately three and a half times more than another employee at the Education Program, who worked more hours per week.

e. Based on my review of Energy Company documents and interviews of three Energy Company executives, including Executive-1, I learned that, in or around June and July 2014, KELLY, for the second time, falsely claimed to have an ethics opinion authorizing the Energy Company's hiring of PERCOCO's wife. This false representation was made in response to questions raised by two executives of the Energy Company after they noticed a substantial invoice from Consultant-1 in or around June 2014. On or about July 2, 2014, in a meeting with those executives and the then-CEO of the Energy Company, KELLY stated, in sum and substance, that PERCOCO's wife was being paid through Consultant-1 but her name could not appear on Consultant-1's invoices because of who she was, *i.e.*, the wife of a high-level State official. In the same meeting, KELLY stated -- falsely -- that there was an ethics opinion from the Governor's Office approving the arrangement, and that he had seen such opinion, but he did not have a copy. KELLY further (falsely) stated that lawyers had reviewed the arrangement and there was "nothing illegal about it." Although KELLY was asked to provide additional information about the purported approvals from the Governor's Office after the meeting, KELLY never did so.

f. KELLY was voluntarily interviewed by federal law enforcement agents in or around April 2016, prior to any public reports of the investigation in this matter. During that interview, KELLY admitted, in part and in substance, that Consultant-1 acted as a pass-through for the payments from the Energy Company to PERCOCO's wife but also falsely claimed that the arrangement was strictly for administrative ease.

v. PERCOCO Failed to Disclose Payments from the Energy Company

45. Pursuant to the New York State Public Officers Law, certain employees of the Executive Chamber, including, during his State employment, JOSEPH PERCOCO, a/k/a "Herb," the defendant, are required

to file financial disclosure statements on an annual basis with the New York State Joint Commission on Public Ethics. The financial disclosure statement is entitled "Annual Statement of Financial Disclosure" (the "Disclosure Form") and is required to be signed and presented for filing by the reporting individual. A primary purpose of the Disclosure Form is to require high-ranking public officials to disclose outside income, activities, finances, and assets that may indicate a financial impropriety or conflict of interest.

a. At all times relevant to this Complaint, the Disclosure Form required reporting individuals, among other things, to list "completely" the "nature and amount of any income in EXCESS of $1,000 from EACH SOURCE for the reporting individual and such individual's spouse." (Emphasis in original.)

b. In his required filings 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. As set forth herein, however, the representations made with respect to his wife were false and misleading because, in truth and in fact, and as PERCOCO well knew, PERCOCO's wife did not work for Consultant-1, but rather was employed by the Energy Company, which paid PERCOCO's wife through Consultant-1 at the direction of PETER GALBRAITH KELLY, JR., a/k/a "Braith," the defendant, in order to disguise the source of the payments.

vi. PERCOCO Agreed to Take Official Action for the Energy Company

46. As set forth in more detail below, based on my review of emails and interviews of individuals including Howe and various State employees and officials, I believe that in return for the secret monthly payments from the Energy Company to his wife, JOSEPH PERCOCO, a/k/a "Herb," the defendant, agreed to use, and did in fact use, his official position and influence to benefit the Energy Company and advance its interests as the need arose. PERCOCO was effectively "on call" for PETER GALBRAITH KELLY, JR., a/k/a "Braith," the defendant, whenever KELLY required help for the Energy Company before the Executive Chamber or State agencies. More specifically, in return for the payments to his wife, PERCOCO agreed to take, and did in fact take, official actions related to two State issues that were critical to the Energy Company's business: the Reciprocity Agreement and the PPA.

vii. PERCOCO Helped the Energy Company Obtain the Reciprocity Agreement

47. Based on my review of emails and interviews of, among others, Howe and an official at the DEC (the "DEC Official"), I know that in or about August 2013, at the request of PETER GALBRAITH KELLY, JR., a/k/a "Braith," the defendant, JOSEPH PERCOCO, a/k/a "Herb," the defendant, agreed to use, and in fact did use, his official position and influence to help the Energy Company obtain the valuable Reciprocity Agreement described above, which allowed the Energy Company to purchase emission reduction credits ("ERCs") in New York in connection with the power plant it was building in New Jersey. Evidence of this agreement includes the following:

a. On or about August 12, 2013, KELLY advised Howe that KELLY had been attempting to secure the Reciprocity Agreement from the DEC and a New Jersey state agency, and that the DEC Official "indicated that he could use a 'push from above' to get it done as a priority." I understand from reviewing Energy Company documents and interviewing an Energy Company employee that a certain number of ERCs were required before the New Jersey plant could become operational, and purchasing ERCs in New York was necessary at that time because there were a limited number available for sale in New Jersey and the cost of purchasing the ERCs in New Jersey was much higher than purchasing them in New York.

b. On or about August 14, 2013, PERCOCO responded to an email from Howe regarding the Reciprocity Agreement, stating that he (PERCOCO) would "check with" the Commissioner of DEC. Later in the same email chain, on or about August 24, 2013, PERCOCO responded to the same email chain and asked that the Former State Operations Director or another member of the Former State Operations Director's staff (the "Operations Deputy") "help [. . .] on this" because PERCOCO was dealing with a pressing personal situation. Approximately one hour later, the Former State Operations Director (who appears to have been blind copied on PERCOCO's email) agreed to assist.[4]

---

[4] The Former State Operations Director used his personal email in agreeing to take this action despite having a signature line that

c. Based on my review of emails and my interview of the Operations Deputy, I learned that the Operations Deputy instructed the DEC Commissioner to enter into the Reciprocity Agreement. Specifically, on or about Tuesday, August 27, 2013, the Operations Deputy, responding to the same email chain, which contained all of the emails set forth in the above paragraphs, wrote to Howe, copying PERCOCO, stating, "Spoke to [the DEC Commissioner]. They are moving forward and will get it done ASAP."[5]

d. Based on an interview of the DEC Official, I learned that the DEC Official received direction from the Governor's Office, via the DEC Commissioner's Office, to proceed with the Reciprocity Agreement. The DEC Official indicated that without instructions from the Governor's Office to enter into the Reciprocity Agreement, which I believe, based on the emails and interviews described above, came initially from PERCOCO, the DEC likely would not have entered into the Reciprocity Agreement.

48. Based on records obtained from the Energy Company and DEC, I learned that, in or around late 2014, the DEC and the New Jersey state agency signed the Reciprocity Agreement, which allowed the Energy Company to proceed with purchasing critical emission reduction credits in New York for its New Jersey power plant then in development, and resulted in significant savings to the Energy Company.

---

stated: "Important Note: Please direct any emails or questions regarding New York State official business to [the Former State Operations Director's New York State email address]. I will not reply to any emails dealing with state business on this account."

[5] Records obtained from the DEC indicate that just four days earlier, on or about of August 23, 2013, DEC had "not identified a material state interest to be served by the reciprocity agreement, other than interstate cooperation," and planned to confer with the Executive Chamber on whether to enter in to such an agreement.

viii. PERCOCO Took Official Action Regarding the PPA

49. Based on my review of emails, documents obtained in the course of this investigation, and interviews of, among others, Howe and State employees, I know that starting in or about September 2012, JOSEPH PERCOCO, a/k/a "Herb," the defendant, agreed to use, and did in fact use, his official position and influence to help the Energy Company obtain the PPA described above. While the PPA ultimately was not awarded to the Energy Company or to any other energy company in light of the State's energy needs, PERCOCO intervened and used his official authority in the Executive Chamber to exert pressure on behalf of the Energy Company in particular.

50. Based on publicly available information, I learned that on or about April 3, 2013, NYPA issued the Energy RFP, which, as set forth above, sought proposals for new power plants and offered a PPA to purchase all output for up to fifteen years from any selected new power plant. On or about May 20, 2013, the Energy Company filed its response to the Energy RFP, which, among other things, set forth its plans and progress to date to build the Power Plant.

51. In the fall of 2013 -- as the New York State Public Service Commission ("PSC"), which was in charge of making selections under the Energy RFP, was in the process of making certain decisions regarding the Energy RFP -- JOSEPH PERCOCO, a/k/a "Herb," the defendant, agreed to take and in fact took official actions to advocate for the Power Plant, as follows:

a. On or about September 18, 2013, Howe sent an email to PERCOCO which stated, in part, "When we talked last week, you asked that I send you a note on the 'fat man' project." As set forth above, Howe and PEROCCO sometimes referred to PETER GALBRAITH KELLY, JR., a/k/a "Braith," the defendant, as "fat man." The email continued: "They put up $14m, last week and are awaiting the results of the award. Word on the street is that the PSC Staff is recommending the starting up some old plants in the City, and not giving it to the [Energy Company] project. As you know Labor is all over the [Energy Company] project. Again Fat Man said there is some former [State Official] who is spearheading the starting up [of old plants . . . .] Can you talk to your folks and see what the story is?" PERCOCO responded, "I need that guys name asap!" and Howe replied with a name and employer. Howe understood PERCOCO's response to mean that he intended to work to

stop the reigniting of old coal-fired plants that would potentially compete with the construction of the Energy Company's Power Plant.

b. On or about October 8, 2013, Howe wrote in an email to PERCOCO, reporting, "Herb - spoke to [the NYPA President] this morning about 'operation fat man'. He says you need to get Herbert focussed [*sic*] so he calls a meeting with all involved to coordinate otherwise those psc folks will be off the reservation. Seems like [the NYPA President] feels it should be done soon as this issue goes public mid-week next week. Will let you handle as you know best how to move forward." PERCOCO responded, "ok. Thanks." In reference to this email, Howe explained that "Herbert" is the Former State Operations Director (who was part of the same group of friends, including Howe and PERCOCO, who called each other "Herb") and that Howe was asking PERCOCO to influence the Former State Operations Director to set up a meeting with NYPA, NYSERDA, and the PSC to encourage the issuance of a PPA to the Energy Company.[6]

c. Two days later, on or about October 10, 2013, Howe wrote an email to PERCOCO reflecting that the NYPA President, among other things, "said he wants to make sure ALL the options come to [the Former State Operations Director]." PERCOCO responded, "Ta[l]king to herbert about it today. Thanks." I know from the context of this email, my review of many other similar emails in this investigation, and my discussions with Howe, that "Herbert" in this email refers to the Former State Operations Director, and that PERCOCO was emphasizing that he was going to talk to the Former State

---

[6] Howe forwarded this chain to KELLY, with a note, "See below... all good" but in doing so, Howe changed "operation fat man" to "[Energy Company]" and also changed "ok. Thanks" to "Ok. on it now. thanks." Howe has acknowledged that he revised this email and certain others before forwarding, and explained that he did so in part to emphasize that PERCOCO was advocating for the Energy Company, as PERCOCO had promised to do. When I reference herein PERCOCO's email statements, I am relying unless otherwise noted on original emails provided by PERCOCO's personal email service provider in response to judicially-authorized search warrants, or other sources for which there is no indication of alteration.

Operations Director to try to steer him to favor the Energy Company's bid to obtain the PPA.

d. On or about October 14, 2013, the NYPA President, from his personal email address, informed Howe that the Governor's then-Assistant Secretary for Energy (the "Former Energy Assistant Secretary") was trying to set up a briefing with the Former State Operations Director, and suggested, "You might want to tell [the Former State Operations Director] to make time - at least an hour - for him to understand the entire picture including all pros and cons." Based on my review of emails and discussions with State employees, I know the proposed meeting was to discuss certain issues related to the Energy RFP, including PPAs.

i. Howe forwarded this email chain to PERCOCO, stating, "Herb-can you push on [the Former State Operations Director] . . . the fat man is sweating it!"

ii. PERCOCO replied, "He always sweats!! Ok will get to herbert!!" I know from the context of this email, my review of many other similar emails in this investigation, and my discussions with Howe, that "Herbert" in this email refers to the Former State Operations Director, and that PERCOCO was again telling Howe that he would intervene with the Former State Operations Director regarding the PPA for the Energy Company.

iii. Howe replied, "Good man Herb!!! Thanks, concerned as the PSC is supposed to hold a meeting on this Thursday, so [the NYPA President] believes something will come out about this. Hold [the Former State Operations Director]'s feet to the fire Herb . . . got to keep the ziti flowing Herb!" Howe has explained that, in the email chain, he was telling PERCOCO to influence the Former State Operations Director to help the Energy Company get the PPA, which PERCOCO agreed to do -- and that by doing so, PERCOCO would be able to keep the "ziti" (*i.e.*, the monthly payments from the Energy Company to PERCOCO's wife) "flowing."[7]

---

[7] When Howe sent this email chain to KELLY, Howe edited the NYPA President's email to take out "for him to understand the entire picture including all pros and cons"; modified Howe's email to PERCOCO to

ix. PERCOCO Extorted KELLY for More Money After Learning that the Energy Company Would Not Receive the PPA

52. Based on my interview of the Former Energy Assistant Secretary, I learned that, in or about October 2013, JOSEPH PERCOCO, a/k/a "Herb," the defendant, contacted the Former Energy Assistant Secretary and asked whether the Energy Company was going to be awarded a PPA under the Energy RFP. The Former Energy Assistant Secretary advised PERCOCO that the Energy Company was unlikely to be awarded a PPA because there were other projects that were viewed more favorably by the reviewing committee. The Former Energy Assistant Secretary recalled that PERCOCO appeared surprised by the Former Energy Assistant Secretary's response. The Former Energy Assistant Secretary also explained that what he told PERCOCO was confidential information, to which the Energy Company did not have access, and in fact the Energy Company's application for a PPA remained pending for at least another 20 months. The Former Energy Assistant Secretary further explained that he interacted infrequently with PERCOCO, and when they interacted it often related to logistics of the Governor's events. This contact was one of very few such contacts on substantive issues that the Former Energy Assistant Secretary recalled having with PERCOCO during the approximately four years they both worked at the Governor's Office.

a. On or about October 16, 2013, PERCOCO told Howe by email that Howe should call PERCOCO at his office in Manhattan and noted that Howe should "get the pine box 1st!!" Howe understood "pine box" to mean casket -- *i.e.*, that there was going to be bad news for the Energy Company. When they ultimately connected, Howe learned from PERCOCO that the Energy Company was not likely to be awarded the PPA.

---

add "You should be in mtg"; and modified PERCOCO's response to add "and make sure all is good"; and removed the last part of the chain about "ziti." Howe explained that he made these edits for the same reasons as explained above.

53. Based on my review of emails, documents obtained in the course of this investigation, and interviews of, among others, Howe and State employees, I believe that, in or around the end of 2013, JOSEPH PERCOCO, a/k/a "Herb," the defendant, and Howe deliberately did not inform PETER GALBRAITH KELLY, JR., a/k/a "Braith," the defendant, that they had learned that a PPA would not be forthcoming. To the contrary, PERCOCO and Howe decided to continue to assure KELLY that PERCOCO was using his official position and influence to help the Energy Company obtain a PPA so the Energy Company would continue to make payments both to PERCOCO's wife and to Howe through Howe's LLC. In order to maintain the illusion, PERCOCO arranged several meetings in 2014 and 2015 between KELLY and State officials who held relatively senior positions but, in reality, had little or no involvement in the Energy RFP and PPA selection processes. Evidence of PERCOCO's efforts to continue to extract money from KELLY includes, among other things, the following:

a. In or around July 2014, PERCOCO arranged a meeting between KELLY and the Chairman of Energy and Finance for New York, a member of the Governor's Cabinet who is often referred to as the State's "energy czar," and to whom the following State agencies report -- NYPA, NYSERDA, DPS and the Long Island Power Authority (the "Energy and Finance Chair").

i. On or about July 17, 2014, KELLY wrote to PERCOCO: "Joe – wondering if you had a couple minutes to talk Monday? I'm taking heavy heat. A quick conversation could help a lot." In reference to this email, Howe explained that the Energy Company's leadership was criticizing KELLY for the lack of progress with respect to the PPA, as the Energy Company's application for the PPA was still pending.

ii. On or about July 18, 2014, Howe emailed PERCOCO, "Herb – getting messy. I told Braith that you were asking [the Energy and Finance Chair] to hold a meeting with Braith and the ISO [or, Independent System Operator] and determine if this deal is possible. [. . .] This makes Braith happy. And gets us out of the middle and the group determines if possible. If he gets you on the phone just listen to him as I have been trying to keep this alive now at the end of the line as time has run out so a meeting is necessary." Based on public documents, I know that the ISO is an organization that, among other things, operates wholesale electricity markets and manages transmission lines.

iii. On or about July 22, 2014, Howe wrote to PERCOCO, in part, "Handle fat boy carefully. We don't need an interruption in that Zitti delivery or else we[']ll really be up the creek. Just need to tell him 'you called [the Energy and Finance Chair] and he is arranging a meeting the end of this week beginning of next week with himself, Braith and [an individual at the New York ISO] to figure out how to move this forward.' We can not have any interruption in delivery, and right now we are teetering. Ok?" In reference to this email, Howe has explained that he was telling PERCOCO to pay attention to KELLY so that KELLY would feel assured that the Energy Company's interests were being handled by PERCOCO, and KELLY would then continue to pay Howe and PERCOCO's wife.

iv. Later that day, PERCOCO wrote to Howe, "ok. he is here in my ofc now" to which Howe replied, "Remember Zitti!!" In reference to this email, Howe confirmed that "he" is KELLY.

v. Approximately 20 minutes later, PERCOCO emailed Howe that his meeting with KELLY "Just finished" and it "looks like [the Energy and Finance Chair] will see him and his guys this fri." Howe replied, "Great work Herb!," to which PERCOCO replied "now do your part! sending new invoices shortly." As set forth in more detail below, I know from documents I reviewed and from discussions with Howe, that around this time, PERCOCO sought payment through Howe from other clients of Howe who had business before the State, and Howe has confirmed that the "invoices" PERCOCO referred to relate to seeking payments from the Syracuse Developer.

vi. Based on interviews with the Energy and Finance Chair's Chief of Staff (the "Chief of Staff") and the Energy and Finance Chair, I learned that PERCOCO asked the Chief of Staff to arrange a meeting between KELLY and the Energy and Finance Chair. The Chief of Staff ultimately arranged the meeting, which occurred on or about July 25, 2014. PERCOCO's request to the Chief of Staff was the only such request for a meeting the Chief of Staff could recall receiving from PERCOCO.

b. On or about August 20, 2014, Howe informed KELLY that PERCOCO was "anxious" to set up a meeting for KELLY with the newly-appointed Director of State Operations (the "State Operations Director"), who had recently replaced the Former State Operations Director. Howe and PERCOCO then worked to set up this meeting, as follows:

i. On or about October 1, 2014, at approximately 7:50 a.m., Howe wrote to PERCOCO, "Herb - Braith wants to meet with [the State Operations Director] this Friday either in NYC or Albany [. . .] Can you make it happen?" Approximately three hours later, PERCOCO wrote, "Have Braith call [the State Operations Director's Administrative Assistant] at [phone number] and ask to see [the State Operations Director] Friday in NYC. [They] are expecting the call." In an interview, the State Operations Director's administrative assistant confirmed that PERCOCO requested a meeting between KELLY and the State Operations Director around this time, and it was one of relatively few meetings the administrative assistant recalled PERCOCO requesting for the State Operations Director.

ii. Howe replied to PERCOCO, "On it. Make sure to have the 'be receptive' discussion with [the State Operations Director]. Don't want to tip over the Zitti wagon." Based on an interview of Howe, I understand that Howe was explaining to PERCOCO that the State Operations Director had to appear receptive to KELLY so that KELLY would continue to pay PERCOCO and Howe.

iii. Ultimately, due to a scheduling conflict, the State Operations Director sent his Deputy Director to the meeting. After the meeting, Howe informed PERCOCO that KELLY was upset and gave Howe "an earful."

c. In or around March 2015, PERCOCO and Howe arranged a meeting for KELLY with the Secretary to the Governor. In an email to the Secretary to the Governor, Howe wrote, "As Joe told you, Braith is 'family' and we have been trying to figure out his project for the last few years..." The Secretary to the Governor replied that he looked "forward to connecting with Braith."

x. KELLY Stopped Payments to PERCOCO's Wife After It Became Apparent that the Energy Company Would Not Receive the PPA

54. Based on my review of publicly available information and my interviews of various State employees I know that, to date, NYPA has not selected any new power generation projects nor has it awarded a PPA to any company in connection with the Energy RFP.

55. Based on interviews of, among others, Howe and employees of the Energy Company, and my review of emails, I believe that by

in or around the spring of 2015, it had become clear to PETER GALBRAITH KELLY, JR., a/k/a "Braith," the defendant, that the Energy Company likely would not be getting the PPA, and the Energy Company's need for the PPA had lessened because the Energy Company had obtained at least some private funding for the construction of the Power Plant. In or around June 2015, the Energy Company stopped paying the monthly retainer for Howe that it had been paying to Howe's LLC, and Howe reached out to KELLY by email to try to get paid. Based on the interview of the External Affairs Manager, I learned that, in or around August 2015, KELLY informed the External Affairs Manager that funding for the wife of JOSEPH PERCOCO, a/k/a "Herb," the defendant, would not be included in the Energy Company's budget for 2016. In an email dated November 23, 2015, the External Affairs Manager discussed with KELLY the new payment structure for teachers, a per diem of $250 per day (far less than PERCOCO's wife was paid in the preceding years) and noted that the External Affairs Manager wanted to hire a new teacher. Based on my interview of the External Affairs Manager, I understand that the new teacher was being hired to replace PERCOCO's wife, and would be paid at the new per diem rate.

56. Financial records reflect that the last payment from Consultant-1 to the wife of JOSEPH PERCOCO, a/k/a "Herb," the defendant, was on or about January 28, 2016.

B. *The Syracuse Developer Paid Bribes to PERCOCO in Exchange for Official Action*

57. As set forth in more detail below, even after JOSEPH PERCOCO, a/k/a "Herb," the defendant, was able to get the Energy Company to make payments to his wife in the amount of $7,500 per month, PERCOCO remained in a difficult personal financial situation and tried to address this by seeking additional money from Howe's clients who had business before the State. Beginning in or around early 2014, PERCOCO, through Howe, solicited bribe payments from the Syracuse Developer. In response to these requests, in or around the spring of 2014, PERCOCO, Howe, and two executives of the Syracuse Developer -- President STEVEN AIELLO and General Counsel JOSEPH GERARDI, the defendants -- entered into a bribery scheme whereby the Syracuse Developer would make tens of thousands of dollars in payments to PERCOCO, using Howe as a pass-through to help conceal that the payments to PERCOCO came from the Syracuse Developer, and in exchange, PERCOCO agreed to use, and did in fact use, his official position and influence to assist the Syracuse Developer with a number of issues as the

opportunities arose. Specifically, PERCOCO agreed to, and did, take official action to (a) reverse the adverse decision by the Empire State Development Corporation ("ESD"), which is the State's main economic development agency, that would have required the Syracuse Developer to enter into a costly labor peace agreement ("LPA"), (b) free up a backlog of State funds that had already been awarded to the Syracuse Developer but were delayed in payment, and (c) secure an approximately $5,000 raise for AIELLO's son, who worked in the Executive Chamber.

i. PERCOCO Solicited Bribe Payments from the Syracuse Developer

58. Based on my review of emails and my discussions with Howe, I learned that, in or about January 2014, while still employed as the Deputy Executive Secretary to the Governor, JOSEPH PERCOCO, a/k/a "Herb," the defendant, began discussions with Howe about how PERCOCO wanted to receive payments from the Syracuse Developer. For example:

a. On or about January 15, 2014, PERCOCO and Howe were scheduled to meet with STEVEN AIELLO, the defendant, at the Governor's Office in New York, New York. Shortly before that meeting, Howe emailed PERCOCO and advised PERCOCO to "Lay it on thick , govs loves you [. . .] Lay it on heAvy Herbie! Zitti herb! Zitti!!" PERCOCO then responded, "I may pull gov and herbert in to say hello to him if they are still here!" Howe replied, "That would be great! Worth another crate of Zitti!" Howe has explained that the "herbert" referenced in PERCOCO's message was the Former State Operations Director, and that PERCOCO was suggesting that he might have the Governor and the Former State Operations Director greet AIELLO during AIELLO's visit to the Governor's Office in order to be able to later solicit "zitti" from the Syracuse Developer. Howe has confirmed that the meeting with AIELLO, the Governor, and the Former State Operations Director took place, which is corroborated by records showing that AIELLO did in fact visit the Governor's Office that day.

b. In a subsequent email in the same chain described above, which appears to have been sent prior to the meeting, Howe wrote, in part, that Howe had suggested to AIELLO that PERCOCO might eventually seek AIELLO's advice about the Syracuse region in connection with the Governor's upcoming reelection campaign. PERCOCO, however, responded, "only if that other thing happens! I will advise him on how to play a role and be relevant!" Howe has

explained that the "other thing" referred to PERCOCO's expectation that he would receive payments from the Syracuse Developer.

59. Based on my review of documents and emails and an interview with a former assistant counsel to the Governor (the "Assistant Counsel"), I know that in or around July 2014, before JOSEPH PERCOCO, a/k/a "Herb," the defendant, left the Executive Chamber to work as the Governor's campaign manager, PERCOCO sought an opinion from the Assistant Counsel about the possibility of PERCOCO working private sector jobs while he was employed as the Governor's campaign manager. Based on the interview with the Assistant Counsel and related documents, and the information uncovered in this investigation, I believe that PERCOCO provided false and misleading statements when he met with the Assistant Counsel and sought the Assistant Counsel's guidance. For example, PERCOCO informed the Assistant Counsel that he planned to work at a law firm on issues related to labor organizations, and that he would work only on issues pending before municipal governments. Percoco did not mention that he anticipated to work on issues related to New York State government when, in truth and in fact, and as set forth below, PERCOCO did not expect that his work would be strictly confined to issues pending before municipal governments. Instead, at the time of this conversation, PERCOCO already was planning to receive payments from the Syracuse Developer, which, as he well knew, had substantial business before the State.

a. On or about the same day of the meeting with PERCOCO, the Assistant Counsel wrote a memorandum, dated on or about July 9, 2014, with the subject line "Post-Employment Ethics Rules/Restrictions" (the "Employment Memorandum"). The Employment Memorandum addressed whether PERCOCO would be allowed under New York State law to work at a law firm on issues before municipal authorities. The Assistant Counsel wrote, in part, "Joseph Percoco has asked whether Public Officers Law (POL) § 74, subd. 8 impacts his post-State employment activities. He has advised me that he has been asked by a law firm to engage in discussions with various labor organizations on local matters pending before local municipalities." The Assistant Counsel concluded that, "In sum: there are no restrictions on his proposed activities. The POL limits the actions of a covered State employee with respect to appearances or matters before State agencies; not local governmental entities."

b. The Employment Memorandum expressly pointed out that

PERCOCO was barred by State law from working on issues pending before State agencies or the Executive Chamber. The Assistant Counsel wrote that, for two years after leaving State service, "an Executive Chamber employee is prohibited from receiving compensation for services rendered in connection with any matter before the Executive Chamber and is also prohibited from appearing or practicing before the Executive Chamber or any state agency." (Emphasis in original.)

c. The Assistant Counsel has explained that his advice with respect to PERCOCO's post-State employment would have been different if PERCOCO had proposed working on behalf of clients with business before New York State government. The Assistant Counsel also stated that, following their early July 2014 meeting, PERCOCO did not seek any additional advice or guidance from the Assistant Counsel.

d. On or about July 10, 2014, PERCOCO forwarded the Employment Memorandum to Howe. In response, Howe wrote, "Herb Zitti !! Very nice."[8]

60. Based on my review of emails and my discussions with Howe, I know that, in and around this same time period, between June and July 2014, JOSEPH PERCOCO, a/k/a "Herb," the defendant, sent a number of increasingly aggressive emails to Howe requesting additional monetary payments from Howe's clients. Based on my review of bank records and the FBI's financial analysis, I know that PERCOCO had

---

[8] As described above, PETER GALBRAITH KELLY, JR., a/k/a "Braith," the defendant, told executives at the Energy Company on two separate occasions that he had obtained a memo from the Governor's Office approving the hiring of PERCOCO's wife. Based on my review of documents and interviews in this matter, the Employment Memorandum cannot be the purported memo to which KELLY was referring. First, the Employment Memorandum was written more than a year after KELLY first claimed he had seen such a memo and approximately one week after KELLY, for a second time, claimed he had seen it. Second, the Employment Memorandum does not relate in any way to PERCOCO's wife's employment, and it expressly prohibits PERCOCO from doing any work on any matter pending before the Executive Chamber or any State agency.

an approximately $800,000 balloon payment due on his mortgage in or around July 2014. Furthermore, PERCOCO indicated to Howe that he would not provide Howe's clients with his official assistance unless and until he received monetary payments. For example:

a. On or about July 23, 2014, Howe forwarded PERCOCO an email from a client proposing a promotional opportunity for the administration and added, in part, "Herb - we should talk about this." PERCOCO replied, "ok. will deal with it after I get my ziti!"

b. Two days later, on or about July 25, 2014, Howe sent an email to PERCOCO related to the Energy Company in which Howe reported that "Braith Txd me to say [the Energy and Finance Chair] meeting went well. Looks like a few more months of Zitti." PERCOCO replied, "I have no ziti herb. none. but . . . enjoy your vacation. I will send my kids in the backyard with the garden hose." Approximately two hours later, Howe asked PERCOCO to, among other things, speak with the Energy and Finance Chair about the Energy Company. PERCOCO responded in part: "No. I cannot. I am barred from having those conversations." Howe has explained that PERCOCO had never previously refused to intervene with a State official on behalf of the Energy Company (once the Energy Company had begun paying PERCOCO's wife), and in fact had repeatedly done exactly that despite "being barred from having those conversations." Howe understood that PERCOCO's refusal to speak with the Energy and Finance Chair at this time was because PERCOCO was seeking additional money from other clients of Howe and had not yet received it.

ii. The Syracuse Developer Wanted PERCOCO's Assistance with ESD

61. Based on my review of emails, my discussions with Howe, and interviews with employees of ESD, I learned that, around this same time, in the summer of 2014, the Syracuse Developer was locked in a disagreement with ESD over whether, by law, one of the Syracuse Developer's construction projects in Syracuse required a costly labor peace agreement ("LPA") with organized labor. Having failed to persuade ESD that its project did not need an LPA or to modify the project as suggested by ESD to avoid triggering the statutory LPA requirement, the Syracuse Developer repeatedly sought the assistance of JOSEPH PERCOCO, a/k/a "Herb," the defendant, to avoid the LPA requirement.

a. The issue first arose in or around early summer 2014. At that time, the Syracuse Developer was constructing a parking lot (the "Parking Lot") in Syracuse. ESD had awarded more than approximately $1.5 million to the Syracuse Developer for this project. On or about June 27, 2014, JOSEPH GERARDI, the defendant, informed ESD that a portion of the Parking Lot would service, among other things, a neighboring hotel and a future hotel that had not yet been built.

b. On or about July 7, 2014, a Syracuse-based employee of ESD ("ESD Employee-1") emailed GERARDI and explained that "ESD legal counsel has reviewed the information you have provided" and "has determined that" because the Parking Lot will directly service a hotel, "ESD funding for this project will trigger the requirement for the Labor Peace Agreement (LPA) we previously discussed." ESD Employee-1 instructed the Syracuse Developer to "please contact the appropriate local labor organization and negotiate an LPA at your earliest convenience." From speaking with Howe and employees of ESD, I learned that certain State-funded construction projects that involve or relate to hotels require an LPA between the developer and the relevant hotel workers' unions, which would have significantly increased the cost of the Parking Lot.

62. Based on my review of emails and interviews of, among others, Howe, I learned that STEVEN AIELLO and JOSEPH GERARDI, the defendants, were concerned that the need to obtain a LPA would delay construction of the Parking Lot or would compel the Syracuse Developer to forgo ESD funding. AIELLO and GERARDI characterized their disagreement over the need for a LPA as "time sensitive." In or around late July 2014, having failed to persuade ESD to change its mind on their own, AIELLO and GERARDI asked Howe to secure the help of JOSEPH PERCOCO, a/k/a "Herb," the defendant, in reversing ESD's decision that an LPA was necessary.

a. On or about July 30, 2014, AIELLO emailed Howe and asked, in part, "is there any way Joe P can help us with this issue while he is off the 2nd floor working on the Campaign. We can't seem to put it behind us. I think Labor keeps drumming up their interpretation , to force us to sign with them. I could really use an advocate with regard to labor issues over the next few months."

b. The following day, on or about July 31, 2014, the head

of a regional body of a national labor union ("Labor Leader-1") wrote an email to AIELLO stating, in part, "Attached is a copy of the 'Labor Peace Agreement' that we spoke about at our meeting earlier this month. [. . .] I look forward to getting the Labor Peace Agreement finalized and signed." A few hours later, AIELLO forwarded this email to Howe and wrote, "Todd, can call Joe P. Need help on this. Thanks."

iii. The Syracuse Developer Paid PERCOCO Approximately $35,000

63. Based on my review of emails and my discussions with Howe, I believe that, less than two weeks after STEVEN AIELLO and JOSEPH GERARDI, the defendants, sought the help of JOSEPH PERCOCO, a/k/a "Herb," the defendant, with respect to the LPA, PERCOCO, AIELLO, GERARDI, and Howe reached an agreement whereby the Syracuse Developer would pay PERCOCO approximately $35,000 in return for PERCOCO's use of his official influence to help the company, including with regard to the company's issues with ESD. The Syracuse Developer's payments to PERCOCO would be run through Howe, who acted as a pass through in order to disguise the source of the payments. Evidence of the disguised payments to PERCOCO include, among other things, the following:

a. Based on my discussions with Howe, I learned that after AIELLO and GERARDI agreed to make payments to PERCOCO, AIELLO and Howe decided that the payments would be made through Howe's LLC (*i.e.*, the shell company Howe originally set up; in coordination with PETER GALBRAITH KELLY, JR. a/k/a "Braith," the defendant, to receive additional payments from the Energy Company) in order to mask the source of the payments, because AIELLO and Howe were concerned about the optics of paying PERCOCO while the Syracuse Developer had business and procurement contracts before the State. Accordingly, and as reflected in financial records I have reviewed, the Syracuse Developer paid PERCOCO by writing checks to Howe's LLC; and Howe then wrote checks in the same amount from Howe's LLC to PERCOCO's wife, to further disguise the source and nature of the payments.

b. The Syracuse Developer's first payment to PERCOCO was made in August 2014. On or about August 11, 2014, Howe sent an invoice for approximately $15,000 from Howe's LLC to AIELLO. Howe wrote in the accompanying email, "Steve - per our discussion. Attached is the Labor Relations Invoice for June, July & August 2014. Thank you." According to the invoice, Howe's LLC sought payment for "NYS

Consultation / Labor Strategy-Relations / Labor Financing" work covering the "June-July-August, 2014" time period. Howe has explained that the invoice in fact sought payment for PERCOCO, ostensibly for PERCOCO's work for the Syracuse Developer even though PERCOCO had not yet performed any work on behalf of the company.

c. In or around mid-August 2014, the Syracuse Developer paid by check $15,000 to Howe's LLC. In turn, Howe wrote a check for the same amount to PERCOCO's wife, which was later deposited into the PERCOCOs' joint bank account.

d. A second payment from the Syracuse Developer to PERCOCO, in the amount of $20,000, was made in or around October 2014. As with the August 2014 payment, the Syracuse Developer paid by check $20,000 to Howe's LLC. Howe then sent a check for the same amount to PERCOCO's wife, which was subsequently deposited into the PERCOCOs' joint bank account using an automated teller machine ("ATM") located in Westchester County, New York.[9]

iv. PERCOCO Pressured ESD to Reverse Its Decision on the Labor Peace Agreement

64. As set forth in more detail below, I believe, based on my review of emails and my discussions with Howe, that, in exchange for the $35,000 in payments from the Syracuse Developer, JOSEPH PERCOCO, a/k/a "Herb," the defendant, agreed to use, and did in fact use, his official position and influence to benefit the Syracuse Developer on at least three occasions as those opportunities arose. PERCOCO agreed to use, and did in fact, use his influence to cause ESD to

---

[9] As set forth above in paragraph 45, PERCOCO completed the Disclosure Form for the year 2014 in or around May 2015. Despite prior efforts to mask the payments from the Syracuse Developer by running the payments through Howe's shell company (*i.e.*, Howe's LLC), PERCOCO ultimately represented that he earned consulting fees totaling approximately $50,000 to $75,000 from the Syracuse Developer on the Disclosure Form. Pursuant to State law, the disclosure forms of State employees, including PERCOCO's, are not made available to the public unless sought through a State Freedom of Information Law request.

reverse its decision that the Parking Lot required a costly LPA. The evidence showing PERCOCO's agreement to use, and his actual use, of his influence on that issue includes, among other things, the following:

a. On or about August 22, 2014, JOSEPH GERARDI, the defendant, emailed Howe and copied STEVEN AIELLO, the defendant. GERARDI wrote, in part, "I wanted to follow up on ESD's position that we are required to enter into a LPA, in order to be able to utilize ESD funds [. . .] to construct a parking lot and infrastructure along the eastern shore of the Inner Harbor development." GERARDI continued, in part, "Steve and I wondered whether it would be appropriate at this time to engage our labor consultant, to try to resolve this matter, given that we would like to start construction this fall, but will not be able to proceed if an LPA is required." Howe has explained that GERARDI's reference to "our labor consultant" referred to PERCOCO, who at this time had already been paid $15,000 by the Syracuse Developer.

b. On or about August 28, 2014, Howe sent an email to PERCOCO and wrote, in part: "Will provide you with [Labor Leader-1]'s number tomorrow, you need to call her let her know you don't see an issue (as she agrees) with the need for a Laboe [*sic*] Peace Agreement for the [Syracuse Developer] INter [*sic*] Harbor Hotel parking lot project. [. . .] Then after you hear from her that she's ok with it, let [the Deputy State Operations Director] know so he can get the damn ESD lawyer to drop it, as no one sees it as an issue other than our own lawyer!" From speaking with Howe and employees of ESD, I know that the Deputy State Operations Director was the Executive Chamber official responsible for development policies and therefore had significant interaction with, as well as influence over, officials at ESD.

c. Also on or about August 28, 2014, Howe sent an email to AIELLO and copied PERCOCO. Howe wrote, "Steve - email Joseph, [Labor Leader-1's] number and he said he'd call her per our discussion tonight regarding the need to have a Labor Peace Agreement for the parking lot of the Inner Harbor Hotel. Joe understands the message that needs to be delivered and understands that [Labor Leader-1] agrees with us, that there is no need for one given the lot is primarily for the general public."

d. In or about November 2014 -- after the Syracuse Developer had paid PERCOCO a total of $35,000 -- AIELLO and GERARDI again sought PERCOCO's assistance in attempting to change ESD's decision requiring the LPA for the Parking Lot. On or about November 19, 2014, GERARDI wrote an email to PERCOCO, copying AIELLO and Howe, that explained the Syracuse Developer's unhappiness and disagreement with ESD's requirement of an LPA. The email began, "Hello Joe, [. . .] According to [ESD Employee-2], the local ESD Regional Director, ESD NYC Counsel has determined that our 'project' will trigger the requirement for a LPA."

e. On or about December 1, 2014, ESD Employee-2 emailed GERARDI to schedule time to discuss the LPA and "get this issue resolved." GERARDI then forwarded that email on or about December 3, 2014 to Howe, copying AIELLO, and wrote, in part, "Anything with JP on this. [ESD Employee-2] is pressing to 'resolve' this issue . . . . . and we don't want to be in jeopardy of losing the ESD funding . . . . . sorry to be a pest."

i. Howe, in turn, forwarded the email to PERCOCO with the message "???" PERCOCO responded to Howe and wrote "stand by." By this time, the Governor had been reelected and PERCOCO was less than a week away from returning to his former State position.

ii. Approximately ten minutes later, Howe wrote back to GERARDI and AIELLO: "Just hung up with JP. [ESD Employee-2] is being informed as I type this that ESD HQ in NYC does NOT concur with his read on this . . . . . JP said we should stand by and let message sink in over next several hours and then look for ESD to reach back out to you, with a 'different' perspective." Soon thereafter, Howe sent another reply stating, in part, "JP just called me back to say [ESD Employee-2] should be reaching out to you. Let me know when you do and I'll close loop with JP."

iii. The next day, on or about December 4, 2014, GERARDI wrote an email informing Howe that ESD Employee-2 called and stated that ESD had changed its position on the need for an LPA. GERARDI reported, in part, "I wanted to let you know that I spoke with [ESD Employee-2] this morning and he advised that they have convinced ESD that the hospitality portion of the Syracuse Inner Harbor development is relatively minor. Therefore, the ESD funds awarded can be used to build the parking lot and infrastructure

contemplated without the need for a LPA. [. . .] Thank you and JP for your efforts!" AIELLO responded, "They convinced ESD? Laughable!" Howe then replied, "Amazing how [ESD Employee-2] re-writes history!"

f. Based on my discussions with Howe and interviews with employees of ESD, I learned that the Syracuse Developer in fact was not required to obtain an LPA for the Parking Lot and was allowed to use ESD funds for the project.

v. PERCOCO Assisted the Syracuse Developer in Obtaining the Release of State Funds

65. I also believe, based on my review of emails and my discussions with Howe, that, in exchange for the $35,000 he was paid by the Syracuse Developer, JOSEPH PERCOCO, a/k/a "Herb," the defendant, also agreed to use, and did in fact, use his official position and influence on a second State matter of concern to the Syracuse Developer: the release of more than $14 million in State funds that had previously been awarded to the Syracuse Developer but had not yet been paid out due to backlogs at certain State agencies. The evidence showing PERCOCO's use of his official position and influence on this issue includes, among other things, the following:

a. In or around mid-2015, the State had not yet released significant blocks of funds to the Syracuse Developer for the construction of certain CNSE projects that had previously been awarded to the Syracuse Developer. As set forth in more detail below, in or around the end of 2013, CNSE chose the Syracuse Developer as its preferred developer in the Syracuse area and subsequently awarded the Syracuse Developer two major construction projects, specifically, an approximately $90 million manufacturing plant and an approximately $15 million film hub (the "Film Hub"). By in or around August 2015, the Syracuse Developer complained that approximately $14.2 million in State payments were either past due or about to come due on the two projects. Pressured by subcontractors and vendors that were threatening to stop working unless they were paid, STEVEN AIELLO, the defendant, and Howe asked PERCOCO, who had returned to his position as Executive Deputy Secretary, to intervene and help secure the release of those payments.

b. On or about August 31, 2015, AIELLO notified Howe and an employee of CNSE about a "vendor demanding payment" in connection

with the manufacturing plant. AIELLO wrote: "Help!! It's mounting!" Howe forwarded AIELLO's email to PERCOCO and asked him to attend a conference call with Howe, AIELLO, GERARDI, an employee of CNSE, and an employee at the Dormitory Authority of the State of New York ("DASNY"), which is responsible for facilities financing and construction. As Howe explained in the email, the purpose of the call was "to go over these asap this week if your schedule permits? As we discussed, [the Syracuse Developer] is getting hit left and right by vendors who are threatening to walk off the job . . . etc." PERCOCO responded, "ok. let me find out who is the right person to talk to at dasny. thanks."

c. Based on emails sent and received from PERCOCO's personal email account, I believe that within a day of the above exchange with AIELLO, PERCOCO had determined that the State Division of the Budget ("DOB") was the source of the delay in releasing the State funds to the Syracuse Developer, and that PERCOCO would meet with the DOB himself to try to resolve the issue. In an email sent on or about September 1, 2015, PERCOCO told Howe to "do a mtg on this tomorrow with budget folks which is where I am told this is stuck. thanks." Howe responded and asked PERCOCO to "do call with us?? They aren't going to listen to us." PERCOCO, however, responded, "you misunderstood me. I am doing the mtg with budget. as of now I dont need your guys on the call."

d. On or about September 3, 2015, Howe asked PERCOCO, "how did you make out with Budget on [the Syracuse Developer]. Out here in Syracuse and Steve is having a heart attack? Do you need a call with the [CNSE] folks to get budget anything?" PERCOCO replied, "No. Sit tight. Mtg is today."

e. The next day, on or about September 4, 2015, Howe emailed PERCOCO again to ask, in part, for "an update on the DOB meeting yesterday." PERCOCO responded, "There are some checks that are being freed up from the slow process next week. I am getting the exact list as we speak."

f. On or about September 9, 2015, the Deputy State Operations Director wrote to an employee of the DOB ("DOB Employee-1") and asked about the "timeframe" of the first significant disbursements for the Film Hub. Later the same day, DOB Employee-1 replied, in part, "$1.184m: Should happen within a week or so, depending on DASNY and SUNY Poly's responsiveness. DOB has allocated the funds. We're

checking with DASNY on [grant disbursement agreement] status, information outstanding from SUNY Poly and anything else needed for payment." (Emphasis in original.) Based on my review of emails and publicly available sources, I learned that, after the DOB made the Film Hub funds available, DASNY had to complete its own approval process and then enter into a grant disbursement agreement with Fort Schuyler, which, in turn, would provide the Film Hub funds to the Syracuse Developer.

g. Based on my review of emails, I know that, in or around the second of half of September 2015, DASNY requested certain additional documents from Fort Schuyler and the Syracuse Developer related to the Film Hub funds.

h. On or about September 30, 2015, Howe forwarded a text message from AIELLO in which AIELLO expressed disappointment that he had not been invited to the events surrounding the Governor's visit to Syracuse that was scheduled to take place later that day. In a follow-up email to PERCOCO and the Deputy State Operations Director that day, Howe wrote, in part, "Today is just another nail in Steve"s [*sic*] back, he wasn't even invited to attend. We need to put ourselves in his position. He built one building on time and completed it and can't get final payment and he's half way done on a second building and hasn't gotten paid a penny, we constantly ask him to help us. . . . It's not a good situation. It's an issue of managing our friends. We just can't abandon them when things get tough and I think that's what he is venting about."

i. In a reply soon thereafter, PERCOCO asked, in part, "agree with you todd about abandoning people. [Deputy State Operations Director] why didn't we invite steve?"

ii. Howe replied and wrote, in part, "Just need your help to get that funding moving the bureaucracy is killing them."

iii. PERCOCO responded to Howe's email and stated, in part, "I have done everything I can. The small check should be breaking free [. . .] soon. The problem is your client at nano. You fix. I am fucking pissed at nano and the team there. [. . .] I need a mtg with you, alain and [the current Secretary to the Governor] asap! I am fuckin pissed!!!!" Based on my review of emails and my participation in this investigation, I know that the "client at nano" refers to CNSE, which, as set forth above, was a client of Howe and

has the nickname "Nano" and that "alain" refers to ALAIN KALOYEROS, a/k/a "Dr. K," the defendant.

iv. In a subsequent email in the same chain, also sent on or about September 30, 2015, the Deputy State Operations Director wrote, "I spoke to Steve directly. He will be at the site and have a few construction workers from the hotel ready to greet the gov at 115."

v. Howe replied, "Thank you. This eases the funding headache. Important that community see this project is still on Govs radar screen."

vi. I learned from reviewing emails and media reports that, later the same day, on or about September 30, 2015, the Governor toured a hotel located in the Syracuse Inner Harbor that was being constructed by the Syracuse Developer and met with, among others, AIELLO.

vi. PERCOCO Secured a Raise for AIELLO's Son

66. I also believe, based on my review of emails and my discussions with Howe and State employees, that, in exchange for the $35,000 he was paid by the Syracuse Developer, JOSEPH PERCOCO, a/k/a "Herb," the defendant, agreed to use, and did in fact, use his official position and influence in a third way to benefit the Syracuse Developer: to secure a salary increase of approximately $5,000 for the son of STEVEN AIELLO, the defendant, ("AIELLO's Son") who worked in the Executive Chamber. The evidence showing PERCOCO's use of his official position and influence with respect to AIELLO's Son's salary includes, among other things, the following:

a. In or around July 2014, AIELLO's Son left his job at New York State Housing and Community Renewal ("HCR") to work on the Governor's reelection campaign as an assistant to PERCOCO. AIELLO'S Son was not paid while working for the campaign. Following the election in November 2014, AIELLO's Son returned to HCR and then moved to a position in the Executive Chamber in or around September 2015. Between November 2014 and around August 2015, AIELLO's Son received two raises and a locality adjustment, increasing his salary approximately ten percent. From speaking with, among others, an employee of the Executive Chamber who managed a variety of human resources issues and reported directly to PERCOCO ("Chamber

Employee-1"), I learned that salary increases for Executive Chamber employees are usually limited to no more than ten percent in a given year. Chamber Employee-1 could not recall any specific employee who has received a salary increase of greater than ten percent.

b. Notwithstanding the ten percent increase in his son's salary in less than a year, AIELLO sent an angry text message to Howe on or about September 25, 2015 complaining about the modest size of his son's most recent pay raise: "I just got a call from [my son], he got his paperwork for his raise. He went from 54 thousand a year to 56 thousand! We have waited patiently months for money for these projects with [CNSE]. The administration has embarrassed me in my community, as a slow pay.completely tarnished our reputation, we are considered a slow pay. [My son] bust his ass, loyal as the day is long. I have been loyal as the day is long. They insult us like this. I'm finished!!! Everybody else gets what they need and want. I keep giving. It's a sad statement!" Howe forwarded AIELLO's text to PERCOCO, and added: "I told Steve just now that I spoke to you and you were going to address the salary issue today [. . .] try to get him to 65 k or above." Howe then followed up later that same day, and PERCOCO responded, "I am working on it herb!"[10]

c. Based on my review of emails, publicly available documents, documents obtained in the course of this investigation, and interviews of, among others, Howe and employees of the Executive Chamber, I learned that, on or about September 25, 2015 -- the same day that Howe passed along AIELLO's complaints to PERCOCO -- PERCOCO sent an email to Chamber Employee-1 and three employees of the State Office of General Services ("OGS"), which handles certain human resources issues for the Executive Chamber. PERCOCO asked: "What

---

[10] This email echoed one from several months before. On or about May 27, 2015, Howe emailed PERCOCO and wrote, in part, "got a call from Steve Sr. Wanted to see if you could try and help jr. with that salary issue we had talked about?" Howe then specifically asked, "Is it impossible for him to get a $10k bump? He's at 54 k now is it possible to get him to 64k. ?" At the time, PERCOCO had responded, in part: "Tough do [*sic*] $10k bump. Can do $6k now then the rest later after session. Concerned about optics."

happened with [AIELLO's Son's] raise when he was moved to policy team? I am told he never got it. Also, we discussed moving him out of HCR?"

i. An employee of OGS ("OGS Employee-1") responded, "We moved him out of HCR. Didn't know it was supposed to go with a bump. 10%?"

ii. PERCOCO replied, "This is another stupid blunder. Another we had no idea. BS. I raised this months ago. Now he is quitting because you guys cant get the simplest things executed. [Chamber Employee-1], you handle this. I will call you."

iii. OGS Employee-1 informed PERCOCO that they would prepare a request for an additional ten percent salary increase; OGS then submitted the request to the DOB, which approved the raise on or about September 28, 2015. From speaking with Chamber Employee-1 and two of the OGS employees copied on the above email, I learned that they had no recollection of PERCOCO being so involved in seeking the raise of any other Executive Chamber employee.

d. On or about September 25, 2015, approximately two hours after PERCOCO learned the salary increase request had been submitted to the DOB, PERCOCO emailed Howe and wrote, "[AIELLO's Son] issue resolved. will take effect immediately. spoke to him and all is good." I know that, in fact, AIELLO's Son did receive a ten percent raise amounting to approximately $5,700 per year on or about October 1, 2015 that was made retroactive to on or about September 24, 2015. The raise pushed his total salary to approximately $65,000 per year.

IV. THE BUFFALO BILLION FRAUD AND BRIBERY SCHEME

67. The PERCOCO Bribery Scheme described above was not the first scheme involving bribery and unlawful access to State benefits in which the Syracuse Developer participated. Rather, as described below, beginning in or around 2013, the Syracuse Developer and the Buffalo Developer conspired with Howe and ALAIN KALOYEROS, a/k/a "Dr. K," the defendant, to defraud Fort Schuyler -- which was charged with awarding significant development contracts paid for with taxpayer dollars obtained from ESD -- into giving lucrative contracts to the Syracuse Developer and the Buffalo Developer.

68. As part of this scheme, the Syracuse Developer and the Buffalo Developer paid bribes to Howe, which were purported to be "consultancy" payments and bonuses but which were in fact payments for Howe's actions in his capacity as an agent and representative of CNSE and the Research Foundation who had, along with ALAIN KALOYEROS, a/k/a "Dr. K," the defendant, substantial control over Fort Schuyler's State-funded development projects. In exchange for the payments to Howe, and as described more fully below, Howe worked with KALOYEROS to defraud Fort Schuyler by secretly rigging the bids for large development deals so that they went to the Syracuse Developer and the Buffalo Developer, while falsely representing to Fort Schuyler that the bidding process was fair, open, and competitive. In particular, as set forth below, (a) KALOYEROS caused Fort Schuyler to issue purportedly competitive requests for proposal ("RFPs") for companies to be named preferred developers for CNSE in Buffalo and Syracuse, where CNSE intended to undertake significant development projects paid for under the Buffalo Billion initiative and other state development programs; (b) KALOYEROS and Howe secretly tailored the RFPs so that the RFPs requested qualifications held by the Syracuse Developer and the Buffalo Developer; and (c) Fort Schuyler's evaluation committee and Board of Directors evaluated and voted on the bids not knowing that KALOYEROS and Howe had prevented competing bids and designed the requirements to fit the Syracuse Developer and the Buffalo Developer. For his part in the scheme, KALOYEROS was able to maintain his leadership position and substantial salary at CNSE and garner support from the Office of the Governor for projects important to him, including the creation of SUNY Poly.

A. *KALOYEROS Hired Howe to Be an Agent and Representative of CNSE*

69. Based on my review of emails and interviews with, among others, Howe, I learned that, in or around the fall of 2011, ALAIN KALOYEROS, a/k/a "Dr. K," the defendant, contacted Howe for the purpose of retaining Howe as a consultant for CNSE. As set forth above, Howe had close connections to the Office of the Governor, whose support would be helpful with two goals of KALOYEROS: (i) the receipt of State funding; and (ii) the merger of CNSE into SUNY Poly, which KALOYEROS would found and lead. Among other things, Howe understood that KALOYEROS was concerned about his relationship with the Office of the Governor and was worried that he might lose his leadership position at CNSE. According to public records, in 2011 KALOYEROS was paid a salary of approximately $800,000 and received at least $500,000 in additional compensation through grants and/or other

payments. KALOYEROS accordingly told Howe that he wanted to hire Howe to help KALOYEROS maintain his position at CNSE/SUNY Poly, assist CNSE in its relationship with the Office of the Governor, and represent CNSE in its efforts to undertake large, State-sponsored development projects.

70. Based on my review of documents obtained from CNSE and the Government Relations Firm and its associated Law Firm, and interviews with, among others, Howe and individuals associated with CNSE and Fort Schuyler, I learned that in or around 2012, ALAIN KALOYEROS, a/k/a "Dr. K," the defendant, caused the Research Foundation to retain Howe as a consultant for CNSE and Fort Schuyler, at a rate of $25,000 per month, which continued until at least in or about 2015. These payments were made to the Law Firm. During the relevant time period, Howe physically worked at CNSE approximately twice per week. Howe had a parking space and an office at CNSE. Although the location of the office changed from time to time, it was always near KALOYEROS's office.

B. ***Executives of the Syracuse Developer and Buffalo Developer Bribed Howe for His Assistance in Obtaining State Contracts***

71. Based on my review of emails, publicly available and other documents, and interviews with, among others, Howe, I learned that throughout 2013 and 2014, STEVEN AIELLO and JOSEPH GERARDI, the defendants, caused the Syracuse Developer to pay Howe as a "consultant" knowing that Howe was acting as an agent and representative of CNSE and intending for him to use his official position for their benefit, as set forth below.

a. In or around November 2011, AIELLO, on behalf of the Syracuse Developer, entered into an agreement with the Government Relations Firm (which was run by Howe) under which Howe would serve as a "consultant" (and not a lobbyist), and the Syracuse Developer would pay the Government Relations Firm $6,500 per month. The following year, the Syracuse Developer expanded its relationship with Howe, agreeing to pay an additional $7,500 per month, for a total fee of $14,000 per month.

b. In or around August 2014, October 2014, November 2014, and June 2015, which were after the Syracuse Developer was named CNSE's preferred developer for Syracuse as set forth below, the Syracuse

Developer paid Howe bonuses totaling at least approximately $385,000. These bonuses were not paid to the Government Relations Firm. Rather, $135,000 in bonuses were paid to Howe's LLC, and $250,000 in bonuses were paid directly to Howe.

c. Further, I have learned from Howe that he kept AIELLO informed as he (Howe) negotiated his role at CNSE with ALAIN KALOYEROS, a/k/a "Dr. K," the defendant, and that Howe informed AIELLO and GERARDI of his official role and influence within CNSE. This fact has been corroborated by, among other things, an interview of a principal of another development company who worked with Howe, who stated that Howe told him, in substance and in part, that Howe acted as an agent and representative of CNSE in finding partners for development projects; interviews with certain State employees; and emails (including ones described below) in which Howe forwarded to AIELLO and GERARDI communications with KALOYEROS and other individuals associated with CNSE in which internal CNSE business was discussed.

72. Based on my review of emails, publicly available and other documents, and interviews with, among others, Howe, I learned that throughout 2013 and 2014, LOUIS CIMINELLI, MICHAEL LAIPPLE, and KEVIN SCHULER, the defendants, caused the Buffalo Developer to pay Howe as a "consultant" knowing that he was acting as an agent and representative of CNSE and intending for him to use his official position for their benefit, as set forth below.

a. In or around January 2013 -- just as the Buffalo Developer began seeking large State contracts through the Governor's Buffalo Billion initiative -- SCHULER, on behalf of the Buffalo Developer, entered into an agreement with the Law Firm, through which the Government Relations Firm would provide "strategic advice and counsel regarding business generation initiatives across New York State." The agreement specified that it would not include any lobbying of State or Federal officials. In return for Howe's services, the Buffalo Developer agreed to pay $100,000 per year. Prior to this agreement, the Buffalo Developer had not retained or paid any money to Howe or the Government Relations Firm.

b. I believe, based on my review of emails and interviews with, among others, Howe, that before and during the time in which CIMINELLI, LAIPPLE, and SCHULER caused the Buffalo Developer to pay Howe, they knew that Howe was an agent of CNSE who had substantial

influence with ALAIN KALOYEROS, a/k/a "Dr. K," the defendant, the President of CNSE and a board member of Fort Schuyler. In particular, Howe has stated that, in or around the end of 2012, he approached CIMINELLI and told CIMINELLI, in substance and in part, that he (Howe) was acting on behalf of the Office of the Governor and CNSE, which were looking for help in creating large development projects in the Buffalo area. CIMINELLI, LAIPPLE, and SCHULER's knowledge that Howe was acting as an agent and representative of CNSE has been corroborated by, among other things and as noted above, an interview of a principal of another development company who worked with Howe, interviews with certain State employees, and emails in which Howe forwarded to LAIPPLE and SCHULER communications with KALOYEROS and other individuals associated with CNSE in which internal CNSE business was discussed. For example:

i. On or about October 7, 2013, Howe forwarded to LAIPPLE and SCHULER an email exchange between Howe and KALOYEROS in which Howe and KALOYEROS discussed internal CNSE matters, including personnel matters, as well as the timing and method of the announcement of the Buffalo RFP. In his email to LAIPPLE and SCHULER, Howe stated, "we decided to get this Buffalo [RFP] out asap."

ii. On or about December 3, 2013, Howe forwarded an email between him, a partner at the law firm representing CNSE, and a representative of another company that had business with CNSE, discussing business between that other company and CNSE. In his email to LAIPPLE and SCHULER, Howe wrote, among other things, "Keep this close to the vest."

73. Prior to the Fort Schuyler bidding process, individuals associated with the Syracuse Developer, including STEVEN AIELLO and JOSEPH GERARDI, the defendants, and the Buffalo Developer, including LOUIS CIMINELLI, the defendant, had become significant contributors to the Governor's election campaigns. I believe that these contributions were intended at least in part to develop a relationship with the Office of the Governor that would help enable the Syracuse Developer and the Buffalo Developer to obtain State-funded development contracts. Evidence of this intent includes the following:

a. Based on my review of publicly available records and interviews of Howe, I learned that from in or around 2001 through

in or around 2010, the Syracuse Developer did not make large contributions to State gubernatorial campaigns -- contributing a total of approximately $39,000 over that ten-year period. Similarly, prior to the fall of 2011, AIELLO made two contributions to the Governor's campaign, each in the amount of $5,000, and GERARDI made no contributions to State gubernatorial campaigns. During these years, as set forth above, the Syracuse Developer's business focused principally on private development projects. Beginning in December 2011, however, as the Syracuse Developer began to seek State-funded development work with the assistance of Howe, contributions from its executives and related parties increased dramatically. Beginning in December 2011, after the Syracuse Developer retained Howe, AIELLO, GERARDI, and other executives from the Syracuse Developer -- largely at the direction of Howe -- personally began making, and directed the Syracuse Developer to make, substantial campaign contributions to the Governor's campaign and related entities. Specifically, from December 2011 through 2013, AIELLO, GERARDI, their family members, another executive of the Syracuse Developer ("Syracuse Developer Executive-1"), an entity associated with Syracuse Developer Executive-1, and the Syracuse Developer itself contributed at least approximately $250,000 to the Governor's election campaigns, with each contribution being in an amount of $10,000 or greater. Notably, on or about July 9, 2013, which, as described below, was approximately one month before AIELLO and GERARDI supplied information to Howe to use to rig the Syracuse RFP, AIELLO, GERARDI, their family members, Syracuse Developer Executive-1, and the Syracuse Developer together contributed approximately $65,000 to the Governor's election campaign. The following day, on or about July 10, 2013, an entity associated with Syracuse Developer Executive-1 made a $60,000 contribution to the Governor's election campaign. As a result of these contributions, the Syracuse Developer has been publicly reported as the top donor to the Governor in or around upstate New York.

b. I know from my review of emails and interviews with Howe that Howe encouraged AIELLO and GERARDI to make contributions to the Governor's campaigns and to make contributions in higher amounts so that the Governor's Office would know and remember them. For example, on or about May 18, 2011, Howe sent an email to AIELLO, in which Howe instructed, "you should hold on making any political $$ contributions to any state or federal electeds, so we can make sure you can [get] the most leverage out of them."

c. Between in or around December 2009 and January 2014, CIMINELLI and his immediate family members contributed at least $100,000 to the Governor's election campaigns. Additionally, in or around November 2013 -- when the Buffalo Developer's bid to become a preferred developer was under consideration by Fort Schuyler, as described below -- CIMINELLI hosted a fundraising dinner for the Governor, at which approximately $250,000 was raised.

d. Further, JOSEPH PERCOCO, a/k/a "Herb," the defendant, made specific requests to Howe for both the Syracuse Developer and the Buffalo Developer to make donations to the Governor's campaign, and Howe relayed those requests to the Syracuse Developer and the Buffalo Developer. For example, on or about November 12, 2013, PERCOCO wrote an email to Howe, in which PERCOCO stated that a commitment by CIMINELLI to host the fundraising dinner described above in which $175,000 would be raised for the Governor's re-election campaign "does not work Herb," because CIMINELLI had previously committed to a higher amount. As noted, the dinner ultimately raised approximately $250,000.

C. Fort Schuyler Was Defrauded into Awarding State Development Contracts to the Syracuse Developer and the Buffalo Developer

74. Based on my review of emails, publicly available and other documents, and interviews with, among others, Howe, I learned that in 2013, ALAIN KALOYEROS, a/k/a "Dr. K," the defendant, and Howe developed a plan to identify preferred developers for potential construction projects associated with CNSE in Syracuse and Buffalo, New York. This plan was motivated, in part, by the announcement of the Governor, in or about January 2012, that the State would invest $1 billion in Buffalo, New York. This plan included issuing two requests for proposal (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. However, the Syracuse Developer and the Buffalo Developer had been preselected by KALOYEROS and Howe to become the preferred developers in Syracuse and Buffalo, respectively, after the Syracuse Developer and the Buffalo Developer had each made sizable contributions to the Governor and had begun paying Howe for Howe's access to the Governor and 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. In order to award these valuable deals to the Syracuse Developer and Buffalo Developer, KALOYEROS and Howe manipulated the RFP process to prevent Fort Schuyler from receiving or being able to fairly consider competing bids.

i. Fort Schuyler Issued RFPs for Preferred Developers for Syracuse and Buffalo

75. Based on publicly available and corporate documents, and interviews with, among others, employees and members of the Board of Directors of Fort Schuyler, I have learned that the Board of Directors of Fort Schuyler has the authority to enter into agreements with private companies in which public funds will be spent to pay the companies to build facilities for CNSE. Prior to entering into a significant contract with private companies, Fort Schuyler typically issues a "request for proposal." "Request for proposal" is a term of art that refers to a type of solicitation in which an organization such as Fort Schuyler sets forth the fact that funding is available for a project and seeks bids from qualified and interested parties. I know from speaking with members of Fort Schuyler's Board of Directors that, particularly with respect to State-funded projects, RFPs issued by Fort Schuyler were supposed to be designed and drafted to provide a fair, open, and competitive bidding process with respect to both quality and price, and accordingly should not be drafted to favor any particular potential bidder and should not be provided to any parties in advance of publication.

76. Further, I learned that in or around 2013 and 2014, the Research Foundation had policies governing procurement that were used by Fort Schuyler. As set forth in these policies, the procurement process was intended "to promote open and free competition in procurement transactions" and "to ensure that procurements are priced competitively and that the selection process is not influenced improperly." Among other things, the policies required that "[s]uppliers that develop or draft specifications, requirements, statements of work, or requests for bids or proposals for a procurement must be excluded from competing in any resulting procurement."

77. Based on my review of emails, publicly available documents and interviews of members of the Board of Directors of Fort Schuyler, I learned the following regarding the process by which the Board of Directors selected preferred developers for Syracuse and Buffalo:

a. On or about August 20, 2013, ALAIN KALOYEROS, a/k/a "Dr. K," the defendant, sent an email to Howe and to an executive of Fort Schuyler (the "Fort Schuyler Executive"), in which KALOYEROS told the Fort Schuyler Executive that KALOYEROS would "like to issue an RFP for a strategic partner in Syracuse and a similar one in Buffalo. It should not focus on a specific project, but more on a strategic partnership with local developers who know the two regions, are grass root, have the construction and business credibility, and are willing to expand in jobs and investments in those regions in partnership with CNSE."

b. As set forth in more detail below, KALOYEROS and Howe worked together to draft the Syracuse and Buffalo RFPs. I know, based on interviews of, among others, a former executive of Fort Schuyler, that KALOYEROS maintained close oversight and control over the day-to-day operations of CNSE and Fort Schuyler, including over the design of development projects and the drafting of RFPs.

c. In or around October 2013, the Board of Directors of Fort Schuyler, by resolutions of the Board, issued the Syracuse and Buffalo RFPs, which requested proposals "for a strategic research, technology outreach, business development, manufacturing, and education and workforce training partnership with a qualified local developer" in the greater Syracuse area and in the greater Buffalo area, respectively. Because the RFPs were designed to select preferred developers that would, once chosen, be able to obtain potentially hundreds of millions of dollars in State-funded contracts from Fort Schuyler without further competitive bidding, the RFP selection process had substantial economic importance for both Fort Schuyler and the Research Foundation, through which such future contracts would be funded. The Board Resolutions authorizing the RFPs each stated that the Fort Schuyler Board would approve a contract only "[u]pon completion of a competitive RFP process and evaluation of responses." The RFPs themselves explained that Fort Schuyler would appoint a selection committee to review submissions, which would recommend the selection of a preferred developer to the Board of Directors of Fort Schuyler. The Board of Directors of Fort Schuyler

had the final authority for making the selection of preferred developers and authorizing contracts.

d. Despite the highly lucrative nature of the contracts, the Syracuse Developer ultimately was the only party to bid on the Syracuse RFP, and the Buffalo Developer was one of only three parties to bid on the Buffalo RFP.

e. In or about December 2013, the Board of Directors of Fort Schuyler voted to name the Syracuse Developer the preferred developer for Syracuse, and in or about January 2014, the Board of Directors of Fort Schuyler voted to name the Buffalo Developer one of two preferred developers for Buffalo. The Board of Directors based its decisions on, among other things, matrices created by the evaluation committee in which the evaluation committee compared each bidder's submission to the qualifications set forth in the relevant RFP.

ii. The Syracuse RFP Was Designed to Defraud Fort Schuyler

78. Based on my review of emails and interviews of, among others, Howe, I learned, that, unbeknownst to members of the Board of Directors of Fort Schuyler, the Syracuse RFP was designed so that the Board of Directors of Fort Schuyler would have no choice but to name the Syracuse Developer the preferred developer for Syracuse, as follows:

a. In or about August 2013, Howe informed JOSEPH GERARDI and STEVEN AIELLO, the defendants, that Fort Schuyler would issue the Syracuse RFP. On or about August 15, 2013, GERARDI sent an email to Howe, copying AIELLO and another executive of the Syracuse Developer. The subject line of the email stated: "[Syracuse Developer] Company Qualifications and Experience." Attached to the email was a document entitled "[Syracuse Developer] Company Qualifications.08-15.13" (the "Syracuse Developer Qualifications").

b. The Syracuse Developer Qualifications contained a list of qualifications of the Syracuse Developer and its executives, including AIELLO and GERARDI. For example, the Syracuse Developer Qualifications stated that employees use "Sophisticated project management tools, such as InSite SiteWork (www.insitesoftware.com) to accurately and efficiently coordinate all aspects of site and

utility construction, to create ideal building conditions, and USGlobalNet, or USGN's (www.usgn.net) web-based project management software, to effectively manage all projects on budget and on schedule."

c. On or about August 16, 2013, Howe replied to GERARDI'S email containing the Syracuse Developer Qualifications, writing "This works. Let me hand deliver to dr k. You guys should not email this to anyone but me. All good." I know based on my review of email and interviews with Howe and others that "Dr. K" is a nickname for ALAIN KALOYEROS, a/k/a "Dr. K," the defendant. Howe has explained that he sent this email because he did not want anyone else at CNSE or Fort Schuyler, other than himself or KALOYEROS, to learn of their scheme.

d. As described above, on or about August 20, 2013, KALOYEROS sent to Howe and to the Fort Schuyler Executive an email directing the Fort Schuyler Executive "to issue an RFP for a strategic partner in Syracuse and a similar one in Buffalo."

e. The following day, on or about August 21, 2013, Howe responded to KALOYEROS only, at KALOYEROS's work email address, stating "I have 'vitals' for buffalo and Syracuse friends." Howe has explained that "buffalo and Syracuse friends" referred specifically to the Buffalo Developer and the Syracuse Developer, respectively. Howe has further explained that the word "friends" was used to refer to "friends of the Governor," and that the Buffalo Developer and Syracuse Developer qualified as "friends" due, in part, to their donations to the Governor's campaigns and, in part, due to their relationship as clients of Howe. Furthermore, "vitals" referred to information about the Buffalo Developer and the Syracuse Developer that would be used to tailor the RFPs so that the Buffalo Developer's and the Syracuse Developer's proposals would be selected.

f. Later that day, on or about August 21, 2013, KALOYEROS, using his personal "gmail" address, responded to Howe's email and stated, "Please gmail not email."[11] Howe then asked in an email to

---

[11] It appears that KALOYEROS forwarded Howe's email to his personal "gmail" address before responding.

KALOYEROS, "did you understand that gmail email I sent this morning?" KALOYEROS responded, apparently sarcastically, "Vitals is so complicated to understand that I was hoping you'd break it down for me in 3 letter words, 2 word sentences."

g. On or about August 23, 2013, Howe sent an email to KALOYEROS at KALOYEROS's gmail account with the subject "FW: [Syracuse Developer] Company Qualifications and Experience." Attached to that email was the Syracuse Developer Qualifications, which Howe has explained were sent to him from GERARDI and AIELLO to be used in the development of the Syracuse RFP.

h. On or about September 13, 2013, KALOYEROS sent an email to several executives and employees of CNSE and Fort Schuyler and to Howe that contained a draft of the Syracuse RFP (the "Draft Syracuse RFP"). Howe forwarded the email and the Draft Syracuse RFP to AIELLO and GERARDI, writing "FYI---they are fine tuning now, but expect to release to public this week….what do you think? Keep Confidential pls." Under the heading "Developer Requirements," the Draft Syracuse RFP provided, among other things, the following language, which is nearly identical to language excerpted above from the Syracuse Developer Qualifications: the developer should use "sophisticated tools and advanced capabilities (such as InSite Sitework (www.insitesortware.com) to accurately and efficiently coordinate all aspects of site and utility construction, to develop ideal building conditions, and USGlobalNet, or USGN's (www.usgn.net) web-based project management software) to effectively manage projects expeditiously, professionally, on-time, and within budget."

i. On or about September 13, 2013, GERARDI replied by email to Howe and AIELLO, attaching a scanned version of the Draft Syracuse RFP that contained GERARDI's handwritten notes. These handwritten notes included the following:

i. In the paragraph of the Draft Syracuse RFP quoted above, the phrases "(such as InSite Sitework (www.insitesortware.com)" and "USGlobalNet, or USGN's (www.usgn.net)" were underlined, and in the margin was written "too telegraphed?? I would leave out these specific programs." Based on the context of this email and others, and interviews with Howe, I believe that GERARDI was expressing his concern that including these

specific qualifications in the RFP would make it too obvious that the RFP was being rigged to favor the Syracuse Developer.

ii. In a section of the Draft Syracuse RFP that stated that "the response to the RFP must specifically include . . . Latest audited financial statement for DEVELOPER," the word "audited" was crossed out in GERARDI's handwritten notes, and in the margin was written, among other things, "not available - typically prepared for not-for-profits, or public corp." Howe has explained that, based on his experience working with the Syracuse Developer, GERARDI and AIELLO were concerned about any requirement for audited financial statements because such a requirement had disqualified them from previous public contracts.

j. On or about September 13, 2013, several hours after sending the Draft Syracuse RFP containing the handwritten notes to Howe, GERARDI sent another email to Howe, copying AIELLO, reiterating that the Syracuse RFP should not include a requirement of audited financials, and suggesting instead that it read, "Latest audited financial statement if available, or other financial information/statements that demonstrate the DEVELOPER's financial qualifications." On or about September 16, 2013, Howe sent to KALOYEROS an email stating: "On syr rfp , where it says 'audited financials' just need to add an additional few words, 'audited financials or letter of financial reference from major financial institution.'"

k. On or about September 24, 2013, Howe forwarded to AIELLO and GERARDI a revised draft Syracuse RFP. This revised draft Syracuse RFP still contained the phrases "(such as InSite Sitework (www.insitesortware.com)" and "USGlobalNet, or USGN's (www.usgn.net)," but after the phrase "Latest audited financial statement for DEVELOPER" the phrase "or letter of financial reference from major financial institution" was included, as had been requested by AIELLO and GERARDI via Howe.

l. Despite having retained Howe and worked with Howe to tailor the Syracuse RFP to match the qualifications of the Syracuse Developer, the Syracuse Developer's RFP submission (which was affirmed by JOSEPH GERARDI, the defendant) falsely stated that no one "was retained, employed or designated by or on behalf of [the Syracuse Developer] to attempt to influence the procurement process."

iii. The Buffalo RFP Was Designed to Defraud Fort Schuyler

79. Based on my review of emails and interviews of, among others, Howe, I learned, that, unbeknownst to members of the Board of Directors of Fort Schuyler, the Buffalo RFP also was designed so that the Board of Directors of Fort Schuyler would have no choice but to name the Buffalo Developer the preferred developer for Buffalo, as follows:

a. As noted above, on or about August 21, 2013, Howe sent an email to ALAIN KALOYEROS, a/k/a "Dr. K," the defendant, stating "I have 'vitals' for buffalo and Syracuse friends."

b. On or about August 23, 2013, Howe sent an email to KALOYEROS at his gmail account with the subject "FW: RFQ,"[12] in which Howe wrote "Attached are vitals for buffalo. They expressed the 'broader' descriptions below help, versus narrower." Below that text was a section that Howe has explained came from the Buffalo Developer and that began "Todd - Our thoughts for the RFQ: RFQ Requirement - Selecting based on qualifications not price is important." Below that text were seven bullet points that were sent by MICHAEL LAIPPLE, the defendant, to be used to draft the Buffalo RFP.

c. Also on or about August 23, 2013, an individual from an architecture firm sent to KALOYEROS, Howe, and others associated with CNSE a power point containing details, including, among other things, the location, of a potential construction project (the "Riverbend Project") to be undertaken by CNSE in Buffalo. Howe then forwarded the email and power point regarding the Riverbend Project to LAIPPLE.

i. Based on conversations with, among others, Howe, individuals associated with CNSE, and developers, I learned that the

---

[12] Howe has explained that he occasionally referred to the RFPs as "RFQs," which stands for "Request for Qualifications," because the RFPs requested qualifications from interested bidders, as opposed to proposals on building specific projects.

Riverbend Project was not made public prior to the Governor's announcement of the Riverbend Project on or about November 21, 2013 -- which was more than three months after Howe had forwarded information about the Riverbend Project to LAIPPLE -- and that the details associated with the Riverbend Project contained in the power point described above were not shared with any developer other than the Buffalo Developer prior to the issuance of the Buffalo RFP.

d. Later in the day, on or about August 23, 2013, LAIPPLE sent an email to Howe stating, "One last thought on the RFQ. If the RFQ included something about MWBE promotion and compliance, that would be helpful." Howe has explained that "MWBE" refers to "minority and women business enterprises," and that the Buffalo Developer believed that they were stronger than their competitors in terms of their working with MWBEs. My review of the Buffalo Developer's website further confirmed that the Buffalo Developer publicly highlights its commitment "to proactively supporting Minority and Women-Owned Business Enterprise (MWBE)." Later on August 23, 2013, Howe forwarded the email from LAIPPLE to KALOYEROS, stating, "Additional vital for buffalo, stronger on the mwbe than usual would help."

e. On or about September 3, 2013, KALOYEROS responded to Howe's email from August 23, 2013 regarding the "Additional vital for buffalo," writing: "these are not unique to [the Buffalo Developer]..we need more definite specs, like minimum X years in Y, Z number of projects in high tech, etc, etc." Howe has explained that it was his understanding based on his course of dealing with KALOYEROS that when KALOYEROS referred to "minimum X years in Y," he was asking for information about the number of years that the Buffalo Developer had worked in a particular area, so that the Buffalo RFP could be more specifically tailored to the Buffalo Developer's qualifications.

f. On or about September 6, 2013, the Deputy State Operations Director sent an email containing a power point attachment entitled "RiverBend-FINAL.pptx" to Howe, KALOYEROS, and an executive at CNSE, with the message, "I pulled together the following ppt. A cut and paste of the various documents we have done over the last few weeks. Can you review. If all is okay, I will send for final review." The attached power point contained further details, including, among other things, the location and purpose, of the Riverbend Project. Later that day, on or about September 6, 2013, Howe forwarded this email, including the attachment, to LAIPPLE, with the message,

"Michael. FYI, confidential." LAIPPLE forwarded the email, with the attachment, to KEVIN SCHULER, the defendant.

g. On or about September 9, 2013, KALOYEROS sent an email from his gmail address to the gmail address of LOUIS CIMINELLI, the defendant, stating, "Draft of relevant sections from RFP enclosed..obviously, we need to replace Syracuse with Buffalo and fine tune the developer requirements to fit..hopefully, this should give you a sense of where we're going with this..thoughts?" Attached to the email was a draft of the Syracuse RFP. Under the "Developer Requirements" section of this draft of the Syracuse RFP, the draft stated, among other things, "Over 15 years proven experience." On the same day, CIMINELLI forwarded the email from KALOYEROS and the attached draft of the Syracuse RFP to LAIPPLE and SCHULER.

h. On or about September 13, 2013, SCHULER sent an email to KALOYEROS, copying CIMINELLI, LAIPPLE, and Howe. The email stated, among other things: "As Louis continues to enjoy the much warmer weather on the West Coast, I am sending along three attachments that I hope will meet your request for information." Attached to SCHULER's email to KALOYEROS was, among other things, a two-page document entitled "Company Profile." Included in the "Company Profile" was a statement noting that the Buffalo Developer had "over 50 years of experience."

80. The Buffalo RFP as publicly issued in or around October 2013 contained several provisions that were not in the draft of the Syracuse RFP that ALAIN KALOYEROS, a/k/a "Dr. K," the defendant, sent as a model on or about September 9, 2013, to LOUIS CIMINELLI, the defendant, but that were consistent with the Buffalo Developer's qualifications and I believe were included to further tailor the RFP for the Buffalo Developer, including the following:

a. Under "Developer Requirements," the Buffalo RFP stated, "Bidder is required to comply with equal opportunities for minorities and women pursuant to section 312 of the New York Executive Law. This includes the achievement of at least 23% Women and Minority Owned Business Enterprise participation (WMBE). Accordingly, it is expected that DEVELOPER be able to demonstrate a track record in WMBE participation."

b. Also under "Developer Requirements," the Buffalo RFP stated that it was seeking "a local DEVELOPER in the Greater Buffalo Area," with "Over 50 years of proven experience," which corresponded to the "Company Profile" provided to KALOYEROS by KEVIN SCHULER, the defendant.

81. On or about November 1, 2013, an email (the "50/15 Email") was sent by the Director of Procurement for the Research Foundation to developers who had expressed interest in the Buffalo RFP indicating that the requirement of 50 years of proven experience was a typographical error and that the requirement should have been 15 years of proven experience. Based on interviews with executives of CNSE and their related entities, I learned that it was the practice of ALAIN KALOYEROS, a/k/a "Dr. K," the defendant, to closely edit the language of all RFPs prior to publication and was known not to miss errors or changes. Based on these interviews, the timing of the 50/15 Email, the inclusion of the "50 years" requirement in the original RFP following KALOYEROS's receipt of the Buffalo Developer's company profile, and the emails set forth below, I believe that the original "50 years" requirement was not in fact a "typographical error."

a. On or about November 1, 2013, the following email exchange occurred:

i. An executive of the Buffalo Developer ("Buffalo Developer Executive-1") forwarded the 50/15 Email to LOUIS CIMINELLI and KEVIN SCHULER, the defendants, with the message "Grrrrr."

ii. SCHULER responded, "50 was a bit obnoxious."

b. Beginning or about November 2, 2013, the following email exchange occurred:

i. Buffalo Developer Executive-1 replied to the 50/15 Email, stating, "We confirm receipt and understand the intent of the change." Buffalo Developer Executive-1 then forwarded his message to two employees of the Buffalo Developer, including a marketing coordinator (the "Buffalo Developer Marketing Coordinator").

ii. On or about November 4, 2013, the Buffalo Developer Marketing Coordinator forwarded the email from Buffalo Developer Executive-1 to SCHULER, stating, "FYI - so much for that thought."

iii. SCHULER responded to the Buffalo Developer Marketing Coordinator: "15 is still pretty good."

82. On or about November 6, 2013, ALAIN KALOYEROS, a/k/a "Dr. K," the defendant, sent an email (the "November 6 Email") to a representative of a large, global construction company, that stated, among other things:

> As you know, we are in the midst of an RFP process and, while you are a valued and qualified partner, particularly for cleanrooms, we cannot endorse nor support a pre-cooked process or any process that singles out anyone, including you for business before the RFP process has been completed and a merit based group has been selected.

On or about November 6, 2013, KALOYEROS forwarded the November 6 Email to Howe. Approximately two minutes later, Howe forwarded that email chain to MICHAEL LAIPPLE and KEVIN SCHULER, the defendants, with the message "See below. Ouch!"

83. Based on my review of emails and publicly available documents and interviews of, among others, Howe, I learned that on or about November 14, 2013, which was approximately one week before the Governor announced the Riverbend Project publicly, Howe sent an email to LOUIS CIMINELLI, KEVIN SCHULER, and MICHAEL LAIPPLE, the defendants, stating, among others things, "Well looks like the Riverbend Announcement is going to happen next Thursday .... Please keep confidential." SCHULER responded, "How do they announce the riverbend site in the middle of this procurement? Site selection is supposedly part of the eval. Now mind you, I don't think it's a big deal but it does need to be considered." Based on my review of emails, I believe that SCHULER was concerned that if the Governor announced the Riverbend Project publicly before bids on the Buffalo RFP were due, the Buffalo Developer could lose the improper advantage it had secured from advanced notice that Riverbend would be the site of a CNSE project.

84. Based on my review of emails and publicly available documents, and interviews of, among others, Howe and employees of CNSE and its affiliated entities, I learned, among other things, that on or about December 10, 2013, the Buffalo Developer submitted its response to the Buffalo RFP, which included a proposed option of a development at the Riverbend Project's site. Despite having retained Howe and worked with Howe to tailor the Buffalo RFP to match the qualifications of the Buffalo Developer, the Buffalo Developer's RFP submission (just like the Syracuse Developer's) falsely stated that no one "was retained, employed or designated by or on behalf of [the Buffalo Developer] to attempt to influence the procurement process." Two other companies submitted responses to the Buffalo RFP. However, based on my review of emails between other developers, I know that at least two other developers decided at the time not to submit responses to the Buffalo RFP, because, among other thing, the RFP seemed vague and appeared written to provide an advantage to a specific company.

iv. Fort Schuyler Awarded Contracts to the Syracuse Developer and Buffalo Developer

85. Based on interviews of employees of CNSE and members of the Board of Directors of Fort Schuyler, I believe that the individuals associated with Fort Schuyler involved in evaluating the responses to the Syracuse RFP and to the Buffalo RFP and voting on awarding the preferred developer contracts were not aware of any developer receiving a draft of the Syracuse RFP or Buffalo RFP in advance of their public announcements. I learned from both employees of CNSE and members of the Board of Directors of Fort Schuyler that they would have viewed the pre-announcement sharing of a draft of an RFP with a developer as an unfair and improper practice. One member of the Board of Directors stated that he was disappointed that only one company -- the Syracuse Developer -- submitted a response to the Syracuse RFP and that only three developers submitted responses to the Buffalo RFP, because additional responses would have created competition and yielded a better result for Fort Schuyler.

86. Based on my review of emails and public documents and interviews of employees of CNSE and members of the Board of Directors of Fort Schuyler, I learned that:

a. On or about December 18, 2013, the Syracuse Developer was chosen by vote of the Board of Directors of Fort Schuyler as the preferred developer for CNSE in Syracuse, and soon thereafter was awarded an approximately $15 million contract to construct the Film Hub. In or around October 2015, without any further RFP, the Syracuse Developer was awarded an approximately $90 million contract to build a manufacturing plant in Syracuse.

b. On or about January 28, 2014, by vote of the Board of Directors of Fort Schuyler, the Buffalo Developer, along with another company (the "Second Buffalo Developer"), was chosen as the preferred developer for CNSE in Buffalo.

c. ALAIN KALOYEROS, a/k/a "Dr. K," the defendant, officially "recused" himself from the votes and accordingly he did not officially vote to select either the Syracuse Developer or the Buffalo Developer. I believe KALOYEROS did so in order to continue to deceive the other members of the Fort Schuyler Board of Directors into believing that the bidding process was fair, open, and competitive, when in fact KALOYEROS had manipulated the process so that the Syracuse Developer and the Buffalo Developer would be chosen regardless of whether KALOYEROS was involved in the voting.

87. Based on my review of emails and publicly available documents, and interviews of, among others, Howe and employees of CNSE and its affiliated entities, I learned, among other things, that in or around March 2014, without any further RFP process, the Buffalo Developer was chosen over the Second Buffalo Developer -- and without further competition from other interested developers -- to receive a contract worth approximately $225 million for the Riverbend Project.[13] In or around 2014, the contract for the Riverbend project was expanded to be worth approximately $750 million.

---

[13] The Second Buffalo Developer received a contract worth approximately $25 million for another project in Buffalo, New York.

V. FALSE STATEMENTS BY AIELLO AND GERARDI

88. On or about June 21, 2016, STEVEN AIELLO and JOSEPH GERARDI, the defendants, each met with law enforcement agents and prosecutors at the United States Attorney's Office. AIELLO and GERARDI were represented by counsel, and each spoke with the Government pursuant to a proffer agreement that protected each of them from having his statements used against him except, among other things, insofar as he lied and was accordingly charged with making false statements. Before the proffers, the Government informed counsel that AIELLO and GERARDI were subjects of the Government's investigation, and warned them that the Government believed that statements that AIELLO had previously made to the FBI, which were consistent with the statements described below, were false. During their respective proffer sessions, AIELLO and GERARDI were warned repeatedly that if they told any lies, they could be charged with a federal crime. Moreover, both AIELLO and GERARDI were told that their respective stories did not appear to be credible, and they were given multiple opportunities to tell the truth. During these meetings, AIELLO and GERARDI made the following statements, which I believe to be false, based on the facts set forth above:

a. AIELLO and GERARDI each separately stated that, after AIELLO was approached by Howe in or around late spring 2014 to ask whether AIELLO would be interested in hiring JOSEPH PERCOCO, a/k/a "Herb," the defendant, to work for the Syracuse Developer, AIELLO spoke with GERARDI and they both decided not to hire or make payments to PERCOCO. Furthermore, AIELLO and GERARDI each separately stated that they did not pay PERCOCO approximately $35,000 by sending money to Howe's shell company bank account, and they each separately stated that they had no knowledge that Howe had paid PERCOCO, and that they never authorized Howe to do so. I believe, based on my review of emails and interviews of, among others, Howe, and as further described above, that these statements were false because AIELLO and GERARDI agreed to and did pay PERCOCO and deliberately did so through Howe's LLC in order to disguise the fact that the Syracuse Developer was making payments to PERCOCO.

b. AIELLO and GERARDI each separately stated that Howe never asked them to make campaign contributions. I believe, based on my review of emails and interviews of, among others, Howe, and as further described above, that these statements were false because

Howe did in fact advise AIELLO and GERARDI to make certain campaign contributions.

c. GERARDI stated that Howe sent the Draft Syracuse RFP to him and AIELLO in order for the Syracuse Developer to help Howe and his associated Law Firm draft a broader, more open RFP so that other companies could compete to be the preferred developer, even though drafting the RFP in this way would hurt the Syracuse Developer. GERARDI further stated that when he wrote "too telegraphed?" next to a portion of the Draft Syracuse RFP that matched, verbatim, language from the Syracuse Developer Qualifications, he meant that the section in the Draft Syracuse RFP was too narrow and should be made broader to allow other developers to apply. I believe, based on my review of emails and interviews of, among others, Howe, and as further described above, that these statements were false because AIELLO and GERARDI conspired with others to tailor the Syracuse RFP to benefit the Syracuse Developer.

WHEREFORE, deponent respectfully requests that warrants be issued for the arrests of 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, and that they be imprisoned or bailed, as the case may be.

DELEASSA PENLAND
Criminal Investigator
United States Attorney's Office
Southern District of New York

Sworn to before me this
20th day of September, 2016

THE HONORABLE GABRIEL W. GORENSTEIN
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK

Daniel Charles Richman

From: Daniel Charles Richman
Sent: Friday, February 03, 2017 5:00 PM
To: [redacted](DO) (FBI) b6 1, 4 b7C 1, 4
Subject: Re: Professor Richman's contact(s)

https://www.justice.gov/usao-sdny/pr/nine-defendants-including-joseph-percoco-former-executive-deputy-secretary-governor-and
thx
d

On Fri, Feb 3, 2017 at 4:16 PM, Daniel Charles Richman <[redacted]> wrote:

Thx. May be a bit after 4:30. This meeting is interminable

Daniel Richman
Paul J. Kellner Professor of Law
Columbia Law School
Office: [redacted]
Cell: [redacted]

> On Feb 3, 2017, at 3:24 PM, [redacted] (DO) (FBI) [redacted] wrote: b6 1 b7C 1 b7E 3
>
> Prof Richman: Dan, thank you for the reply. Yes, 4:30 good for me. I'm here in the office until 6pm if you're not able to talk right then. You're also welcome to call me at any time on my work cell; listed below.
>
> -[redacted]
>
> -----Original Message-----
> From: Richman, Daniel C. (DO) (OGA)
> Sent: Friday, February 03, 2017 12:51 PM
> To: [redacted] (DO) (FBI) <[redacted]>; Rybicki, James E. (DO) (FBI) [redacted] b6 1, 4 b7C 1, 4 b7E 3
> Cc: [redacted] (DO) (FBI) <[redacted]>
> Subject: Re: Professor Richman's contact(s)
>
> Hi [redacted]- Thanks for reaching out. Would you be free to talk at 4:30 today? (I have an awful faculty mtg most of the afternoon). More generally, a quick way to reach me is my school email [redacted] or my cell [redacted] or my office [redacted] thx dan r

> 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)
>

> 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] b6 1 b7C 1
>
> [redacted]
> Chief, Ethics and Integrity Unit (EIU)
> Office of Integrity and Compliance (OIC)
> Desk [redacted] Mobile [redacted]
>
>
>
> --
> BEGIN-ANTISPAM-VOTING-LINKS
> ---------- ----------
>
> Teach Email if this mail (ID 01SEknXnD) is spam:
> Spam: https://antispam.law.columbia.edu/canit/b.php?i=01SEknXnD&m=c3cbf031da39&t=20170203&c=s
> Not spam: https://antispam.law.columbia.edu/canit/b.php?i=01SEknXnD&m=c3cbf031da39&t=20170203&c=n
> Forget vote: https://antispam.law.columbia.edu/canit/b.php?i=01SEknXnD&m=c3cbf031da39&t=20170203&c=f
> ---------- ----------
> END-ANTISPAM-VOTING-LINKS
>

--
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

[redacted] (DO) (FBI) b6 1 b7C 1

From: [redacted] (DO) (FBI)
Sent: Saturday, February 04, 2017 6:33 PM
To: [redacted] (DO) (OGA)
Subject: RE: Professor Richman re U.S. v. Percoco

Right now I'm available any time Monday afternoon. Please let me know if you would like to also meet with AD Kelley, too. If so, his schedule shows he would be available 1:30-2pm, or any time after 3pm; although that window tends to get filled throughout the day. I can send an invite now, or first thing Monday morning, if you can let me know. If with Pat, as you may know he's in the AD corridor [redacted]. If just with me, I can come to your office, or meet at mine [redacted]. Thanks.

From: [redacted] (DO) (OGA) b6 1, 4 b7C 1, 4 b7E 3
Sent: Saturday, February 04, 2017 5:04 PM
To: [redacted] (DO) (FBI) [redacted] Richman, Daniel C. (DO) (OGA) [redacted]
Cc: Kelley, Patrick W. (DO) (FBI) [redacted] (DO) (FBI) [redacted]
Subject: RE: Professor Richman re U.S. v. Percoco

Thank you [redacted] I think a quick conversation Monday afternoon might be helpful, if there is a time that suits you.

-

-------- Original message --------
From: [redacted] (DO) (FBI)" [redacted]
Date: 2/4/17 3:21 PM (GMT-05:00)
To: [redacted] (DO) (OGA)" [redacted] "Richman, Daniel C. (DO) (OGA)" [redacted] b6 1, 4 b7C 1, 4 b7E 3
Cc: "Kelley, Patrick W. (DO) (FBI)" [redacted] (DO) (FBI)" [redacted]
Subject: Professor Richman re U.S. v. Percoco

[redacted] good afternoon. By all means, we can discuss at your convenience, including today if you happen to see this message. My contacts are also below. I'm in the office now and foreseeably a bit longer, and also will have my Bureau mobile. If you prefer, I can also continue to correspond via UNET email.

I talked with Prof. Richman last night, who was planning to call and apprise you; so I thought best to add him here, too. I've also copied my boss OIC AD Pat Kelley, who as you may know is the FBI's Deputy Designated Agency Ethics Official (DDAEO), and ethics attorney [redacted] who has been assisting on this matter, as well as communicating with Prof. Richman. [redacted] and I discussed this matter with Pat late last Thursday.

The gist is that while there appears to be no 18 U.S.C. §§ 203 or 205 concerns, since Prof. Richman has not worked more than 60 days as a Special Government Employee (SGE) for the FBI in the last 365 days, there is

still the issue of "outside employment" which means any form of employment involving "personal services," whether or not for compensation. The DOJ Supplemental Regulations (5 C.F.R. § 3801.106) restricts Department employees, including SGEs, from engaging in outside employment that, per Subsection (b)(1) involves: (i) the practice of law, unless uncompensated and in the nature of community service or on behalf of yourself, your parents, spouse or children; (ii) any criminal or habeas corpus matter, be it Federal, State, or local; or, (iii) litigation, investigations, grants or other matters in which the Department of Justice is or represents a party, witness, litigant, investigator or grant-maker. Professor Richman's role as "part of the joint defense team" (per the Engagement Letter he provided us) in the case of *U.S. v. Percoco*, involves the practice of law, a criminal matter, and litigation in which the DOJ is a party; per the attached indictment.

Although the DOJ/JMD/DEO summary of the SGE ethics rules (https://www.justice.gov/jmd/summary-government-ethics-rules-special-government-employees) states: "[t]hese prohibitions may be waived by the Deputy Attorney General and generally are waived in the case of a special government employee ..." -- at this time we do not have a waiver. Moreover, it is not necessarily a given that a waiver would be granted for this particular matter. To assist all parties with this determination, we have contacted the NY field office for any additional information on the FBI's interests in this case. Meanwhile, we have recommended that Prof. Richman not be involved with the defense team until we can better determine whether a waiver will or will not be granted. We should know more, hopefully definitively, by the end of next week.

Please let us know if you have any questions, or if you would like to meet to discuss further by phone or in person. Thank you.

[redacted]

-----Original Message-----
From: [redacted] (DO) (OGA) b6 1
Sent: Friday, February 03, 2017 6:23 PM b7C 1
To: [redacted] (DO) (FBI); [redacted] b7E 3
Subject: Re:

[redacted]

Your message below was forwarded to me by Jim Rybicki to follow up. Could we set up a time for a quick phone call to get me up to speed on Dan Richman's status early next week sometime?

Thanks.

[redacted]
Special Counsel to the Director
Federal Bureau of Investigation

From: [redacted] (DO) (FBI) b6 1
Sent: Friday, February 3, 2017 9:35 AM b7C 1
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.

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

[redacted]

Chief, Ethics and Integrity Unit (EIU)
Office of Integrity and Compliance (OIC)
Desk [redacted] Mobile: [redacted]

[redacted] (DO) (FBI)

From: [redacted] (DO) (FBI)
Sent: Sunday, February 05, 2017 12:03 AM
To: [redacted] (DO) (OGA)
Subject: RE: Professor Richman re U.S. v. Percoco

b6 1
b7C 1
b7E 3

Will do.

From: [redacted] (DO) (OGA)
Sent: Saturday, February 04, 2017 11:25 PM
To [redacted] (DO) (FBI) [redacted]
Subject: RE: Professor Richman re U.S. v. Percoco

How about 3:30 with AD Kelley?

.

-------- Original message --------
From: [redacted] (DO) (FBI)" [redacted]
Date: 2/4/17 6:32 PM (GMT-05:00)
To: [redacted] (DO) (OGA)" [redacted]
Subject: RE: Professor Richman re U.S. v. Percoco

Right now I'm available any time Monday afternoon. Please let me know if you would like to also meet with AD Kelley, too. If so, his schedule shows he would be available 1:30-2pm, or any time after 3pm; although that window tends to get filled throughout the day. I can send an invite now, or first thing Monday morning, if you can let me know. If with Pat, as you may know he's in the AD corridor (rm 7149). If just with me, I can come to your office, or meet at mine (7441). Thanks.

b6 1, 4
b7C 1, 4
b7E 3

From: [redacted] (DO) (OGA)
Sent: Saturday, February 04, 2017 6:04 PM
To: [redacted] (DO) (FBI) [redacted]; Richman, Daniel C. (DO) (OGA)
[redacted]
Cc: Kelley, Patrick W. (DO) (FBI) [redacted] (DO) (FBI)
[redacted]
Subject: RE: Professor Richman re U.S. v. Percoco

Thank you [redacted] I think a quick conversation Monday afternoon might be helpful, if there is a time that suits you.

.

-------- Original message --------
From: [redacted] (DO) (FBI)" [redacted] b6 1, 4 b7C 1, 4 b7E 3
Date: 2/4/17 3:21 PM (GMT-05:00)
To: [redacted] (DO) (OGA) [redacted] "Richman, Daniel C. (DO) (OGA)" [redacted]
Cc: "Kelley, Patrick W. (DO) (FBI) [redacted] DO) (FBI)" [redacted]
Subject: Professor Richman re U.S. v. Percoco

[redacted] good afternoon. By all means, we can discuss at your convenience, including today if you happen to see this message. My contacts are also below. I'm in the office now and foreseeably a bit longer, and also will have my Bureau mobile. If you prefer, I can also continue to correspond via UNET email.

I talked with Prof. Richman last night, who was planning to call and apprise you; so I thought best to add him here, too. I've also copied my boss OIC AD Pat Kelley, who as you may know is the FBI's Deputy Designated Agency Ethics Official (DDAEO), and ethics attorney [redacted] who has been assisting on this matter, as well as communicating with Prof. Richman. [redacted] and I discussed this matter with Pat late last Thursday. b6 1 b7C 1

The gist is that while there appears to be no 18 U.S.C. §§ 203 or 205 concerns, since Prof. Richman has not worked more than 60 days as a Special Government Employee (SGE) for the FBI in the last 365 days, there is still the issue of "outside employment" which means any form of employment involving "personal services," whether or not for compensation. The DOJ Supplemental Regulations (5 C.F.R. § 3801.106) restricts Department employees, including SGEs, from engaging in outside employment that, per Subsection (b)(1) involves: (i) the practice of law, unless uncompensated and in the nature of community service or on behalf of yourself, your parents, spouse or children; (ii) any criminal or habeas corpus matter, be it Federal, State, or local; or, (iii) litigation, investigations, grants or other matters in which the Department of Justice is or represents a party, witness, litigant, investigator or grant-maker. Professor Richman's role as "part of the joint defense team" (per the Engagement Letter he provided us) in the case of *U.S. v. Percoco*, involves the practice of law, a criminal matter, and litigation in which the DOJ is a party; per the attached indictment.

Although the DOJ/JMD/DEO summary of the SGE ethics rules (https://www.justice.gov/jmd/summary-government-ethics-rules-special-government-employees) states: "[t]hese prohibitions may be waived by the Deputy Attorney General and generally are waived in the case of a special government employee ..." -- at this time we do not have a waiver. Moreover, it is not necessarily a given that a waiver would be granted for this particular matter. To assist all parties with this determination, we have contacted the NY field office for any additional information on the FBI's interests in this case. Meanwhile, we have recommended that Prof. Richman not be involved with the defense team until we can better determine whether a waiver will or will not be granted. We should know more, hopefully definitively, by the end of next week.

Please let us know if you have any questions, or if you would like to meet to discuss further by phone or in person. Thank you.

[redacted] b6 1 b7C 1 b7E 3

-----Original Message-----
From: [redacted] (DO) (OGA)
Sent: Friday, February 03, 2017 6:23 PM
To: [redacted] (DO) (FBI) [redacted]
Subject: Re:

[redacted]

Your message below was forwarded to me by Jim Rybicki to follow up. Could we set up a time for a quick phone call to get me up to speed on Dan Richman's status early next week sometime?

Thanks.

[redacted]
Special Counsel to the Director
Federal Bureau of Investigation

b6 1
b7C 1

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)

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

[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: Monday, February 06, 2017 10:29 AM
To: [redacted] (DO) (FBI)
Subject: RE: Professor Richman re U.S. v. Percoco

Forgot to ask, could you bring a copy of the referenced engagement letter this afternoon? Thanks.

From: [redacted] (DO) (FBI)
Sent: Saturday, February 04, 2017 3:21 PM
To: [redacted] (DO) (OGA) [redacted]; Richman, Daniel C. (DO) (OGA) [redacted]
Cc: Kelley, Patrick W. (DO) (FBI) [redacted] (DO) (FBI) [redacted]
Subject: Professor Richman re U.S. v. Percoco

b6 1, 4
b7C 1, 4
b7E 3

[redacted] good afternoon. By all means, we can discuss at your convenience, including today if you happen to see this message. My contacts are also below. I'm in the office now and foreseeably a bit longer, and also will have my Bureau mobile. If you prefer, I can also continue to correspond via UNET email.

I talked with Prof. Richman last night, who was planning to call and apprise you; so I thought best to add him here, too. I've also copied my boss OIC AD Pat Kelley, who as you may know is the FBI's Deputy Designated Agency Ethics Official (DDAEO), and ethics attorney [redacted] who has been assisting on this matter, as well as communicating with Prof. Richman [redacted] and I discussed this matter with Pat late last Thursday.

b6 1
b7C 1

The gist is that while there appears to be no 18 U.S.C. §§ 203 or 205 concerns, since Prof. Richman has not worked more than 60 days as a Special Government Employee (SGE) for the FBI in the last 365 days, there is still the issue of "outside employment" which means any form of employment involving "personal services," whether or not for compensation. The DOJ Supplemental Regulations (5 C.F.R. § 3801.106) restricts Department employees, including SGEs, from engaging in outside employment that, per Subsection (b)(1) involves: (i) the practice of law, unless uncompensated and in the nature of community service or on behalf of yourself, your parents, spouse or children; (ii) any criminal or habeas corpus matter, be it Federal, State, or local; or, (iii) litigation, investigations, grants or other matters in which the Department of Justice is or represents a party, witness, litigant, investigator or grant-maker. Professor Richman's role as "part of the joint defense team" (per the Engagement Letter he provided us) in the case of *U.S. v. Percoco*, involves the practice of law, a criminal matter, and litigation in which the DOJ is a party; per the attached indictment.

<< File: US v Percoco et al Indictment - Foreperson Signed (1).pdf >>

Although the DOJ/JMD/DEO summary of the SGE ethics rules (https://www.justice.gov/jmd/summary-government-ethics-rules-special-government-employees) states: "[t]hese prohibitions may be waived by the Deputy Attorney General and generally are waived in the case of a special government employee ..."

-- at this time we do not have a waiver. Moreover, it is not necessarily a given that a waiver would be granted for this particular matter. To assist all parties with this determination, we have contacted the NY field office for any additional information on the FBI's interests in this case. Meanwhile, we have recommended that Prof. Richman not be involved with the defense team until we can better determine whether a waiver will or will not be granted. We should know more, hopefully definitively, by the end of next week.

Please let us know if you have any questions, or if you would like to meet to discuss further by phone or in person. Thank you.

[redacted]

-----Original Message-----
From: [redacted] DO) (OGA)
Sent: Friday, February 03, 2017 6:23 PM
To: [redacted] (DO) (FBI) [redacted]
Subject: Re:

b6 1
b7C 1
b7E 3

[redacted]

Your message below was forwarded to me by Jim Rybicki to follow up. Could we set up a time for a quick phone call to get me up to speed on Dan Richman's status early next week sometime?

Thanks.

[redacted]
Special Counsel to the Director
Federal Bureau of Investigation

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]

b6 1
b7C 1

[redacted]

Chief, Ethics and Integrity Unit (EIU)
Office of Integrity and Compliance (OIC)
Desk: [redacted]; Mobile [redacted]

[redacted] b6 1, 2 b7C 1, 2

From: [redacted]
Sent: Thursday, January 05, 2017 1:39 PM
To: Oconnell, Sasha C. (DO) (FBI); Daniel Charles Richman; [redacted] (OGC) (FBI)
Subject: CNAS Surveillance Policy report
Attachments: CNAS-Report-Surveillance-Final.pdf

Sasha, Dan, and [redacted]

I hope this finds you well. I wanted to make sure that you received our final Surveillance Policy report, particularly given how generous you were with your time and perspectives during the project.

The final report is attached here as a pdf. Below I've also included links to a Lawfare post I did to coincide with our rollout event in December and an op-ed I had in Politico yesterday on the future of the PCLOB.

https://lawfareblog.com/surveillance-policy-trump-administration

http://www.politico.com/agenda/story/2017/01/privacy-board-trump-national-security-000264

Many thanks again for all of your help with the project. I hope to see each of you again soon.

All the best,

[redacted] b6 2 b7C 2

—

[redacted]
Senior Fellow
Center for a New American Security
1152 15th Street NW, Suite 950
Washington, DC 20009
https://www.cnas.org/

[redacted]
[redacted] - mobile
- office

SURVEILLANCE POLICY

A Pragmatic Agenda for 2017 and Beyond

Adam Klein, Michèle Flournoy, and Richard Fontaine

Center for a
New American
Security

About the Authors

ADAM KLEIN is a Senior Fellow at the Center for a New American Security (CNAS). His research centers on the intersection of national security policy and law, including government surveillance in the digital age, counterterrorism, and rules governing the use of military force. Before coming to CNAS, Klein served as a law clerk to Justice Antonin Scalia of the U.S. Supreme Court and Judge Brett M. Kavanaugh of the U.S. Court of Appeals for the D.C. Circuit and was a Senior Associate at WilmerHale, an international law firm. Klein has also worked on national security policy at the RAND Corporation and the 9/11 Public Discourse Project, the nonprofit successor to the 9/11 Commission. He began his career as a legislative assistant in the office of U.S. Rep. C.W. "Bill" Young. His work on this project was supported in substantial part by a Council on Foreign Relations International Affairs Fellowship.

MICHÈLE FLOURNOY is Co-Founder and Chief Executive Officer of the Center for a New American Security. She served as Under Secretary of Defense for Policy from February 2009 to February 2012. She was the principal advisor to the Secretary of Defense in the formulation of national security and defense policy, oversight of military plans and operations, and in National Security Council deliberations. She led the development of the Department of Defense's (DoD's) 2012 Strategic Guidance and represented the department in dozens of foreign engagements, in the media, and before Congress. Prior to confirmation, Flournoy co-led Barack Obama's transition team at DoD.

RICHARD FONTAINE is President of the Center for a New American Security. He served as a Senior Advisor and Senior Fellow at CNAS from 2009–2012 and previously as foreign policy advisor to Sen. John McCain for more than five years. Fontaine has also worked at the State Department, the National Security Council, and on the staff of the Senate Foreign Relations Committee. Fontaine served as foreign policy advisor to the McCain 2008 presidential campaign and, after the election, as the minority deputy staff director on the Senate Armed Services Committee. Prior to this, he served as Associate Director for Near Eastern Affairs at the National Security Council from 2003–04. He also worked in the NSC's Asian Affairs directorate, where he covered Southeast Asian issues.

Acknowledgments

The authors are grateful to the dozens of experts from the technology, national security, and privacy communities who offered their expertise and insights to inform this work. The authors would also like to thank Loren DeJonge Schulman and Neal Urwitz for their insightful comments on our draft and Maura McCarthy and Melody Cook for, respectively, their editorial guidance and graphic design.

Readers should note that some project participants were affiliated with organizations that support CNAS financially. CNAS maintains a broad and diverse group of more than 100 funders, including private foundations, government agencies, corporations, and private individuals, and retains sole editorial control over its ideas, projects, and publications. A complete list of our financial supporters can be found at www.cnas.org/support-cnas/cnas-supporters.

The authors are solely responsible for the analysis and recommendations in this report.

About the Series

The Papers for the Next President series is designed to assist the next president and his or her team in crafting a strong, pragmatic, and principled national security agenda. The series explores the most critical regions and topics that the next president will need to address early in his or her tenure and will include actionable recommendations designed to be implemented during the first few months of 2017.

Cover Photo
Matthew Henry/Unsplash

SURVEILLANCE POLICY

A Pragmatic Agenda for 2017 and Beyond

Executive Summary

Today, the United States faces a more diverse, more complex array of national security threats than ever before. With ever more human activity taking place on electronic networks, surveillance is an essential tool for protecting the nation from these threats. The American people are fortunate to have a world-leading intelligence community, with a mission-oriented workforce operating under a robust legal and oversight regime. At the same time, the intelligence community's immense capabilities and necessary secrecy raise inevitable and important questions for individual privacy, the rule of law, and public accountability.

In late 2014, the Center for a New American Security began a two-year initiative aimed at developing a new approach to surveillance policy for the next administration. As part of this project, CNAS has held 14 expert workshops and roundtables and conducted more than 80 private conversations and interviews with leaders in the national security, privacy, and technology communities. These experts' participation was invaluable in informing this report; the views expressed here, however, are our own.

While the leaks by former National Security Agency contractor Edward Snowden violated the law and harmed ongoing intelligence-gathering efforts, they also represented a watershed moment in the debate over government surveillance in the digital age. The leaks revealed that the scale of government data collection – even lawful, court-approved data collection – was orders of magnitude greater than most Americans had believed. And the leaks created the impression around the world (fostered in some cases by imprecise media reports) that the United States was indiscriminately collecting the personal data of ordinary people.

Three years after the leaks, their effects continue to reverberate across the policy landscape. The post-Snowden backlash has impeded law enforcement and intelligence gathering, harmed the U.S. technology industry's competitiveness in international markets, and created diplomatic friction with important allies. Most importantly, many Americans remain skeptical that their government respects their digital privacy.

Since 2013, the executive branch and Congress have attempted to repair the damage by making important reforms to surveillance practices and legal authorities. These include:

- President Obama's Review Group on Intelligence and Communications Technologies, many of whose recommendations have become law or policy, and whose balanced, thoughtful report remains an important touchstone for surveillance policy.
- Presidential Policy Directive 28 (PPD-28), which, most notably, required U.S. signals-intelligence (SIGINT) practices to consider the privacy interests of non-Americans overseas – a commitment still unequaled by any other country.
- The USA Freedom Act, which ended the NSA's bulk collection of Americans' telephone call records and adopted a number of important, but underappreciated, measures to enhance transparency in government surveillance.
- The intelligence community's unprecedented efforts to explain its work, and the robust legal and compliance regime under which it operates, directly to the American people.
- The emergence of the Privacy and Civil Liberties Oversight Board (PCLOB) as a visible, energetic, public-facing, and credible independent evaluator of key surveillance programs.

While these changes are a strong beginning, they cannot be the end, for several reasons. They are not widely known overseas; indeed, given the technical and bureaucratic nature of many of the changes, they are unknown even to most Americans. The post-Snowden focus on collection of Americans' personal data, while understandable, overshadowed other important issues, such as outreach to foreign publics and the challenges facing the U.S. technology sector. Finally, these successes are fragile. New leaks could rekindle latent skepticism and mistrust. Some changes, such as PPD-28 and the intelligence community's transparency efforts, could be rolled back by a new president or altered by new legislation.

For these reasons, surveillance reform should be seen as a work in progress rather than a finished product. The agenda we propose would take the next step toward rebuilding trust with the American people, the technology industry, and partners and publics abroad. It would enable the new administration to speak with one voice in support of a pragmatic, privacy-enhancing agenda. It would make clear to foreign populations that their countries and the United States share basic values on data privacy and surveillance. It would safeguard the United States' enviable position as the world leader in information technology. It would help inoculate the new administration against the risk of future unauthorized disclosures. And it would further these goals while preserving needed national security capabilities.

Six Principles for Pragmatic Surveillance Policy

Six basic premises underlie our pragmatic approach to surveillance policy:

1. The next president and Congress should take meaningful steps both to enhance Americans' digital privacy and to reassure the American people that government surveillance is consistent with American values and the rule of law. Protection from unwarranted government intrusion into personal privacy is a bedrock element of American liberty. But greater transparency about surveillance practices is also needed to shore up public faith in government institutions. When the public learns that government surveillance practices dramatically outstrip what laws and the statements of government officials would lead a reasonable observer to believe, it erodes faith in governing institutions, with corrosive and dangerous long-term effects for U.S. democracy.
2. A thriving, world-leading American technology industry is in the United States' economic interest. It also benefits U.S. intelligence and counterterrorism efforts. Millions of American jobs rely on the information-technology industry, and tech is a vital and growing export sector. But the benefits of technological pre-eminence are not economic alone: U.S. law enforcement, counterterrorism, and intelligence efforts also benefit from the fact that much of the world's data is stored on U.S. soil and much of the world's internet traffic passes through the United States. Unfortunately, in the wake of the Snowden revelations, other governments have begun taking regulatory steps to align the storage and transfer of their citizens' data with physical borders. Below, we recommend various steps to help slow or reverse this trend.
3. Signals-intelligence collection and analysis are vital national security tools. The United States will and should continue to maintain world-leading SIGINT capabilities. Dramatically curtailing the government's electronic surveillance capabilities is neither prudent from a national security perspective nor politically realistic. No president could responsibly surrender vital, lawful national security capabilities at a time of serious threat to the nation.
4. Improving public and foreign trust on surveillance and digital-privacy issues is an important goal, but no reform agenda can dispel completely the aftereffects of the Snowden leaks. The heightened skepticism and expectation of transparency that the Snowden leaks created will not simply disappear. Rather, they are features of the new landscape, and policymakers and the intelligence community will have to acknowledge and adapt to them.
5. The oft-employed metaphor of "balance" between civil liberties and security is a poor guide for optimizing surveillance policy. In a time of diverse national security threats, Americans will demand robust counterterrorism, law enforcement, and intelligence capabilities to secure the homeland. They will also insist on safeguards for personal privacy and fidelity to the rule of law. The answer is not to choose between security or liberty but to work toward both. A focus on zero-sum tradeoffs between privacy and security deters security officials from embracing a privacy-enhancing reform agenda and assumes incorrectly that surrendering some amount of one value automatically yields a concomitant benefit for the other.
6. Signals intelligence and the powers of the NSA are not neatly severable from other issues affecting domestic and international data privacy. In practice, issues that experts would consider only loosely related to signals intelligence – such as debates over iPhone encryption and whether the government needs a warrant to read Americans' email – powerfully influence Americans' willingness to entrust the government with collecting, monitoring, and analyzing communications and user data. A pragmatic surveillance-policy agenda must not artificially exclude other data-privacy issues that are highly salient to the public and where constructive reform is possible.

The Case for Pragmatic Surveillance Reform

The next administration has an opportunity to refresh the narrative surrounding the U.S. government's approach to surveillance and digital privacy – if it acts proactively. But this opportunity is perishable. As the new president's term unfolds, other controversies and crises will inevitably arise, making it far harder for the administration to dictate the policy agenda. And reforms undertaken reactively after a crisis tend to garner less public goodwill than those enacted before a crisis occurs.

Some might argue in favor of a bold, controversial surveillance-policy agenda – whether reformist (such as allowing the FISA Amendments Act to sunset) or security-driven (such as pushing aggressively for decryption legislation). Yet either course would be both impracticable and inadvisable for a new administration. The new president's first actions, if divisive, will consume the president's political capital and harden political opposition. In addition, the public will hold the new administration responsible for any terrorist attacks that occur on its watch. By contrast, the agenda we outline below would expand the new president's political capital, earn public support and bipartisan credibility, and to some extent inoculate the president against a backlash should there be future unauthorized disclosures.

A new administration would be best served by announcing the measures recommended in this report as a unitary reform agenda rather than simply farming them out to various parts of the government for quiet implementation. The reforms will be more effective as a restorative tonic for past breaches of trust if they are widely known. And a major initiative, publicly promoted by the White House, will more effectively define the new administration in the public mind as serious about Americans' digital privacy than a series of atomized technical changes quietly implemented by the bureaucracy.

By doing so, the next president can seize the near-term – and possibly unique –opportunity to repair the various deficits in trust that have emerged in the wake of the NSA disclosures. In so doing, the government can ensure respect for critical civil liberties, protect national security, and bolster the strength of the American economy. The window for action will not remain open indefinitely; the time to act is now.

The National Security Agency's headquarters at Fort George G. Meade, in Maryland. (NSA)

Recommendations

A. STRENGTHENING PUBLIC TRUST

Email Privacy and Government Access to Other Personal Data

1. If the Email Privacy Act does not pass during the 114th Congress, the next president should, in the first 100 days of the new administration, call for legislation (i) requiring a warrant to obtain the content of email and documents stored in the cloud and (ii) imposing reasonable limits on nondisclosure orders.
2. The new administration should launch a White House initiative to propose standards for government access to other types of sensitive data, such as cell-site location data, data generated by "internet of things" devices, license-plate readers, facial recognition systems, and other foreseeable technologies with significant implications for personal privacy.

Intelligence Transparency and Secret Law

3. The NSA should expand its efforts to demystify the agency's work in the mind of the general public.
4. Senior leaders should not hesitate to defend the many valid purposes of signals intelligence beyond counterterrorism. Limiting the public defense of SIGINT to counterterrorism alone invites a backlash when uses other than counterterrorism are revealed.
5. The next president should publicly embrace the principle that all domestic surveillance and surveillance of Americans overseas will be based on clear statutory authority, publicly interpreted, with sufficient oversight to hold the government to its construction of the statute.
6. The president should task the general counsels of the Office of the Director of National Intelligence, NSA, FBI, and CIA, and the Assistant Attorney General for National Security, in consultation with the PCLOB, with proposing, within six months, other ways to reduce the amount of classified legal interpretation and programmatic guidance governing electronic surveillance. This could include, where consistent with national security, further declassification of relevant presidential directives, agency procedures, interagency memoranda of understanding, opinions of the Justice Department's Office of Legal Counsel, and classified annexes to legislation.
7. Even those documents in these categories that cannot be safely declassified and published should be shared, in a manner consistent with their classification and to the extent permitted by executive privilege, with the congressional intelligence committees.

Section 702

8. Section 702 should be reauthorized, but with reforms to enhance public confidence, transparency, and privacy.
9. The FBI should publicly explain with greater precision why it needs to search databases containing 702 information for data about U.S. persons.
10. The FBI should consider, and explain, whether it would be sufficient for it to continue to query databases containing 702 data for U.S.-person identifiers but, where such a search returns 702 information, to receive only the responsive metadata rather than the content.
11. Congress, as a condition of reauthorization, should mandate further transparency about several aspects of the 702 program:
    - » Require and enable NSA to fully implement Recommendation 9 from the PCLOB's report on Section 702.
    - » Estimate the overall scale of incidental collection, if a valid and practicable methodology can be found.
    - » Publish annually the number of instances in which an FBI query in an investigation unrelated to national security returns 702 information about a U.S. person.
    - » Estimate the total number of U.S.-person queries of databases containing 702 data conducted by the FBI in non-national-security criminal investigations.
    - » Provide more detail about which cybersecurity offenses the Department of Justice considers "serious crimes" for which it will use 702-derived information in a criminal proceeding.
    - » Publish the Justice Department's standard for determining whether evidence introduced in a criminal proceeding is "derived from" 702 information.
    - » Mandate the appointment of an amicus curiae in 702 certification proceedings.
    - » Provide to the public as much detail as possible about the national security value of Section 702.

The Privacy and Civil Liberties Oversight Board

12. The next president should swiftly appoint new members or reappoint existing members and work with the Senate to ensure that they are promptly confirmed.
13. Congress should pass legislation that permits the remaining members to collectively appoint staff in the absence of a chairman.
14. Congress should enact legislation exempting the Board from the Government in the Sunshine Act.
15. While is appropriate that the Board's activities focus on protecting the privacy rights of U.S. persons, Congress should not expressly restrict the Board's statutory jurisdiction to only the rights of U.S. persons.
16. Congress should not require the Board to keep the Director of National Intelligence or other elements of the intelligence community "fully and currently informed" of its activities.

Whistleblower Laws

17. The next president should issue an executive order making Presidential Policy Directive 19's whistleblower protections binding within the executive branch and clarifying that they extend to contractors working at all intelligence community components.
18. Congress should extend the full panoply of statutory whistleblower protections to contractors working in the intelligence community.
19. The next president should support legislation updating the FBI's whistleblower process in the next Congress.

B. PROTECTING A FLOURISHING TECHNOLOGY INDUSTRY

Encryption

20. Given the impasse over decryption legislation, and given that the debate itself has damaged relations between the government and the technology industry, the next administration should de-escalate the public debate over encryption.
21. The FBI should support its argument for an encryption mandate by publishing more data about the precise contours of the technical challenge posed by encryption.
22. To help the FBI cope with the status quo, Congress should scale up the FBI's resources for gaining access to encrypted devices and communications without compelled assistance from providers.
23. This scaling up should also include resources to enable the FBI to create a centralized repository of expertise and technical assistance for the 15,000 state and local law enforcement agencies in the United States.

Risk Management in SIGINT Decisions

24. Operations that, if exposed, would pose a significant risk to an American company or business sector should be approved by senior political appointees after a process that incorporates, to the greatest extent possible, external input about the scale of the risk.
25. The government should create regularized channels for candid communication between NSA and the technology industry, such as creating an industry advisory board of corporate officials who hold security clearances.
26. To the extent that a dialogue would, for some companies, raise concerns about appearing complicit in NSA practices, NSA should also establish a formalized one-way channel for receiving comment from American companies about the risks that signals-intelligence practices pose to their businesses and other issues of concern.
27. Where the U.S. government wishes to obtain data held by a U.S. company, it should generally seek to access the data through the "front door" provided by U.S. domestic law rather than through overseas intelligence operations or liaison relationships.
28. To the extent that the government contemplates operations that involve tampering with or introducing vulnerabilities into an American company's product before it reaches its end customer,[1] any such operations should be approved by the National Security Advisor with input, where appropriate, from the Deputy National Security Advisor for International Economic Affairs, or another senior official with analogous responsibilities.
29. The government should not, as a rule, pressure American technology companies to compromise their own products or hand over their source code.

30. The government should not pressure American companies that sell to the government to disclose to it vulnerabilities that the company discovers before the company discloses them to other customers.
31. The Vulnerabilities Equities Process should be formalized in an executive order.
32. The executive order should, to the maximum extent consistent with national security, list all agencies that have a say in the process and should specifically state which agencies have a vote on whether to retain or disclose a vulnerability.
33. In order to ensure that the process takes account of the broader interests of the U.S. technology sector, the Department of Commerce should have a regular seat at the table.
34. The executive order should also describe the process to be followed in deciding whether to retain or disclose a vulnerability. In particular, it should clearly state the government's substantive standard for deciding whether a vulnerability's potential national security benefits outweigh the risks of retaining it.
35. The executive order should also require that there be periodic review of whether a retained vulnerability should be disclosed.
36. The executive order should provide for public annual reports containing as much detail about the process's operation as is consistent with national security, along with a classified annex for the relevant congressional committees.

C. MITIGATING THE INTERNATIONAL CONSEQUENCES OF SURVEILLANCE POLICY

Surveillance Diplomacy and PPD-28

37. The next administration should offer to hold a political dialogue, among willing allies with similar rule-of-law cultures, on norms to govern surveillance of one another's citizens and institutions.
38. This dialogue should seek to exchange high-level, public, political (rather than legal) commitments analogous to the public commitments the United States has already made, most notably in PPD-28. For example, the United States should ask partners to mutually agree:
    - To incorporate in their signals-intelligence practices protections for the privacy interests of one another's citizens.
    - To publish, with the maximum detail consistent with national security, agency procedures implementing such protections, including minimization requirements limiting the dissemination and retention of personal information of one another's citizens.
    - To establish a presumptive time limit for retaining the personal information of one another's citizens.
    - To agree to limitations on the use of signals intelligence collected in bulk.
    - To designate a senior official to serve as a point of contact for implementation of these commitments and other concerns related to signals-intelligence practices.
    - To require individualized judicial approval for electronic surveillance of one another's citizens when on the other country's territory.
39. These discussions should also include mutual, public, high-level commitments about the purposes and boundaries of "liaison" cooperation between one another's intelligence services – in particular, the circumstances in which they will exchange information about one another's citizens.
40. In order to encourage allied governments to enter into such discussions and extend appropriate privacy protections to the American people, the United States should make clear to allied publics and their governments that while it is prepared to commit itself to protect their privacy, the American people's privacy deserves equivalent respect and it expects such protections to be reciprocated.
41. The next administration should reaffirm that PPD-28's basic recognition that signals-intelligence activities must consider the basic dignity and privacy of all people, and the fundamental commitments of Section 1 of PPD-28 (signals-intelligence activities must be be authorized by law; no use for discrimination or suppressing dissent; no espionage for commercial advantage of U.S. companies; narrow tailoring), will remain applicable to all countries and their citizens without regard to their own governments' policies.
42. The new administration should announce that after one year, the heightened commitments in PPD-28 Sections 2 and 4 will be guaranteed only to citizens of countries that agree to extend comparable protection to Americans. There is no reason why other countries, and particularly U.S. allies, should resist extending to Americans the same consideration that the U.S. government grants to their citizens.

43. The next administration should also offer to elevate these commitments to an executive order for countries that make credible reciprocal promises.

44. The United States should insist that European Union member states grant to Americans the same judicial-redress rights and access to a surveillance "ombudsperson" that the United States extended to Europeans under Privacy Shield.

45. The United States should demand that allied countries publicly commit not to spy on one another's nationals for the economic benefit of domestic companies – a practice the United States has long forsworn but some close allies have not.

46. The next administration should also make clear that it will consider excluding from any list of allied leaders whose personal communications are off-limits from surveillance the leaders of any country that refuses to publicly renounce such economic espionage against American companies.

47. The next administration and Congress should establish regularized, formal exchanges between congressional, judicial, and executive branch compliance and oversight bodies, including the Privacy and Civil Liberties Oversight Board, and their foreign counterparts.

Public Diplomacy

48. The United States should explain, in a modest and factual manner, the many ways in which the U.S. intelligence community supports Europe in its fight against terrorism.

49. The intelligence community should, with as much specificity as is consistent with national security, offer greater detail about how much and what kind of counterterrorism data the United States shares with European partners, as well as the types of information it receives from them.

50. The next administration should also consider raising the profile of joint counterterrorism efforts by making American ambassadors and senior national security officials available to discuss them with local media, and asking European counterparts to publicly acknowledge the cooperation.

Privacy Shield

51. While legal challenges are pending, U.S. officials should seek to foster a climate conducive to ensuring that Privacy Shield passes judicial muster.

52. This includes continuing to make the case that U.S. and European privacy protections are, at a minimum, "essentially equivalent."

53. U.S. officials should also seek to publicly reinforce the significance of the new ombudsperson mechanism and the Judicial Redress Act.

54. Consumer-protection officials should work to publicly demonstrate that Privacy Shield's consumer protections are being rigorously enforced.

55. American ambassadors in Europe and visiting U.S. government principals should be encouraged to highlight U.S. privacy protections and emphasize that in the United States, as in Europe, the right to privacy is a fundamental right.

56. The next administration should begin to consider what the United States' response will be, other than further concessions, if Privacy Shield is struck down.

57. It should also begin communicating quietly to European partners that while the United States respects their legal institutions, shares their values, and has taken every reasonable measure to help European partners satisfy the Court of Justice, the United States has a "Plan B" and will not respond to another flawed, *Schrems*-like decision with more unilateral concessions.

58. To amplify this message, Congress should consider legislation providing that if a judicial decision restricts data transfers from Europe to the United States, the same limitations will apply to data transfers from the United States to Europe by European companies.

Cross-Border Data Requests

59. If the Justice Department's proposal does not pass during the current Congress, the next administration should seek, and Congress should enact, similar legislation authorizing executive agreements on cross-border data requests.

60. Once the enabling legislation is enacted, the executive branch should move quickly to conclude executive agreements with countries with similar human-rights and rule-of-law standards.

61. Legislation creating an alternative to the Mutual Legal Assistance system should be accompanied by parallel efforts to streamline the existing system.

Introduction

In January 2014, President Obama delivered a landmark speech on signals intelligence at the Department of Justice. "Throughout American history," he noted, "intelligence has helped secure our country and our freedoms."[2] Today, intelligence community personnel work to protect the American people and U.S. allies from a range of threats – from terrorism to military aggression, from the theft of American trade secrets to the subversion of democratic institutions.

In the digital age, electronic surveillance is a necessary component of these efforts. Led by the National Security Agency (NSA), the intelligence community collects and analyzes signals intelligence subject to a system of "oversight, review, and checks-and-balances," which "reduce[s] the risk that elements of the Intelligence Community would operate outside of the law."[3] Yet even with these safeguards in place, these agencies' powerful capabilities and unavoidable secrecy pose serious challenges for individual privacy, public accountability, and democratic control.

The Snowden leaks broke the law and harmed ongoing intelligence operations, yet they produced a watershed moment in the public debate over government surveillance. Importantly, the leaked documents and the subsequent inquiry by the Review Group on Intelligence and Communications Technologies uncovered "no evidence of illegality or other abuse of authority [by the U.S. government] for the purpose of targeting domestic political activity."[4] At the same time, the leaks demonstrated that the scale of government data collection – even lawful, court-approved data collection – was much greater than most Americans would have believed given the available public information. They also created the impression around the world (fostered in some cases by inaccurate media reports) that the United States was indiscriminately collecting the personal data of ordinary people.

Three years after the Snowden disclosures, their effects continue to reverberate across the policy landscape and the U.S. technology industry. Many Americans remain skeptical of their own government's commitment to their digital privacy. Internationally, the widespread misperception that the NSA indiscriminately reads ordinary people's email and wiretaps their phone calls continues to harm American interests. This belief has triggered harmful policy responses abroad, endangering the cross-border data flows that are vital to the global business models of American technology companies. European consumers, companies, and governments continue to question the trustworthiness of American companies' products and services, undermining their competitive standing in foreign markets. The disclosures have damaged U.S. diplomatic ties, including with key allies. And they have undermined efforts by the U.S. government to promote global internet freedom and preserve the free flow of information online.

This status quo is harmful to U.S. diplomatic and economic interests overseas and corrodes faith in government institutions here at home. Despite the significant changes made to policy and messaging since the Snowden disclosures, the U.S. government has yet to adequately mitigate the negative fallout.

Fortunately, the authors believe that the next administration can materially improve upon the status quo on all three fronts – domestic, economic, and diplomatic – while preserving key national security capabilities. This report outlines *how* the next administration can do this and *why* doing so is both urgent and politically feasible.

Three years after the Snowden disclosures, their effects continue to reverberate across the policy landscape and the U.S. technology industry.

Beginning in late 2014, the Center for a New American Security (CNAS) began a two-year initiative aimed at developing a new approach to surveillance policy for the next administration. As part of this project, CNAS has held 14 expert workshops and roundtables and more than 80 private meetings and interviews with leaders in national security, privacy, and technology.

These consultations contributed directly to the analysis and recommendations we present below. They also persuaded us of six basic premises that underlie the pragmatic approach to surveillance policy that follows.

1. ***The next president and Congress should take meaningful steps to enhance Americans' digital privacy and reassure the public that government surveillance is consistent with American values and the rule of law.*** Protection from unwarranted government intrusion into personal privacy is a bedrock element of American liberty. That principle is given effect by the Constitution's Fourth Amendment, which protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." The American legal order presupposes that privacy is inherently valuable.

Personal privacy, however, is not the only important value at stake; greater transparency and improved oversight of government surveillance are also needed to strengthen the public's trust in government institutions.[5] Or, as the post-Snowden Review Group on Intelligence and Communications Technologies put it, surveillance policy should foster, not erode, "a general sense ... that the nation's practices and decisions are worthy of trust."[6] When the public learns that government surveillance practices dramatically outstrip what public laws and the statements of government officials would lead a reasonable observer to believe, it erodes faith in governing institutions, with corrosive and dangerous long-term effects for democracy.

2. *A thriving, world-leading American technology industry is in the United States' economic interest, but it also benefits U.S. intelligence and counterterrorism capabilities.* Technology has always been a key determinant of national power. But as digitization becomes ubiquitous in both commerce and national security, predominance in information technology (IT) will increasingly define which countries are seen as the world's economic and political leaders. Millions of American jobs already rely on the information-technology industry, and tech is a vital and growing export sector. It is also an immense source of economic and cultural influence for the United States. Lest there be any doubt about this industry's importance to modern economies, many other countries and foreign cities are desperately imitating Silicon Valley in the hopes of igniting their own startup booms.[7]

Recent controversies, such as the dispute between the Justice Department and Apple over an encrypted iPhone, have overshadowed the many national security benefits of being home to the world's leading technology industry. The most obvious is economic strength, a fundamental determinant of national power. Less obvious, but equally significant, are the advantages for U.S. intelligence, law enforcement, and defense[8] that derive from having much of the world's data stored on U.S. soil and much of the world's internet traffic pass across the United States. One powerful illustration of how valuable this is: The PRISM program – under which the government can obtain an intelligence target's data, if stored in the United States, directly from providers – was apparently the signals-intelligence activity most frequently cited in NSA's reporting. That U.S. companies hold this data trove yields enormous benefits for the intelligence community and law enforcement, and thus for the security of the United States.

Unfortunately, in the wake of the Snowden revelations, other governments have begun taking regulatory steps to align the storage and transfer of their citizens' data with physical borders. This movement will only abate if the United States can persuade foreign governments and users that their data held by U.S. companies is protected by an adequate legal regime, and that this regime is comparable or superior to that in their home countries. Fortunately, the authors believe that the United States has a strong case that its legal architecture for government access to data is comparatively robust. That said, this report makes recommendations both for further strengthening this legal architecture and for encouraging, in a constructive way, a fair comparison between the United States' architecture for access to data and the relevant law and policy in other countries.

Another significant advantage of IT predominance for U.S. intelligence and counterterrorism is that the intelligence community can purchase the world's best information-technology products from trusted American providers. For example, the CIA paid Amazon Web Services (AWS), the market leader in cloud computing,[9] $600 million to build a cloud-computing infrastructure for the intelligence community.[10] The CIA's Chief Information Security Officer recently described the new system as "a godsend for folks trying to implement systems quickly and for us to secure workloads better."[11] AWS has also launched a classified software "marketplace" from which IC agencies can "evaluate and buy common software" for use in the cloud.[12] Cloud services could ultimately allow the IC to "bypass acquisition problems that have plagued government for decades," with $9.2 billion wasted on large-scale IT acquisitions in the last decade alone.[13]

The ability to purchase the products and services of world-leading, homegrown, trusted technology providers is an enormous advantage for the U.S. national security apparatus over the nation's competitors. But this advantage will only persist as long as companies are able to reconcile doing business with the intelligence community with their (far larger) private-sector customer

Protection from unwarranted government intrusion into personal privacy is a bedrock element of American liberty.

President Obama meets with U.S. intelligence community officials in the Cabinet Room of the White House, April 17, 2012 (Pete Souza/ Official White House Photo)

base. As Peter Swire, a member of the Review Group on Intelligence and Communications Technologies, noted earlier this year: "Post-Snowden, American-based information technology companies don't want to be seen as an arm of the U.S. intelligence community."[14] To take one small example of how this can affect the government's ability to acquire cutting-edge technology: In May, Twitter barred Dataminr, a startup that analyzes Twitter's entire real-time stream of public tweets to derive insights about unfolding events, from selling to the intelligence community.[15] Twitter was reportedly concerned about "seeming too close to American intelligence services."[16]

Of course, this tendency is only one competing factor in companies' decisionmaking and is often not decisive, as AWS's contract with the CIA shows. But if there are future Snowden-like revelations and near-peer competitors emerge to challenge U.S. technology companies, it could become significantly more damaging.

3. Signals-intelligence collection and analysis are vital national security tools. The United States will and should continue to maintain world-leading SIGINT capabilities. Some previous surveillance-reform efforts have recommended that the United States restore the balance between civil liberties and national security by dramatically curtailing the government's electronic surveillance capabilities – for example, by allowing Section 702 of the FISA Amendments Act to lapse or requiring judicial review of all surveillance activities conducted overseas under Executive Order 12333.

Whatever the merits of such an approach as a matter of abstract first principles, it is neither prudent from a national security perspective nor politically realistic. Senior intelligence community leaders reported earlier this year that the Islamic State (ISIS) is "likely" to attempt attacks in the United States in 2016 and that the United States faces the most diverse global threat environment in 50 years.[17] Recent attacks in Europe and the United States have shown that ISIS-directed and ISIS-inspired terrorists intend and are able to kill civilians in the West. Nor is terrorism the only relevant threat. Signals intelligence is also a vital tool for monitoring Iran's adherence to last year's nuclear accord, China's intentions and actions in the South China Sea, Russia's activities in Ukraine and apparent attempts to interfere in the presidential election, and the many other pressing geopolitical challenges facing the United States.

No president could responsibly surrender vital, lawful national security capabilities at a time of serious threat to the nation. But even if it were desirable as an abstract matter to substantially reduce government data collection and analysis, a mass-casualty terrorist attack on U.S. soil could trigger a public clamor for measures even more vigorous than those in use today, as well as a political backlash against the administration that had reduced its

counterterrorism capabilities in the face of an obvious threat. This report recommends reforms that the authors believe are both responsible and politically realistic given the diverse array of grave threats facing the U.S. homeland and American interests worldwide.

4. *Improving public and foreign trust on surveillance and digital privacy is an important goal, but no reform agenda can dispel completely the aftereffects of the Snowden leaks.* This report recommends many ways in which the next administration can improve public faith in the government's approach to digital privacy and can reduce or mitigate international skepticism of American surveillance practices. Yet these trust deficits cannot realistically be eliminated altogether; not even the most forward-leaning surveillance-reform agenda would restore pre-Snowden levels of public agnosticism about electronic surveillance practices. The heightened skepticism and expectation of transparency that the Snowden leaks created are not going away. Rather, they are features of the new landscape – features policymakers and the intelligence community will have to acknowledge and adapt to. This is not entirely a bad thing. Digital-age technologies would pose immense dangers if misused by the state, so heightened vigilance is appropriate.

This climate of persistent skepticism has important implications for policymakers and for the recommendations in this report. Going forward, surveillance policy will have to account not merely for national security needs but also respond to the public's demand for rigorous oversight and transparency – as well as the risk of "involuntary transparency" wrought by disgruntled employees or cyber-penetrations from abroad. This means that surveillance decisions will have to account for the risk of future disclosures. This report recommends several ways in which existing policies and practices can be adjusted to account for these features of the post-Snowden world.[18]

5. *The metaphor of finding a "balance" between civil liberties and security is a poor guide for optimizing surveillance policy.* It is artificially limiting to see the universe of policy options as a set of zero-sum choices between these two essential values. A zero-sum framework is a poor guide for intelligent policymaking in this area, for several reasons.

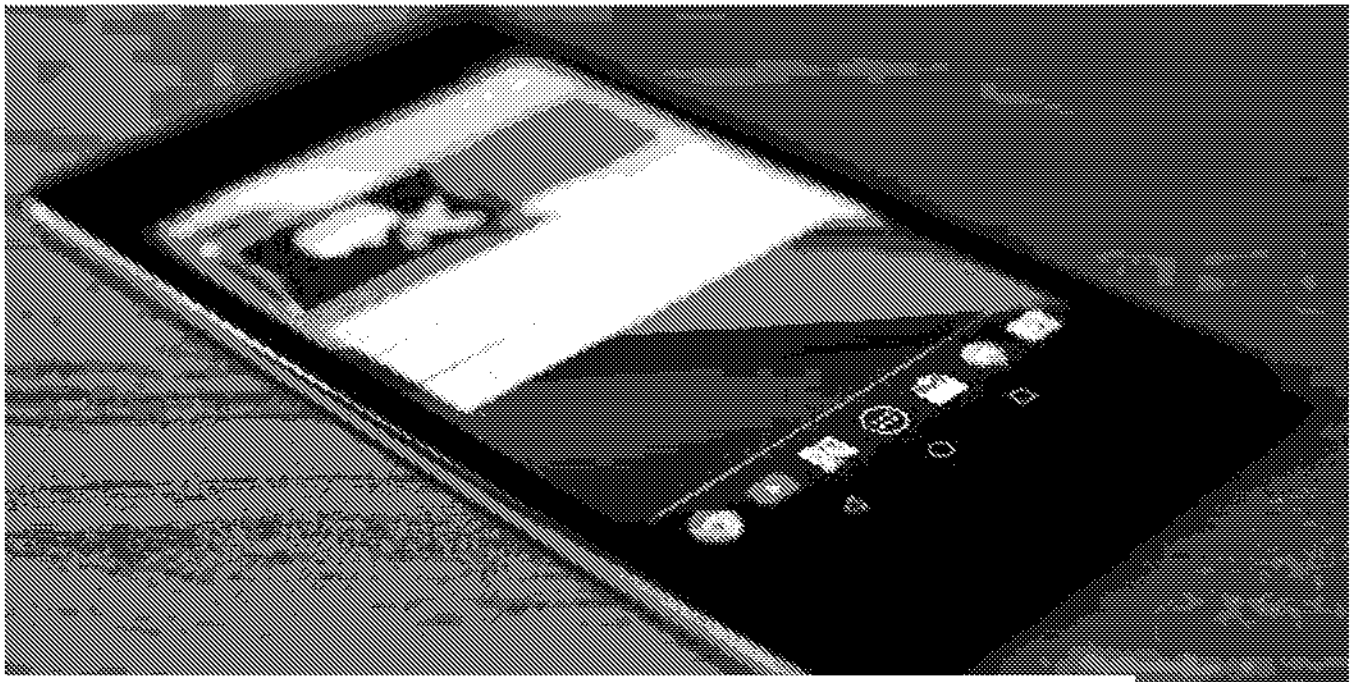
Most fundamentally, in a time of grave and diverse national security threats, Americans will demand robust, effective counterterrorism, law enforcement, and intelligence agencies to secure the homeland from external threats. To be sure, policymakers should seek to foster resiliency and avoid overreaction when attacks occur. But while greater resiliency can reduce the risk of overcorrection, the natural human impulse to seek safety in perilous times will persist. If the United States is to safeguard personal privacy and the rule of law – and it must – that means reconciling a strong and capable national security apparatus with the fundamental liberties that define the American way of life.[19]

Second, the notion that by surrendering a certain amount of security capability one automatically receives a concomitant benefit for civil liberties and public trust is incorrect. Put simply, reducing one of these values does not necessarily produce more of the other. Some surveillance authorities, for instance, are too esoteric to be particularly salient to most Americans. Others are not widely viewed as problematic from a privacy perspective. In either case, eliminating the program might inflict substantial harm to national security but produce relatively little public benefit. Conversely, reform opportunities exist that would strengthen digital privacy and public trust without materially degrading counterterrorism or other national security capabilities.[20]

If the United States is to safeguard personal privacy and the rule of law – and it must – that means reconciling a strong and capable national security apparatus with the fundamental liberties that define the American way of life.

Finally, a focus on zero-sum tradeoffs between privacy and security deters risk-averse policymakers from seeking out and embracing a privacy-enhancing reform agenda. Leaders whose primary mission is preventing terrorist attacks are understandably reluctant to take any measures that might undermine their ability to carry out that mission – especially given that there is little to no public tolerance for failure. If reform is cast as shifting a zero-sum "balance" between privacy and security, it is not hard to see why it might be unwelcome to those who, rightly or wrongly, see their primary mission as security.

6. *Signals intelligence and the powers of the NSA are not neatly severable from other issues affecting domestic and international data privacy.* This project began with a relatively tight focus on issues related to the intelligence community's signals-intelligence practices and the



The public does not draw a bright line between signals intelligence and other issues affecting data privacy, such as smartphone encryption. (Yuri Samoilov)

legal and institutional mechanisms for overseeing them. The authors quickly realized, however, that this was an artificial and ill-advised limitation. Complex issues like the details of Section 702 or the minimization procedures approved by the FISA Court, while important, are not well understood by the public. The debates over iPhone encryption and whether the government needs a warrant to read Americans' email, by contrast, are far more visible and comprehensible to average Americans. Over the course of a year-long series of conversations and interviews, it became clear that issues that experts would consider only loosely related to signals intelligence can directly influence Americans' willingness to entrust the government with powerful capabilities to collect, monitor, and analyze communications and user data. As one expert noted, the public does not draw a bright line between signals intelligence and other issues affecting data privacy.

This has two important implications for policymaking on surveillance and data-privacy issues. First, policymakers must account for how a decision they take in one area will reverberate in other areas. Second, a pragmatic agenda for surveillance policy should not artificially exclude other data-privacy issues that are highly salient to the public and where constructive reform is possible.

The next section describes several trust deficits opened by the Snowden revelations and the real-world problems they have created or exacerbated. Part III discusses the significant reforms already undertaken by the Obama administration and Congress since 2013. Finally, Part IV sets forth a pragmatic surveillance-reform agenda for the next administration.

Defining the Problem

Historically, the U.S. government's electronic surveillance capabilities were cloaked in deep secrecy. In late 2005, however, that cloak began to slip, when *The New York Times* revealed that the National Security Agency was monitoring, without judicial oversight, communications between Americans and overseas terrorism suspects.[21] That revelation generated substantial controversy, but it did not fundamentally alter the policy landscape. In fact, Congress subsequently granted the NSA statutory authority to continue monitoring these communications without individualized court orders.[22]

The Snowden revelations in 2013 changed everything. Domestically, the most jarring revelation was that the government had been using Section 215 of the USA PATRIOT Act to collect, in bulk, records of all telephone calls carried by major telecommunications carriers – including the call records of tens of millions (perhaps hundreds of millions) of ordinary Americans – even though the statute covered only records that were "relevant to an authorized investigation."[23] (The program did not collect or monitor the *content* of those calls – a distinction some in the media and public missed.)

Public Trust and Government Credibility

The use of Section 215 to collect call records in bulk, once revealed, created a major credibility gap surrounding electronic surveillance and the powers of the NSA. Not because the program was nefariously motivated or undertaken without authorization; it had been blessed by the Foreign Intelligence Surveillance Court (FISC), although that approval rested on a legal theory that was debatable at best and came in an *ex parte* proceeding without adversarial scrutiny.[24]

"expansive concept of 'relevance'" was "unprecedented and unwarranted."[25] In short, the biggest blow to public trust was that the scale of the collection was far beyond anything the public could have imagined.

The initial batch of Snowden documents also described an NSA program called PRISM, which allowed the government to domestically target the electronic communications of non-U.S. persons overseas. Some contemporaneous press reports suggested that the NSA had received unmediated access to the servers of Facebook, Google, Apple, Yahoo, and other providers. That proved incorrect, but the impression that leading American companies had provided such access to U.S. intelligence services was extremely damaging and difficult to correct. Taken together with the revelation of the Section 215 call-records program, the PRISM documents fueled widespread cynicism about the scope of government surveillance and the adequacy of democratic oversight and control.

The domestic outcry that erupted in 2013 has diminished over time, in no small part thanks to the many significant reforms and transparency measures, involving all three branches of government, that have been undertaken since the Snowden leaks. We discuss those changes below in Part III. Yet the Snowden disclosures and the resulting trust deficits continue to harm various important U.S. national interests.

Harms to Intelligence and Law Enforcement Capabilities

The Snowden leaks directly harmed ongoing intelligence efforts, including what Director of National Intelligence (DNI) James Clapper described as "the single most important source of force protection and warning for our people in Afghanistan."[26] Less obviously, but just as importantly, the post-Snowden backlash has also created

The scale of government surveillance was revealed to be far greater than ordinary Americans understood – and far greater than they reasonably could have anticipated.

The larger problem was that the scale of government surveillance was revealed to be far greater than ordinary Americans understood – and far greater than they reasonably could have anticipated based on the text of the relevant public law. The statutory phrase "relevant to a terrorism investigation" would not reasonably suggest to an average citizen that the government could simply collect *everything*. Indeed, the U.S. Court of Appeals for the Second Circuit held last year that the program's

significant new obstacles for law enforcement and the intelligence community. In the immediate aftermath of revelations suggesting that the U.S. government had compromised their products, technology companies were understandably outraged and feared a massive backlash from their domestic and international customers. Hardware manufacturers were burned when leaked documents suggested that the NSA had tampered with American-made products en route to their end

customers.[27] Internet companies were left backpedaling after an NSA slide deck describing PRISM was widely (but incorrectly) read to suggest that the agency had direct access to the companies' servers. Yahoo and Google were angered when media reports emerged that the NSA and Britain's Government Communications Headquarters (GCHQ) had cooperated in gaining surreptitious access to "the main communications links" connecting each company's international data centers.[28]

To reassure their customers, many industry leaders reacted to the initial Snowden disclosures by publicizing their intention not to voluntarily assist government surveillance, and indeed to resist where possible.[29] Many companies now refuse to give customer data to the government until presented with binding legal process, even where the law permits them to do so, except where immediate access is needed "to prevent death or serious physical harm."[30] This forces law enforcement to expend more time and resources to obtain needed information. One expert told us that the system was simply not designed to handle the volume of litigation that would be required if companies demanded that the government go to court for every request. Moreover, with respect to data stored overseas, Microsoft has now won a court ruling that the U.S. government must use the cumbersome mutual legal assistance (MLA) process to obtain the data rather than seeking it directly from the company.[31]

The post-Snowden backlash has created significant new obstacles for law enforcement and the intelligence community.

Another reaction was to begin deploying powerful encryption technologies and handing the only key to the customer. While companies' business models have precluded them from using encryption to deny the government access to *all* user data, the post-Snowden move toward encryption has gone far enough to create serious problems for law enforcement. Perhaps the most visible manifestation has been Apple's decision to introduce on iOS devices full-disk encryption keyed only to the user's password. This change meant that Apple could no longer extract user data directly from devices running iOS 8 or later.[32] This became the subject of a high-profile national debate in the wake of the San Bernardino shootings earlier this year. The encryption controversy is discussed in greater detail below.

Diplomatic Costs

The damage wrought by the Snowden disclosures was not limited to intelligence and counterterrorism programs; they also undermined American soft power, credibility, and global leadership. To take just one illustration, Obama's approval rating in Germany fell from 75 percent to 43 percent after Snowden documents revealed the NSA's surveillance of Chancellor Angela Merkel's personal cell phone.[33] Even in 2015, two years after the leaks, a YouGov poll found that Edward Snowden was more admired in Germany than President Obama.[34] Perhaps most troubling, from 2013 to 2014 the share of Germans calling for a more "independent" approach to the transatlantic relationship jumped from 40 percent to 57.3 percent.[35]

High-level government-to-government relationships have largely healed – to some degree out of necessity. Yet there remains what one expert called a "residual trauma" that permeates transatlantic ties on issues related to surveillance and data privacy. Another expert described German public opinion as having settled into a "malaise" in which Germans are very aware of the issue and remain dissatisfied, but feel there's little they can do. In a democratic system, such widely held concerns will inevitably influence policy.

Perhaps the most dramatic international effect of the Snowden revelations was the decision by the Court of Justice of the European Union in *Schrems v. Data Protection Commissioner,* which effectively invalidated the "Safe Harbor" agreement allowing companies to transfer their European users' data to the United States. That decision was prompted in part by concern that U.S. authorities might have "access on a generalised basis" to European customer data transferred to the United States by U.S. companies. That concern was unfounded; the PRISM program on which the court focused requires individualized targeting and does not permit bulk collection.[36] Yet the court nonetheless upended Safe Harbor, triggering a period of intense and costly uncertainty for American companies doing business in Europe.

The United States and European Union have now agreed to a successor to Safe Harbor, known as Privacy Shield, which is discussed in greater detail in Part IV.[37] It bears noting, however, that Privacy Shield's future is far from assured; privacy advocates recently filed a lawsuit contending that Privacy Shield suffers from the same legal flaws the Court of Justice discerned in Safe Harbor.[38] U.S. actions over the next several years have the potential to affect the outcome of that case, in helpful or unhelpful ways.

Germans demonstrate in Berlin against government surveillance. (Markus Winkler/Creative Commons)

Finally, the Snowden disclosures have affected the United States' global internet-freedom agenda. With ever more human activity "mediated through Internet-based technologies," free access to the internet and secure digital communications have "take[n] on an increasingly vital role in political, economic and social life."[39] Under the Bush and Obama administrations, the U.S. government has spent hundreds of millions of dollars to support free access to the internet and secure communications for users around the world, especially those living under authoritarian regimes.[40] The United States has also fought to preserve the multi-stakeholder approach to internet governance and resisted efforts, led by authoritarian regimes, to allow governments to exert greater control over the internet.[41]

High-level government-to-government relationships have largely healed – to some degree out of necessity. Yet there remains what one expert called a "residual trauma" that permeates transatlantic ties on issues related to surveillance and data privacy.

Unfortunately, the Snowden disclosures and the perception that the NSA is engaged in mass online surveillance have dented the United States' credibility as a defender of a free internet. They have also led various countries to enact or consider measures, including "data localization" laws, that if widely adopted would transform the internet from an interconnected global network to a Balkanized mosaic of separate national networks, each tightly controlled by its government.[42]

Effects on the U.S. Technology Sector

The PRISM releases were bad enough – but unfortunately for American technology companies, other damaging leaks were still to come. A Snowden document released in 2014 revealed that NSA had been "interdicting" shipments of U.S.-made computer hardware and implanting beacons that would report back to NSA once installed, raising concerns overseas about the security of U.S. technology products.

In response to the disclosures, various governments, from adversary nations like Russia to friendlier countries like Brazil, have implemented or explored data localization – requiring data about domestic users to be stored on domestic servers. The beneficiaries are local cloud-computing services, which otherwise would struggle to

compete with American market leaders; among the losers would be Silicon Valley startups that could not establish an online presence with global reach without first placing servers in local jurisdictions across the world. In short, public outrage over American surveillance gave some foreign governments political cover to pursue "data protectionism."

rather than adding capacity at existing facilities in the United States is only one measure of the harm. Digitally enabled services – that is, services that can be delivered remotely over the internet – account for more than half of U.S. exports.[48] And with the rise of cloud computing and big-data analytics, the importance of open data flows will only increase. If the overseas clients of U.S.

This backlash has cost American firms billions and provided "a boon for foreign companies."

This backlash has cost American firms billions and provided "a boon for foreign companies."[43] The blowback affected even non-IT deals; for example, Saab unexpectedly beat out Boeing for a $4.5 billion Brazilian military jet contract after Snowden documents revealed that the NSA had spied on Brazilian President Dilma Rousseff.[44] And the authors heard directly from allied government officials that their IT departments no longer had confidence in the integrity of U.S.-made products for their official systems and had even undertaken efforts to develop indigenous alternatives.

The Information Technology and Innovation Foundation (ITIF) estimated in 2015 that the cost of the Snowden revelations for U.S. tech companies would "far exceed" $35 billion.[45] As the ITIF report explained:

> When historians write about this period in U.S. history it could very well be that one of the themes will be how the United States lost its global technology leadership to other nations. And clearly one of the factors they would point to is the long-standing privileging of U.S. national security interests over U.S. industrial and commercial interests when it comes to U.S. foreign policy.[46]

Some have suggested that the damage to U.S. economic interests from the Snowden disclosures is overhyped or even illusory. While reasonable minds can differ on the precise dollar amount of the losses, this critique overlooks various less obvious ways, beyond lost sales, in which the revelations have affected U.S. companies' business prospects in Europe.

For example, while the *Wall Street Journal* recently reported that American companies continue to dominate the cloud-computing market in Europe, the paper also noted that they have been able to do so only by building "at least a dozen new data centers in Europe in recent years."[47] The additional cost of building new data centers

Data protectionism also poses a fundamental threat to the global business models of many American internet companies. Widespread adoption of data localization could stifle the growth of startups offering innovative, transnational services. Given that the United States is the world leader in such products and services and has the most innovative startup ecosystem, it would be the biggest victim from widespread data localization laws. Even absent data localization mandates, however, some foreign customers are asking U.S. technology companies to store their data within national boundaries.[50] This is technologically suboptimal, for several reasons. But if foreign customers request it, U.S. companies will have little choice but to meet that demand.[51]

Hardware manufacturers have also been harmed by increased suspicion of American technology products. In the post-Snowden era, even when large foreign customers do ultimately choose American products, those orders are routinely preceded by skeptical questions about ties to the NSA and are often coupled with demands for extreme and costly measures to secure the supply chain. In an era of widely distributed global supply chains and on-demand manufacturing, such demands impose significant additional costs on the companies. Finally, American providers have traditionally been able not merely to win orders but also to charge a premium for being the most trusted supplier. To the extent that the Snowden revelations have eroded that trust premium, the full extent of the damage may be hidden by U.S. companies' continued ability to win orders.

Finally, the fact that American technology firms have invested so much in responding to the Snowden revelations and in signaling their independence from the U.S. government is a strong proxy for their assessment of the potential costs of Snowden blowback for their business models. These are sophisticated, for-profit public companies with no incentive to add unnecessary overhead in the form of lawyers, privacy officers, government relations, and so forth. Companies have taken various labor-intensive, expensive steps to shore up trust in their products. These include expanding the use of encryption, adding "trust anchors" and "secure boot" technology to prevent hacking, and even shipping products to anonymized addresses to foil possible government interdiction.[52] Companies would not be expending huge amounts of money, engineering time, and other resources on these efforts unless they sincerely believed that the potential blowback would inflict even greater costs.

Data protectionism poses a fundamental threat to the global business models of many American internet companies.

Three years after the Snowden leaks, the climate of mistrust they created remains damaging. Public skepticism persists. American companies must overcome suspicion that their products and customer data are compromised by government surveillance. And the backlash continues to impede some law enforcement and intelligence activities.

That said, the status quo today is not as bad as it might have been; fortunately, much has already been done to reform U.S. surveillance practices and rebuild trust. The next part of this report reviews these significant post-Snowden reform efforts. Part IV then considers both where policymakers should press for further reforms and how to draw more attention to the important steps already taken.

Post-Snowden Responses and Reforms

This part describes the many reforms already enacted in response to the Snowden leaks. These steps, while by no means the end of the surveillance-reform journey, are a substantial and meaningful beginning.

In fact, more has already been done than is widely appreciated, particularly overseas. Congress and the executive branch have implemented most of the headline recommendations of the major post-Snowden reviews. And President Obama has made historic commitments with respect to the privacy interests of foreigners – commitments matched by no other country.

President's Review Group on Intelligence and Communications Technologies

In the wake of the Snowden disclosures, the president appointed a five-member "Review Group" to consider the issues raised by the leaks and to make recommendations for reform. The Review Group considered both specific programs (including Sections 215 and 702) and broader questions about how to set signals-intelligence priorities and manage and oversee collection. Its December 2013 final report included a wide array of recommendations: general principles for structuring surveillance policy, revisions to specific legal authorities, and significant institutional reforms.[53] The report remains an important touchstone that can still usefully inform the next administration's surveillance-policy decisions.

Many of the Review Group's major recommendations have already been implemented or may be implemented imminently. These include:

- *Telephone metadata.* The Review Group urged that telephone metadata no longer be held by the government, but rather be "held privately for the government to query when necessary for national security purposes."[54] The USA Freedom Act fulfilled this recommendation.
- *Transparency.* The Review Group recommended that the government be required to disclose data about surveillance requests; that private telecommunications providers be permitted to do so; and that Congress authorize "Public Interest Advocates" to represent the public interest before the Foreign Intelligence Surveillance Court.[55] The USA Freedom Act fulfilled these recommendations as well.
- *Principles to govern signals intelligence.* Presidential Policy Directive 28 (PPD-28) adopts as binding policy within the executive branch many of the broad principles endorsed by the Review Group to govern signals intelligence.
- *NSA and Cyber Command leadership.* The Review Group recommended that the head of the military's Cyber Command and the Director of the NSA "should not be a single official" and that civilians be eligible to serve as NSA director.[56] The Obama administration is reportedly considering a plan that would fulfill both of these recommendations.[57]

A number of meritorious and significant Review Group recommendations have yet to be implemented, however. Several of these are addressed in Part IV.

Presidential Policy Directive 28

A month after the Review Group presented its final report, President Obama issued PPD-28, "Signals Intelligence Activities," which "articulates principles to guide why, whether, when, and how the United States conducts signals intelligence activities for authorized foreign intelligence and counterintelligence purposes."[58]

Some of these principles are anodyne; for example, that signals-intelligence collection "shall be authorized by" and "undertaken in accordance with" law.[59] Others elevated existing policy to the level of a binding presidential directive: for example, that agencies may not collect "foreign private commercial information" in order "to afford a competitive advantage to U.S. companies and U.S. business sectors commercially."[60]

Others were more newsworthy, however, and arguably historic. These include:

- Signals-intelligence activities must incorporate safeguards for the personal information of "all individuals, *regardless of ... nationality ... or where that individual resides.*"[61] The NSA, FBI, and CIA have now published policies and procedures implementing the required safeguards, including minimization procedures limiting how such data can be retained and when it can be disseminated outside the agency.[62]
- Personal information of non-U.S. persons must be purged after five years absent a specific determination by the DNI that it should be retained.[63]
- Data collected in bulk – that is, without targeting based on a specific identifier or selection term – can be used only for specified purposes, including counterterrorism, counterintelligence, countering proliferation of weapons of mass destruction, cybersecurity, and transnational crime.[64]

- The State Department was required to designate, and did designate, a senior official "to serve as a point of contact for foreign governments who wish to raise concerns regarding signals intelligence activities conducted by the United States."[65]
- "[D]eterminations about whether and how to conduct signals intelligence activities" must be subject to a risk-benefit analysis.[66]

PPD-28's commitment to consider the privacy interests of foreign nationals is now being implemented by the intelligence community. Agencies must now "delete non-U.S. person information collected through SIGINT five years after collection unless" certain national-security-related exceptions apply.[67] This five-year limit, while less protective than some would like, outstrips any privacy protection European governments have offered to Americans. PPD-28 should be the starting point for a more robust dialogue with U.S. allies on the protections they are willing to offer one another's citizens in their intelligence practices.

USA Freedom Act

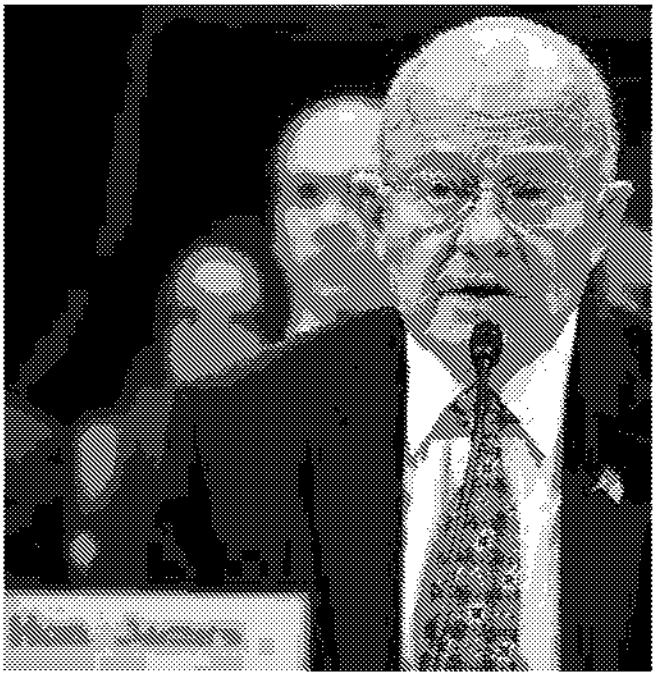
In June 2015, Congress passed and the president signed the USA Freedom Act,[68] which implemented various recommendations from the President's Review Group and the Privacy and Civil Liberties Oversight Board's report on the Section 215 call-records program.[69] The act's most significant reform was prohibiting the government from collecting in bulk telephone call records or other "tangible things" under Section 215. Instead, the new law permits the government to query, on an individualized basis, call records held by telecommunications providers. The government's application for call records must show a "reasonable, articulable suspicion that [a] *specific selection term is associated with ... international terrorism.*"[70] The government can seek records up to two degrees of separation, colloquially known as "hops," out from the original selection term.[71] The act also prohibited the use of national security letters for bulk collection.[72]

Less widely noted was that the USA Freedom Act contained several major transparency reforms, which are already having a notable and salutary effect. Specifically, the act:

- Permits the Foreign Intelligence Surveillance Court to call upon a select group of cleared advocates to represent the public interest in significant cases. These amici curiae can be appointed to offer "legal arguments that advance the protection of individual privacy and civil liberties" or to provide "information related to intelligence collection or communications technology."[73] The court has already used this provision; experienced national security lawyer Amy Jeffress was appointed last year, and raised several important legal arguments, in the FISC's annual review of the government's certifications for the Section 702 program.[74]
- Requires the DNI and the Attorney General to publish, to the greatest extent practicable, any FISC decision "that includes a significant construction or interpretation of any provision of law."[75]
- Requires the Director of National Intelligence to issue annual reports disclosing the total number of queries under Sections 215, 702, and other surveillance authorities.[76]
- Requires the Administrative Office of the U.S. Courts to issue annual reports disclosing similar data about proceedings before the Foreign Intelligence Surveillance Court.[77]
- Permits private companies to issue periodic reports disclosing, within numerical ranges, the number of surveillance orders of various types that they receive.[78] Since 2013, leading internet companies had battled the government for permission to provide their customers with meaningful disclosure about such requests.[79]

The USA Freedom Act's headline-grabbing changes to the Section 215 call-records program overshadowed this array of transparency and oversight reforms. Importantly, these changes do not materially reduce counterterrorism capability, yet they substantially bolster the public legitimacy and democratic accountability of the programs to which they apply. These reforms embody several important principles of intelligence transparency – principles that point the way for future surveillance-reform efforts.

First, and most fundamentally, domestic surveillance or surveillance of U.S. persons overseas should be based on clear statutory authority, publicly interpreted, with rigorous oversight to ensure that the government stays within the publicly understood confines of its legal authority.[80] This oversight role will often be performed by courts, but also includes close supervision by a fully informed Congress and by a vigorous Privacy and Civil Liberties Oversight Board within the executive branch. The judicial role here need not entail individualized review of every targeting decision; in the context of Section 702, regular programmatic review and supervision are appropriate given that the targets are non-U.S. persons living outside the United States.[81]



Director of National Intelligence James R. Clapper testifies before the House Permanent Select Committee on Intelligence. (Brian Murphy/Office of the Director of National Intelligence Public Affairs)

What is essential, however, is that the available public information permit a well-informed citizen to form a reasonably accurate understanding of the general contours of the government's surveillance powers, allowing meaningful democratic control of the scope of surveillance authority. The goal is to avoid the growth of a substantial discrepancy between what is actually happening and what the public believes to be allowed. As the 2013 leaks (like the Church Committee hearings of the 1970s) demonstrated, such discrepancies can lead to a crisis of public trust when the true scale of government activity is revealed. There are several additional ways to prevent such discrepancies from forming, which are discussed in detail later in this section.

Second, while secret facts are unavoidable in this context, the government should declassify, with as much granularity as is consistent with national security, data about the volume and purposes of surveillance activity. Fortunately, this is already happening to a significant degree – an immensely important and underappreciated change from the pre-2013 status quo. For example, the intelligence community's Statistical Transparency Report for 2015 reports that 94,368 individuals or organizations were targeted for collection under Section 702 in that year,[82] a slight increase from 2014.[83] By way of comparison, the government used "traditional" FISA to obtain domestic national security wiretaps for 1,695 targets in the United States in 2015.[84] Publishing this type of high-level data should not harm national security but can give the public a general sense of the overall scale of surveillance activity and the relative importance of various legal authorities.

Third, secret processes for making significant decisions about the scope and nature of government surveillance should be, if not strictly adversarial, at least designed to consider the interests of all stakeholders. The USA Freedom Act's provision for public-interest advocates is one important application of this principle. Part IV offers other ways to apply it, within both the FISC and other intra-governmental forums.

Privacy and Civil Liberties Oversight Board

The 9/11 Commission recommended that Congress create an independent "board within the executive branch to oversee ... the commitment the government makes to defend our civil liberties."[85] Congress adopted that recommendation in the Intelligence Reform and Terrorism Prevention Act of 2004, creating the Privacy and Civil Liberties Oversight Board.[86]

Since 2013, the Board has emerged as a valuable and influential feature of the oversight landscape for counterterrorism and surveillance. Most notably, the Board has issued comprehensive and well-regarded reports on bulk call-records collection under Section 215 and on Section 702. The Board reports that it has received fulsome cooperation from the intelligence community, and its work has spurred the community to declassify many basic facts about the Section 702 program. This enhanced the public's understanding of how the program operates without compromising national security.

As previously noted, the USA Freedom Act implements many of the recommendations from the PCLOB's report on Section 215.[87] The intelligence community has also implemented, in whole or in part, all of the PCLOB's recommendations from its report on Section 702. Among the most notable recommendations were:

- Improving documentation of the foreign-intelligence purpose for individual targeting decisions under Section 702.[88]
- Implementing more rigorous constraints on searches for U.S.-person information incidentally collected under Section 702.
- Giving the Foreign Intelligence Surveillance Court more data on how the government is implementing the broad "authorizations" the court approves under Section 702.[89]

In short, the Board has been a valuable addition to the constellation of oversight entities. Its report on the Section 702 program in particular illustrates how a functioning, well-staffed Board can enhance, in a manner consistent with national security, the public understanding (and thus the democratic legitimacy) of important but controversial signals-intelligence programs. A vigorous Board also strengthens the United States' case to other countries that U.S. signals-intelligence activities operate within a robust oversight framework. For example, in a letter designed to address European concerns related to Privacy Shield, the General Counsel of the Office of the Director of National Intelligence (ODNI) cited the Board and its public reports as evidence of the "rigorous and multi-layered" oversight of U.S. intelligence.[90] Part IV makes several recommendations to ensure that the Board remains a viable and robust presence into the next presidential administration.

Intelligence Community Transparency Agenda

The intelligence community has also moved on its own to increase transparency and public outreach. Last year the Director of National Intelligence publicly committed the community to "appropriate transparency" about its mission and legal authorities, to better public communication and engagement, to "proactive" efforts to declassify and publish relevant information, and to ensuring that classification practices are not excessive or overzealous.[91]

To implement this agenda, ODNI has created "IC on the Record," a website providing "[d]irect access to factual information related to the lawful foreign surveillance activities of the U.S. Intelligence Community."[92] The site provides information about the intelligence budget, periodic transparency and disclosure reports, and many declassified documents related to intelligence programs. IC officials, and particularly NSA officials, have also made a concerted effort to engage publicly with relevant communities.

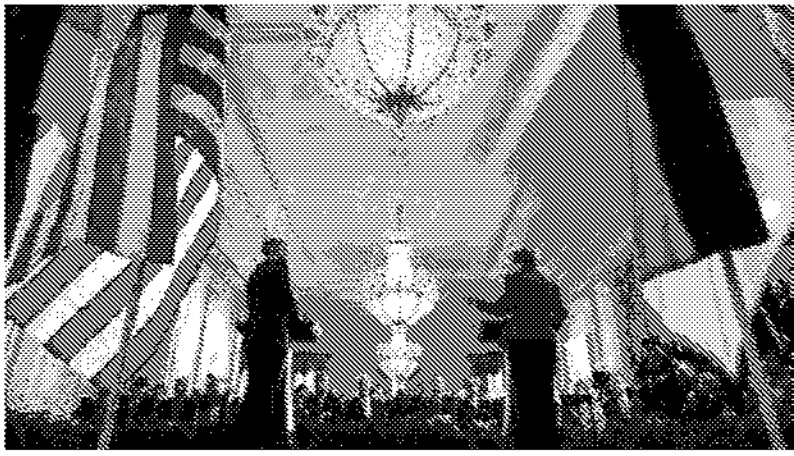
Diplomatic Efforts

Finally, the State Department has led diplomatic efforts to ameliorate the international repercussions of the 2013 disclosures. In the wake of the revelation that the NSA had been monitoring Chancellor Angela Merkel's cell phone, the United States and Germany initiated a series of meetings to discuss surveillance and rules of the road in cyberspace.[93] (President Obama also ended the monitoring of Chancellor Merkel's communications.[94]) While these meetings produced few concrete outcomes, they allowed for open dialogue between American and German officials at a time when such discussions were politically sensitive in Germany.

More broadly, Secretary of State John Kerry and other State Department officials have attempted to delineate a set of general norms that the United States believes should govern surveillance activities in democratic systems. Specifically, in April 2014, Secretary Kerry laid out four principles that the United States believes are "universally applicable" to surveillance in democratic systems:

1. "Rule of law – democracies must act according to clear, legal authorities, and their intelligence agencies must not exceed those authorities."
2. "Legitimate purpose – democracies should collect and share intelligence only for legitimate national security reasons and never to suppress or burden criticism or dissent."
3. "Oversight – judicial, legislative or other bodies such as independent inspectors general play a key role in ensuring that these activities fall within legal bounds."
4. "Transparency – the principles governing such activities need to be understood so that free people can debate them and play their part in shaping these choices."[95]

Below, we consider how to expand and strengthen these diplomatic efforts; in particular, how to ensure that they result in better global awareness of the reform initiatives the United States has undertaken since 2013 and how to encourage mutual commitments among like-minded nations.



President Barack Obama and German Chancellor Angela Merkel hold a joint news conference. (Chuck Kennedy/Official White House Photo)

As this recounting shows, since the Snowden revelations the U.S. government has undertaken significant reforms to its surveillance programs and oversight mechanisms. Yet while these changes are a strong beginning, they cannot be the end, for several reasons. They are not widely known overseas; indeed, given the technical and bureaucratic nature of many of the changes, they are unknown to most Americans. The focus on the Section 215 call-records program in the immediate post-Snowden period, while understandable, overshadowed other important issues, such as outreach to foreign publics and the challenges facing the U.S. technology sector. Finally, and perhaps most importantly, these successes are fragile. New leaks could rekindle latent skepticism and mistrust. Some changes, such as PPD-28 and the intelligence community's transparency efforts, could be rolled back by a new president. And future terrorist attacks could push public opinion dramatically toward security, as in the period immediately after the 9/11 attacks.

Surveillance reform should be seen as a work in progress rather than a finished product.

For these reasons, surveillance reform should be seen as a work in progress rather than a finished product. The agenda this report proposes would take the next step toward rebuilding trust with the American people, the technology industry, and partners abroad. It would enable the new administration to speak with one voice in support of a pragmatic, privacy-enhancing agenda. It would help persuade allied publics that their countries and the United States share basic values on data privacy and surveillance. It would safeguard the United States' enviable position as the world leader in information technology. And it would help inoculate the new administration against the risk of future unauthorized disclosures. Importantly, however, it would further these aims while preserving needed national security capabilities.

A Pragmatic Agenda for Surveillance Policy

Each new president enters office with a chance to reorient the national agenda and signal that the country is leaving behind the controversies of the previous administration. President Obama, for example, signed on his second day in office an executive order unambiguously banning torture and, less successfully, setting out a plan to close the detention facility at Guantanamo Bay.[9] These moves were intended to signal a clear break with certain controversial post-9/11 counterterrorism policies.

Unfortunately, the Snowden leaks placed the Obama administration in the unenviable position of serving as the face of controversial surveillance practices, even though these practices had spanned administrations. Administration officials have worked hard to dispel the legacy of those revelations, most notably by creating the President's Review Group and implementing many of its recommendations. Notwithstanding these positive steps, however, there was an unavoidable limit to the Obama administration's ability to shed the Snowden legacy, particularly with limited time remaining and many competing priorities.

A new administration will have an opportunity to refresh the narrative surrounding the U.S. government's approach to surveillance and digital privacy – if it acts proactively. But this opportunity is perishable for several reasons. As the new president's term unfolds, other controversies and crises will inevitably arise. Once the administration is forced into a reactive, crisis-management posture it becomes far harder for it to proactively set the policy agenda. Moreover, reforms undertaken in response to a crisis tend to garner less public goodwill than those enacted before a crisis occurs; the public assumes that such reforms, like a forced apology, are grudging and self-interested rather than driven by foresight and conviction. Another benefit of taking reform measures proactively is that if further damaging revelations from the Snowden leaks occur, the president will be a credible reform advocate rather than painted as having silently acquiesced in the disputed practices.

Some might argue that the next president should spend down some of the new administration's post-inaugural political capital to enact an aggressive, controversial surveillance-policy agenda – whether reformist (such as allowing the FISA Amendments Act to sunset) or security-driven (such as pushing for decryption legislation). The authors believe that either course would be impracticable and inadvisable for a new administration. While the inauguration typically produces some reservoir of goodwill for a new president, that resource is quickly exhausted. The new president's first actions will quickly shape public perceptions and, if divisive, consume the president's political capital and harden political opposition. In addition, the public will hold the new administration responsible for any terrorist attacks that occur on its watch.

To avoid this trap, the reform agenda outlined here generally eschews approaches that would require the new administration to simply choose one side of an entrenched dispute over the other. The virtue of this approach is that it is politically realistic and would not require the new administration to expend excessive amounts of political capital on this one issue. In fact, we believe that these recommendations would expand the new president's political capital, earn public support and bipartisan credibility, and to some extent inoculate the president against a backlash should there be future unauthorized disclosures.

Finally, a word on how a new administration should implement a program like that proposed here. Policy experts frequently and understandably treat the issues we discuss here as falling into several distinct spheres: Signals intelligence in one basket, law enforcement in another, diplomacy in a third. The public, however, does not perceive these issues as neatly severable. Snowden-type revelations about NSA signals-intelligence programs and FBI efforts to access encrypted smartphone data both shape the public's perception of whether the government is appropriately reconciling national security needs with digital privacy. Indeed, it is unwise for a new administration to treat these issues as severable, because many of the most significant opportunities to enhance Americans' digital privacy come in areas that do not directly affect counterterrorism capabilities.

A new administration will have an opportunity to refresh the narrative surrounding the U.S. government's approach to surveillance and digital privacy – if it acts proactively.

For that reason, a new administration would be better served by publicly announcing these measures as part of a unitary reform agenda than by simply farming them out to various parts of the administration for quiet

implementation. There are both public-spirited and instrumental reasons to do this. These measures will be more effective as a restorative tonic for past breaches of trust if they are widely known; indeed, one of the reasons that the far-reaching commitments of PPD-28 have not had a significant effect on overseas perceptions of U.S. surveillance practices is that most people simply are not aware of them. Announcing a broad reform agenda, in addition to being sound policy, is also good political practice: A major initiative, publicly promoted by the White House, will more effectively define the new administration in the public mind as caring about Americans' digital privacy than a series of atomized technical changes implemented by the bureaucracy and known only to experts.

Accordingly, these recommendations are organized not by implementing agency but by the particular trust deficit – with the American public, American companies, or foreign governments and publics – that each proposal is aimed at improving.

Strengthening Public Trust

The next president will have a brief window of opportunity in which to signal to the American people that the new administration takes their digital privacy seriously. The next administration will also be confronted with pressing challenges that, depending on how they are resolved, have the potential to muddle that message – in particular, the reauthorization of Section 702 and developments that "could plunge the [Privacy and Civil Liberties Oversight Board] back into obscurity."[97]

This report proposes a series of reforms to enhance Americans' digital privacy, boost transparency, and bolster the credibility of key oversight mechanisms – without compromising important national security authorities.

EMAIL PRIVACY AND GOVERNMENT ACCESS TO OTHER PERSONAL DATA

Many of the issues discussed in this paper are relatively esoteric. While important, they are of interest primarily to subject-matter experts and are not well understood by the general public. Section 702 is a prime example – how many Americans have heard of this statute, not to speak of understanding what it does? That is not to suggest that obscure or esoteric issues are unimportant. But it does mean they are less relevant to the public's overall perception of whether the government respects its digital privacy. And restoring that trust should be a key goal of any surveillance-reform agenda.

That does not mean that a reform agenda should exclude esoteric issues; we cover many here. But it does mean that a reform agenda should *include* those high-visibility, emotionally resonant topics that help shape public opinion on these issues.

One such topic is email privacy – that is, whether the government needs to obtain a warrant based on probable cause to view the content of a U.S. person's email. The Electronic Communications Privacy Act's rules for law enforcement to access the contents of electronic messages are byzantine. If the email is stored on your mobile device, the government almost always needs to get a search warrant before accessing its contents.[98] But if the email is stored in the cloud, whether or not the government needs a warrant to obtain a message depends on how long it has been in storage, whether it has been opened by the user, and what type of communications provider is hosting it.[99]

The historical roots of these distinctions are not relevant here.[100] For present purposes it is enough to note that they have been superseded by technological developments. They are also untethered to Americans' expectations of privacy when they use those platforms.[101] And there is a strong argument that search warrants are constitutionally required, whether because users have a "reasonable expectation of privacy" in the contents of their stored email[102] or because stored emails should be considered "papers" directly protected against unreasonable searches by the text of the Fourth Amendment.[103]

Legislation pending in Congress would replace the statute's anachronistic distinctions with a uniform, nationwide warrant requirement for law-enforcement access to email.[104] The bill, known as the Email Privacy Act, would also end the practice of imposing indefinite gag orders barring providers from notifying customers of government requests for their data. Instead, nondisclosure orders would be limited to 180 days, with the possibility of extensions where needed. To issue a new order or an extension, a judge would have to specifically find that a serious harm would result if the customer were notified.[105]

STRENGTHENING PUBLIC TRUST

Email Privacy and Government Access to Other Personal Data

- If the Email Privacy Act does not pass during the 114th Congress, the next president should, in the first 100 days of the new administration, call for legislation (i) requiring a warrant to obtain the content of email and documents stored in the cloud and (ii) imposing reasonable limits on nondisclosure orders.
- The new administration should launch a White House initiative to propose standards for government access to other types of sensitive data, such as cell-site location data, data generated by "internet of things" devices, license-plate readers, facial recognition systems, and other foreseeable technologies with significant implications for personal privacy.

Intelligence Transparency and Secret Law

- The NSA should expand its efforts to demystify the agency's work in the mind of the general public.
- Senior leaders should not hesitate to defend the many valid purposes of signals intelligence beyond counterterrorism. Limiting the public defense of SIGINT to counterterrorism alone invites a backlash when uses other than counterterrorism are revealed.
- The next president should publicly embrace the principle that all domestic surveillance and surveillance of Americans overseas will be based on clear statutory authority, publicly interpreted, with sufficient oversight to hold the government to its construction of the statute.
- The president should task the general counsels of the Office of the Director of National Intelligence, NSA, FBI, and CIA, and the Assistant Attorney General for National Security, in consultation with the PCLOB, with proposing, within six months, other ways to reduce the amount of classified legal interpretation and programmatic guidance governing electronic surveillance. This could include, where consistent with national security, further declassification of relevant presidential directives, agency procedures, interagency memoranda of understanding, opinions of the Justice Department's Office of Legal Counsel, and classified annexes to legislation.
- Even those documents in these categories that cannot be safely declassified and published should be shared, in a manner consistent with their classification and to the extent permitted by executive privilege, with the congressional intelligence committees.

Section 702

- Section 702 should be reauthorized, but with reforms to enhance public confidence, transparency, and privacy.
- The FBI should publicly explain with greater precision why it needs to search databases containing 702 information for data about U.S. persons.
- The FBI should consider, and explain, whether it would be sufficient for it to continue to query databases containing 702 data for U.S.-person identifiers but, where such a search returns 702 information, to receive only the responsive metadata rather than the content.
- Congress, as a condition of reauthorization, should mandate further transparency about several aspects of the 702 program.

The Privacy and Civil Liberties Oversight Board

- The next president should swiftly appoint new members or reappoint existing members and work with the Senate to ensure that they are promptly confirmed.
- Congress should pass legislation that permits the remaining members to collectively appoint staff in the absence of a chairman.
- Congress should enact legislation exempting the Board from the Government in the Sunshine Act.
- While is appropriate that the Board's activities focus on protecting the privacy rights of U.S. persons, Congress should not expressly restrict the Board's statutory jurisdiction to only the rights of U.S. persons.
- Congress should not require the Board to keep the Director of National Intelligence or other elements of the intelligence community "fully and currently informed" of its activities.

In April 2016, the House passed the Email Privacy Act by a vote of 419-0 – a vanishingly rare demonstration of national consensus on such a consequential issue.[106] The Email Privacy Act unites the left, the right, privacy groups, and the business community. Importantly, it would not harm the Department of Justice's ability to prosecute cases or defend against terrorism; because of a judicial ruling applicable in several states,[107] federal prosecutors and FBI agents nationwide already obtain search warrants for the contents of electronic communications as a matter of policy.[108]

Yet the bill has stalled in the Senate. The principal reason is disagreement over an amendment that would allow the FBI to obtain records about online activity without a judicial order. These records are commonly known as "electronic communications transactional records," or ECTRs, and could include information such as what websites a user visits; the senders, addressees, and time-stamps of a user's emails; and information that can pinpoint the user's location.

The authors understand the perspective of those who sought to add the "ECTR fix" (a shorthand that is itself contested[109]) to the bill. Their aim – ensuring that the FBI is able to fight terrorism effectively – is one we share. But a warrant requirement for accessing the content of stored communications – a rare area of overwhelming bipartisan consensus – should not be further delayed. In addition, the types of records covered by the ECTR amendment raise serious, independent privacy concerns. To its credit, the Justice Department recently provided a thorough set of answers to frequently asked questions about how law enforcement obtains ECTRs, what role they play in investigations, and potential privacy concerns.[110] But the terms on which the government can access various types of sensitive non-content data merit their own debate and deliberation by Congress, independent of the (now largely resolved) debate over access to email content.

The Email Privacy Act unites the left, the right, privacy groups, and the business community.

Another objection comes from the Securities and Exchange Commission and other civil-enforcement agencies, which argue that the act will impede SEC investigations.[111] We understand the SEC's need for email content to perform its duties. But the SEC typically obtains email content directly from the subjects of its investigations rather than from providers; powerful sanctions, including contempt of court, are available if a subject refuses to comply. Indeed, the current SEC Chair has acknowledged that during her three-year tenure the Commission has not once subpoenaed content from a communications provider.[112]

High-tech law-enforcement tools, such as video surveillance paired with powerful analytic software, could have game-changing implications for personal privacy. (Aiestivak/Creative Commons)

As of this writing, there remains a chance that the Email Privacy Act will pass during the 114th Congress. But if it does not, the next president should, in the first 100 days of the new administration, call upon Congress to enact legislation requiring a warrant to obtain the content of email and documents stored in the cloud and imposing reasonable limits on nondisclosure orders. This would send a powerful signal that the new administration takes privacy seriously.

The new administration should then build on this call by launching a White House initiative to propose standards for government access to other types of sensitive data. These could include cell-site location data,[113] data generated by "internet of things" devices (from internet-connected cars, to home security systems, to medical devices), license-plate readers, facial recognition systems, and other foreseeable technologies with potentially game-changing implications for personal privacy. The initiative should bring together participants from technology, business, privacy, and national security backgrounds and should culminate in a White House summit highlighting the president's support for legislation addressing these issues.[114]

Congress, to its credit, has already begun considering the privacy implications of many of these technologies.[115] This suggests how salient they are to Americans across the political spectrum. A White House initiative would help earn the new administration political capital and public trust on digital-privacy issues while advancing a critical debate.

INTELLIGENCE TRANSPARENCY AND SECRET LAW

Recently, the government declassified 28 pages from the report of the Congressional Joint Inquiry into the 9/11 attacks. For years, the 28 pages' "secrecy ... made them almost mythical"[116] and spawned various conspiracy theories. Many believed, incorrectly, that the 28 pages contained damning proof that the Saudi government had foreknowledge of the attacks.

When the 28 pages were finally declassified, they turned out to be far less salacious than years of secrecy had led many to suspect. As *The New York Times* reported: "Subsequent investigations into the terror attacks pursued the leads described in the document and found that many had no basis in fact. But the mythology surrounding the document grew with each year it remained classified."[117]

The 28 pages are an object lesson in the risks of excessive secrecy and, simultaneously, an encouraging signal of the public's ability to handle the truth. They illustrate, as one expert told us, that a reflexive anti-disclosure stance has become an "anachronism." While they were secret, the 28 pages fueled years of conspiracy theories and speculation. Once declassified, they made a few days' worth of news and then faded into memory.

It is self-evident that most details of intelligence operations need to remain secret. Fortunately, it is not these details that are most important for democratic accountability, public trust, and political sustainability. The public needs to know and approve of the general contours of what intelligence agencies are empowered by law to do, and why, and have confidence that the agencies are being held to those limits. If unintended disclosures reveal that the scope of government surveillance is qualitatively greater than the public believed, or that oversight is qualitatively less effective, then public trust falters. And, as history shows, it is hard to win back. Important surveillance powers will be politically sustainable only if the public is persuaded that they are necessary, appropriate, and lawful.

In short, the public needs to know the broad strokes of what the government can do, why it needs those powers, and what legal and institutional constraints apply. The U.S. government can provide greater transparency – albeit at this high-altitude level of detail – without compromising the effectiveness of intelligence operations.

What would this mean in practice? Senior leaders should continue and expand efforts to demystify the NSA in the mind of the general public. To their credit, in the wake of the Snowden leaks, NSA leaders have utterly transformed the agency's attitude toward publicity, placing senior leaders in the public eye far more than ever before. Yet few Americans understand *why* the NSA does what it does. The case for robust signals-intelligence capabilities would be persuasive to most Americans if made forthrightly.

Importantly, however, this means making the case for signals intelligence beyond counterterrorism. There are many other valid purposes: Documenting foreign military activity, including in regions like Crimea or eastern Ukraine where the facts are disputed. Unraveling transnational criminal networks. Monitoring proliferation of weapons of mass destruction. Even traditional espionage against foreign governments serves purposes that are not nefarious and that the public would understand. Knowing the intentions and views of foreign governments reduces the risk of miscalculation and escalation. Counterintuitively, surveillance can sometimes help build confidence between countries that do not otherwise trust one another. One illustration of this effect is the Open Skies Treaty, which permits unarmed observation flights over member countries, including the United States and Russia, in order to "enhance mutual understanding and confidence."[118]

It is important to talk about these other purposes of signals intelligence. Limiting the public defense to counterterrorism alone invites a backlash when non-counterterrorism signals-intelligence programs are revealed. The authors repeatedly heard this critique from citizens of allied countries – "you say you use these capabilities for counterterrorism, but why are you spying on our government?" If other uses of signals intelligence are defensible, U.S. leaders should defend them on their own terms, albeit at a high enough level of generality to avoid endangering sources and methods.

Secretary of Defense Ash Carter speaks with NSA Director and U.S. Cyber Command Commander Admiral Michael S. Rogers at NSA headquarters. (Senior Master Sgt. Adrian Cadiz/DoD)

Finally, the next president should announce an administration-wide effort to reduce the amount of what some term "secret law" applicable to surveillance programs.[119] This should include several elements. Most broadly, the next president should publicly embrace the principle that all domestic surveillance or surveillance of U.S. persons overseas will be based on clear statutory authority, publicly interpreted, with sufficient oversight to hold the government to its construction of the statute.[120]

Limiting the public defense to counterterrorism alone invites a backlash when non-counterterrorism signals-intelligence programs are revealed.

The president should then task the General Counsels of the Office of the Director of National Intelligence, NSA, FBI, and CIA, and the Assistant Attorney General for National Security, in consultation with the PCLOB, with proposing, within six months, other ways to reduce the amount of classified legal interpretation and programmatic guidance governing electronic surveillance. This could include, where consistent with national security, further declassification of relevant presidential directives, agency procedures, interagency memoranda of understanding, opinions of the Justice Department's Office of Legal Counsel, and classified annexes to legislation.

Even those documents in these categories that cannot be safely declassified and published, however, should be shared, in a manner consistent with their classification and to the extent permitted by executive privilege, with the congressional intelligence committees.

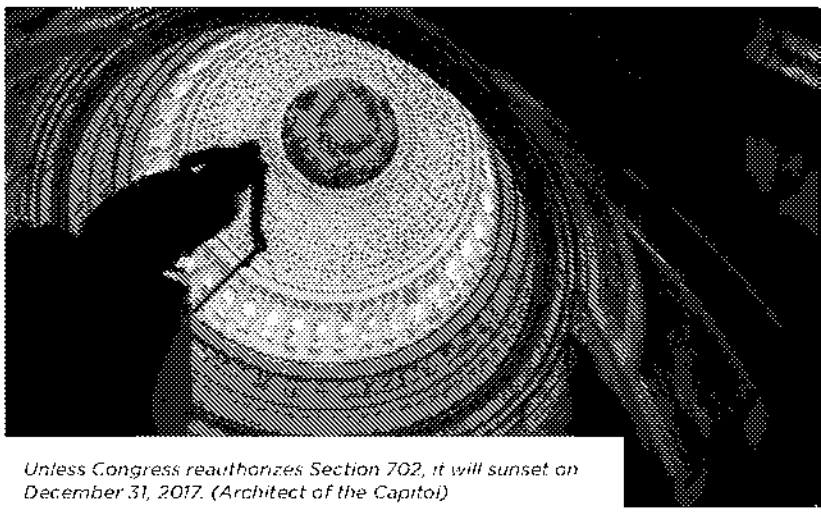
Finally, assuming that some residuum of secret law will unavoidably remain, this inquiry should consider measures to enhance accountability and public confidence. These might include "public notification of secret law's creation, presumptive sunset and publication dates," and creation of a shared repository of relevant "secret law" available to the responsible cleared officials from each of the three branches of government.[121]

SECTION 702 OF THE FISA AMENDMENTS ACT

Section 702 permits the government to acquire, with the compelled assistance of commercial providers, the communications of non-U.S. persons overseas. The government does not need to obtain individualized judicial orders for each target. However, the Foreign Intelligence Surveillance Court annually reviews the program and must approve a detailed "certification" specifying how the program will be administered and what safeguards are applied, jointly submitted by the Director of National Intelligence and the Attorney General.[122] The functioning of the program's two components, PRISM and "upstream," has been thoroughly described in the Privacy and Civil Liberties Oversight Board's report on Section 702.[123]

Title VII of the Foreign Intelligence Surveillance Act, which includes Section 702, will sunset on December 31, 2017, unless Congress reauthorizes it. This means that the next administration will have no choice but to publicly stake out a position on reauthorization and possible reforms to Section 702. This reauthorization process will be both an opportunity and a potential speed bump for the new administration's efforts to establish credibility on surveillance and digital-privacy issues.

Section 702 should be reauthorized, but with additional reforms to enhance public confidence, transparency, and privacy. Outside observers must rely on proxies in assessing this classified program's effectiveness. That said, the available evidence suggests that the program has become a vital intelligence tool, is legitimate in its basic contours, and is subject to adequate transparency in many, but not all, respects (more on that next page).



Unless Congress reauthorizes Section 702, it will sunset on December 31, 2017. (Architect of the Capitol)

TWO TYPES OF COLLECTION UNDER SECTION 702: PRISM AND UPSTREAM

PRISM collection under Section 702: "The government sends a selector, such as an email address," to a U.S.-based service provider. The provider is then "compelled to give the communications sent to or from that selector to the government." The NSA receives all PRISM data; the CIA and FBI receive some of it.

Upstream collection under Section 702: The NSA filters communications to or from the targeted selector directly from "the telecommunications 'backbone' over which telephone and Internet communications transit." Upstream also collects communications that *mention* the targeted selector in other fields of the message. Only the NSA has access to raw upstream data.

Source: Privacy and Civil Liberties Oversight Board, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (July 2, 2014)

Most notably, the authors are moved by the Privacy and Civil Liberties Oversight Board's measured but largely positive judgment in its comprehensive review of Section 702:

> Overall, the Board has found that the information the program collects *has been valuable and effective in protecting the nation's security and producing useful foreign intelligence.* The program has operated under a statute that was publicly debated, and the text of the statute outlines the basic structure of the program. Operation of the Section 702 program has been subject to judicial oversight and extensive internal supervision, and the Board has found no evidence of intentional abuse.[124]

What statistics are publicly available suggest that Section 702 has become a central foreign intelligence tool, particularly for counterterrorism. The Board reported that, at the time of its report last year, "*over a quarter* of the NSA's reports concerning international terrorism include information based in whole or in part on Section 702 collection, and this percentage has increased every year since the statute was enacted."[125] Qualitatively, the Board found that "[m]onitoring terrorist networks under Section 702 has enabled the government to learn how they operate, and to understand their priorities, strategies, and tactics"; that it "has led the government to identify previously unknown individuals who are involved in international terrorism"; and that it "has played a key role in discovering and disrupting specific terrorist plots aimed at the United States and other countries."[126] Overall, in 2015, the intelligence community targeted 94,368 overseas individuals, groups, or entities under 702.[127]

Other sources echo the Board's finding that Section 702 is a vital tool for counterterrorism and foreign intelligence more broadly. Matthew Olsen, former General Counsel of NSA and former Director of the National Counterterrorism Center, recently testified that Section 702 "has proven to be a vital authority for the collection of foreign intelligence to guard against terrorism and other threats to our national security" and "has significantly contributed to our ability to prevent terrorist attacks inside the United States and around the world."[128] The NSA has said that "Section 702 is the most significant tool in the NSA collection arsenal for the detection, identification, and disruption of terrorist threats to the U.S. and around the world."[129]

At the same time, Section 702 raises significant domestic civil liberties concerns — in particular, the "incidental" collection of the communications of U.S. persons and the subsequent use of such information. While the government cannot use Section 702 to target U.S. persons, their communications can be collected if they communicated with a target. Communications between two foreign persons may also contain information about a U.S. person.

What the agencies can do with incidentally collected information about U.S. persons is limited by "minimization" rules approved annually by the Foreign Intelligence Surveillance Court.[130] The minimization rules for the NSA, FBI, CIA, and National Counterterrorism Center are available online, with relatively few redactions.[131] Under the USA Freedom Act, significant FISC opinions, including the court's review of the 2015 Section 702 certification by the DNI and Attorney General, have been declassified and published.

Some have noted that, given these safeguards, "the criticism of Section 702 has focused on *hypothetical* rather than actual abuses of Section 702 authorities."[132] This is true, but hypothetical abuses are an appropriate concern where government is granted concentrated and largely secret power. Indeed, the basic design of the U.S. system of government reflects the Framers' fear of hypothetical abuses of centralized power.

President Barack Obama meets with FBI Director James Comey. (Pete Souza/Official White House Photo)

Beyond incidental collection itself, the most sensitive aspect of Section 702's operation is the FBI's ability to use U.S.-person identifiers to query Section 702 data – most controversially, in criminal investigations unrelated to national security. During the course of investigations, FBI agents and analysts typically search the Bureau's databases to see what it already knows about a particular person. One of those databases contains foreign intelligence information, including information from Section 702 and from traditional FISA.[133]

Critics describe such queries as "backdoor searches," arguing that they evade the Fourth Amendment limits that would otherwise apply to government attempts to collect Americans' communications.[134] The Foreign Intelligence Surveillance Court recently held that this practice comports with the Fourth Amendment.[135] Yet even if such searches are constitutional – a complex legal question we do not attempt to resolve here – searching foreign intelligence databases for information about Americans that was collected without a warrant raises serious privacy concerns.

On the other hand, there are also colorable reasons for not prohibiting such queries altogether. The 9/11 Commission found that the government's inability to synthesize pieces of information that different agencies already had – to "connect the dots," in other words – was a key failing that allowed the attacks to occur. If there is a connection between an FBI investigation in the United States and information the government has already collected under 702 – including the communications of known terrorists – it is important to be aware of that.

The limited public information about this practice means that estimates of its national security value are unavoidably conjectural. Additional clarity could help the FBI persuade observers that it is legitimate and necessary. To that end, the FBI should publicly explain with greater precision why it needs the ability to query databases containing 702 information for U.S.-person identifiers to perform its mission, notwithstanding that (i) where investigators lack probable cause (such as early in an investigation), they can use metadata or traditional investigative techniques to identify suspicious connections and thereby establish probable cause to obtain a warrant, and (ii) with a warrant, the Bureau can obtain information equivalent to any content collected under 702, and more, often without notice to the target of the investigation. The Bureau should provide this explanation during the upcoming 702 reauthorization debate.

To be sure, there may be persuasive answers to these questions; such queries may fill an investigatory niche that the posited alternatives would not. For example, it may be impracticably burdensome or unduly invasive of subjects' privacy to replace queries of information the Bureau already holds with additional investigation that gathers new information into the FBI's files. A more granular explanation of the role these queries play in FBI investigations and the suitability of posited alternatives would, if persuasive, help bolster the public legitimacy and sustainability of this practice.

Alternatively, a compromise solution could allow the FBI to continue to use these queries to identify problematic connections but avoid the most serious potential Fourth Amendment concerns. Specifically, during the upcoming authorization debate, Congress should ask the FBI whether it would be sufficient for it to continue to query databases containing 702 data for U.S.-person identifiers but, where such a search returns 702 information, to receive only the responsive metadata rather than the content. Responsive metadata, if it reveals a problematic connection, could then establish probable cause to view the underlying content.

Searching foreign intelligence databases for information about Americans that was collected without a warrant raises serious privacy concerns.

Congress and the American people would also benefit from additional information about the volume of such queries and the handling of 702 data that they return. It may be that disclosing more information about U.S.-person queries of 702 data would show that the scale of the potential privacy problem is less grave than feared. The FBI receives only a portion of the data collected through PRISM and none of the "upstream" data collected from the internet backbone.[136] It is apparently extremely rare for a query in a non-national-security investigation to return a hit in the FBI's FISA database. The existence of such a connection, while rare, may be a key element in unraveling a terrorist network or other transnational illicit activity. Moreover, only FBI personnel with special training in handling foreign-intelligence information are permitted to *view* responsive information; a query conducted by an agent or analyst without such training returns only a notification that responsive information exists.[137] Analysts without such training must now obtain a supervisor's approval before viewing the responsive information.

Additional information would help inform the public debate about how problematic this practice is from a privacy perspective, and about the scale of incidental collection more broadly. We therefore recommend that Congress, as a condition of reauthorization, mandate further transparency about several various aspects of the 702 program:

Require and enable NSA to fully implement PCLOB Recommendation 9. The Privacy and Civil Liberties Oversight Board recommended in its report on Section 702 that NSA assemble and declassify to the extent practicable several categories of information about the incidental collection, use, and querying of U.S.-person information. For various reasons, that recommendation has been only partially implemented.[138] Congress should incorporate these requirements into reauthorization legislation and, if needed, provide additional funding to enable NSA to comply.

Estimate the overall scale of incidental collection, if a valid and practicable methodology can be found. No one knows how voluminous incidental collection – that is, the collection of data about U.S. persons as an incidental result of permissible targeting of foreigners under Section 702 – actually is. As the PCLOB put it: "[L]awmakers and the public do not have even a rough estimate of how many communications of U.S. persons are acquired under Section 702."[139] The debate about whether Section 702's potential privacy harms outweigh its importance to national security would be better informed if Congress and the public had some idea of how much U.S.-person data is collected.

For obvious reasons, NSA does not review all data collected by the program to identify U.S.-person data. The government argues, reasonably, this would increase the privacy harm to Americans by putting human eyes on data that would otherwise go unreviewed and "age off" its servers after the retention period expires. A representative sample, as some members of Congress and privacy organizations have urged, would be less intrusive.[140] And NSA has conducted analogous statistical reviews before.[141]

That said, while a statistically valid estimate is desirable in theory, it may be difficult to achieve in practice.[142] The principal reason is that communications collected under Section 702 typically lack information that would enable officials to determine whether a U.S person is involved. An email, for example, does not necessarily make clear the nationality of the sender and recipient, much less those discussed in the body text.

These challenges are real, but efforts to surmount them should continue. The intelligence community should persist in seeking to develop an approach that would produce an accurate, statistically valid estimate of incidental collection. If those efforts do not succeed, the next administration and Congress should consider convening a technical working group, perhaps under the auspices of the National Academies of Sciences, Engineering, and Medicine, to consider alternative approaches.

Publish annually the number of instances in which an FBI query in a non-national-security investigation returns 702 information about a U.S. person. The Foreign Intelligence Surveillance Court "now requires the FBI to report to the Court," in detail, every time "FBI personnel view 702 information in response to a query in a non-national-security investigation."[143] While the details of these reports must remain classified, we can identify no national security harm that would result from publishing the overall number of such occurrences.

Estimate the total number of U.S.-person queries of databases containing 702 data conducted by the FBI in non-national-security criminal investigations. The FBI does not currently collect this information.[144] The reason is that its queries "do not distinguish between U.S. persons and others because nationality is not relevant to most criminal investigations."[145] The Bureau need not revamp its entire record-keeping system in order to produce such an estimate, however; a statistically representative sample of cases would suffice.

Provide more detail about which cybersecurity crimes the Department of Justice considers "serious crimes" for which it will use 702-derived information in a criminal proceeding. The General Counsel of the Office of the Director of National Intelligence has stated that the government "will use information acquired under Section 702 as evidence against a person in a criminal case only in cases related to national security or for certain other enumerated serious crimes," and only with approval by the Attorney General.[146] Those "enumerated serious crimes" include, inter alia, "crimes involving ... cybersecurity."[147]

This enumeration provides a constructive and basically adequate level of transparency here. That said, some have raised the specific concern that "'crimes involving cybersecurity' are undefined, and could be applied in an overbroad manner."[148] The spectrum of crimes falling under the rubric of "cybersecurity" is broad; for example, a federal appeals court recently held that unauthorized password-sharing can be prosecuted under the Computer Fraud and Abuse Act.[149] Some additional detail about what types of cybersecurity crimes the government will use Section 702 data to prosecute would help address these concerns.

Publish the Justice Department's standard for determining whether evidence introduced in a criminal proceeding is "derived from" 702 information. FISA requires the government to notify criminal defendants when it introduces into evidence information "derived from" 702.[150] The Justice Department has thus far refused to disclose publicly its standard for determining when this phrase is triggered. It is hard to see how national security would be harmed by the Department's further explaining how it interprets this legal obligation.[151]

Mandate the appointment of an amicus curiae in 702 certification proceedings. The USA Freedom Act included important reforms that enhanced the FISC's credibility – most notably, authorizing the court to appoint, from a pool of cleared advocates, amici curiae tasked with representing the public interest. One of these advocates, Amy Jeffress, raised such arguments in the FISC's review of the government's 2015 certifications for the Section 702 program. Her participation appears to have enhanced the rigor, and thus the public credibility, of that proceeding.[152]

Whether to appoint an amicus in a given case is currently up to the court,[153] but there is no apparent reason why an amicus would not have the same beneficial effect on every annual 702 certification proceeding. When Congress reauthorizes the FISA Amendments Act, it should require that one of the FISC amici be appointed to represent the public interest in the annual certification proceedings for Section 702.

Provide to the public as much detail as possible about the national security value of Section 702. The Privacy and Civil Liberties Oversight Board, along with credible current and former officials, have described Section 702's immense value for national security – albeit in general terms. The Office of the Director of National Intelligence should make every possible effort to add to these credible but relatively vague endorsements concrete details that demonstrate the program's value.

Taken together, these reforms will provide Congress and the public with a much stronger public record on which to assess Section 702 and weigh the program's potential privacy harms against its value for national security. Assuming, as seems likely, that the FISA Amendments Act will be again reauthorized with a sunset provision, these measures should bear fruit in time to usefully inform a future reauthorization debate.

THE PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

The Privacy and Civil Liberties Oversight Board has become a respected and important member of the constellation of oversight entities in this space. The Board's Section 702 report in particular was a landmark; its detailed, unclassified description of the program's basic operation has enabled a much more fact-based public debate about its value and privacy implications.

Importantly, the benefits of a robust Board extend beyond enhancing privacy and civil liberties; it benefits the national security community as well. The Board's judgments can help legitimize controversial programs. Precisely because of its independence, the Board's judgment that the 702 program is "valuable and effective" provides a powerful argument for reauthorization. More broadly, the Board's very existence and its reputation as a vigorous and independent voice strengthen the case that U.S. signals-intelligence programs are subject to robust, multi-layered oversight. This argument is particularly important in Europe, where the Board's existence and independence carry considerable weight.[154]

In short, the Board has been a success – but it is a fragile success. The Board's positive effect on U.S. credibility would evaporate, or even become a negative, if the Board were allowed to fade back into dormancy.

Unfortunately, there is reason to fear that this may happen next year. The Board's chairman resigned this year, and no replacement has been nominated.[155] This alone would be a problem, given that the Board's enabling statute permits only the chairman to hire staff.[156] Yet there are additional

concerns. Another member has been renominated but not reconfirmed; his extended term will expire when the Senate adjourns *sine die* in January.[157] A third member's term will expire in January and can be extended for only 60 days unless the new president nominates a replacement.[158] In sum, by early next year, the Board could be down to as few as two members – less than the quorum it needs to operate.

Accordingly, it is essential that the next president swiftly appoint new board members or reappoint existing members and work with the Senate to ensure that they are promptly confirmed. The Board's inherent bipartisanship means that there should not be a strong partisan valence here. And to ensure that the Board is not paralyzed in situations where it lacks a chairman, Congress should enact legislation permitting the remaining members to collectively appoint staff in the absence of a chairman, as the Senate Select Committee on Intelligence has proposed.[159]

The Privacy and Civil Liberties Oversight has been a success – but it is a fragile success.

In addition, in order to enhance the Board's ability to deliberate effectively, Congress should enact legislation exempting the Board from the Government in the Sunshine Act. The act requires that all Board meetings – vaguely defined as "deliberations" involving more than two members that "result in the joint conduct or disposition of official agency business" – take place in public.[160] To be sure, it is important that the Board involve the public in its work and reach official decisions in a transparent and accountable manner. But the Board's organic statute already provides for significant transparency, requiring the Board to make its meetings and reports "available to the public to the greatest extent that is consistent with the protection of classified information."[161]

The added requirements of the Sunshine Act impede effective collaboration and are a poor fit for the Board's work, for several reasons. First, unlike the regulatory bodies the act was designed to hold accountable, the Board exercises no regulatory authority – it can only perform oversight and offer nonbinding advice. In this context, the benefits of informal collaboration far outweigh any possible concern about opaque decisionmaking. Second, because the Board's work is overwhelmingly classified, it must expend inordinate time and energy following the act's cumbersome procedures for closing its many meetings covering classified subject matter.[162] Finally, since four of the Board's five members are part-time and have conflicting outside commitments, it is especially important that they be permitted to collaborate flexibly outside of formal meetings. The act makes informal collaboration unduly difficult.

Congress should remove this nuisance, which adds little and prevents the Board from being as effective as it might be. Alternatively, Congress should consider making all five Board members full-time, enabling them to devote themselves fully to the job.

Another concern is that legislation circumscribing the Board's authority could undermine its public credibility. Section 603 of the Senate's FY 2017 Intelligence Authorization Act would expressly limit the Board's jurisdiction to activities affecting the privacy and civil liberties "of United States persons."[163] To be clear, it is appropriate that the Board's activities focus on protecting the privacy rights of U.S. persons. But Section 603's express limitation to that effect is a solution in search of problem – and it risks creating several additional headaches. First, it would prevent the Board from responding to requests from the president, the intelligence community, or Congress to look into issues affecting the privacy interests of non-U.S. persons.[164] Second, and most importantly, it would unnecessarily suggest to European audiences that their privacy is not protected by the U.S. oversight infrastructure – a damaging prospect given that the survival of the Privacy Shield agreement will likely turn on just such perceptions.[165] Absent some future development that illustrates a compelling need for such a restriction, the Board's jurisdiction should not be expressly limited to considering the privacy rights of only U.S. persons.

Finally, Congress should not require the Board to keep the Director of National Intelligence or other elements of the intelligence community "fully and currently informed" of its activities.[166] Reporting to Congress is entirely appropriate and indeed essential – the Board, like other executive branch agencies, is subject to Congress' laws and funded by its appropriations. But a requirement to report to the agencies that the Board is meant to oversee impinges upon its independence, and thus its credibility. The Board's reliance on information provided by the intelligence community suffices to ensure that adequate working communication is maintained.

UPDATE WHISTLEBLOWER LAWS

Update Whistleblower Laws In the wake of Edward Snowden's leaks, many debated whether he would or would not have been protected by existing whistleblower laws.[167] Without wading into that debate here, the uncertainty surrounding the question was itself undesirable.

The law should clearly allow civil servants and contractors working in the intelligence community to report potential abuses within cleared channels – specifically, to their supervisors, to inspectors general, and ultimately to the congressional intelligence committees. On the other hand, it should not encourage those entrusted with classified information to take the law into their own hands and publish information that the people's democratically elected representatives have decided must be kept secret for reasons of national security.

Under current law, employees of the intelligence community who report abuses to their agency's inspector general or to the Intelligence Community Inspector General, and from there to the congressional intelligence committees, are protected against retaliatory personnel actions, including retaliatory revocation of their security clearances.[168] However, the statutory term "employee" likely does not apply to the many contractors working within the intelligence community. Presidential Policy Directive 19 (PPD-19), issued by President Obama in 2012, contains many similar protections, and administration officials have suggested that they view PPD-19 as at least partially applicable to contractors.[169] But that protection is at best unclear and could easily be rescinded by a future president.

To ensure that the scope of whistleblower protections is clear, the next president should issue an executive order making PPD-19's protections binding within the executive branch and clarifying that they extend to contractors working at all intelligence community components. Ultimately, Congress should extend the full panoply of statutory whistleblower protections to contractors working in the intelligence community.

The FBI, which is subject to its own agency-specific whistleblower regime, has had various struggles with whistleblower protection over the years.[170] In April, the Senate Judiciary Committee approved bipartisan legislation, co-sponsored by Chairman Charles Grassley and Ranking Member Patrick Leahy, to update the Bureau's whistleblower regime.[171] Among other changes, the bill would extend whistleblower protection to employees who report abuses to their supervisors as well as to the Inspector General and other officials designated by the Attorney General – an uncontroversial change endorsed by Attorney General Loretta Lynch and FBI Director James Comey.[172] The bill also clarifies that FBI employees can report alleged malfeasance to members of Congress[173] and to the Office of Special Counsel.[174] If this bill is not enacted during the 114th Congress, the next Attorney General should support legislation updating the FBI's whistleblower process in the next Congress.

The law should clearly allow civil servants and contractors working in the intelligence community to report potential abuses within cleared channels.

Protecting a Flourishing Technology Industry

The aftermath of the Snowden disclosures illustrated the severe repercussions that surveillance decisions can have for the American technology industry. This is not merely a concern for those companies' shareholders; it is also a national security concern. Economic strength and technological sophistication are fundamental pillars of national power. The United States' leadership in information technology is an important source of employment, wealth creation, and global influence. Information-technology companies create hundreds of thousands of high-paying American jobs. Tech is a leading export industry. And it produces immense advantages for the defense industrial base.

Less obviously, however, it is also an enormous advantage for the U.S. intelligence community and law enforcement that the world's leading internet companies are based in the United States and store much of their data here. For example, Section 702, NSA's "most significant" tool for collecting counterterrorism intelligence, works only because so much relevant data is held by U.S.-based companies or transmitted across internet cables that pass through the United States. In short, there are many reasons -- including national security reasons -- to ensure that surveillance policy does not endanger this golden goose.

The aftermath of the Snowden disclosures illustrated the severe repercussions that surveillance decisions can have for the American technology industry.

Surveillance decisions that harm the U.S. technology sector also drive a wedge between firms and the government. The Snowden disclosures "created an overall fear among U.S. companies that there is 'guilt by association' from which they need to proactively distance themselves."[175] Technology executives, understandably focused on retaining their customers' trust, recoiled from contact with the government and even took highly visible steps to enable their clients to prevent government surveillance. This harms intelligence and law enforcement efforts by making quiet cooperation between industry and government more difficult.

ENCRYPTION

The most prominent example of this backlash is the rapid adoption of strong encryption technologies across a range of widely used consumer products. The accelerated shift toward user-controlled encryption was largely a response to the Snowden leaks. For example, in the immediate wake of the disclosures, Eric Schmidt – whose company's overseas internal server-to-server links the NSA had reportedly accessed without the company's consent or knowledge[176] – said that "[t]he solution to government surveillance is to encrypt everything."[177] Later, in response to Director Comey's concerns about encrypted mobile devices, Schmidt responded: "The people who are criticizing this are the ones who should have expected this."[178]

Since then, leading companies have significantly expanded the use of encryption in their products – both with respect to "data at rest" on mobile devices and "data in motion" between end users. Most prominently, Apple devices running iOS 8 or later now feature full-disk encryption keyed only to the user's passcode. This makes it extremely difficult for law-enforcement officers to access data stored on a suspect's phone -- for example, a phone taken from an arrestee or captured in a raid on a terrorist safehouse -- unless the data is backed up to the cloud, the police learn the passcode, or officers seize the device while it is unlocked.

This means that these phones are inaccessible even if law enforcement has obtained a search warrant to access their contents.[179] Apple's privacy policy explains:

> For all devices running iOS 8 and later versions, Apple will not perform iOS data extractions in response to government search warrants because the files to be extracted are protected by an encryption key that is tied to the user's passcode, which Apple does not possess.[180]

The FBI's struggles to access the iPhone used by one of the San Bernardino shooters brought worldwide attention to the challenges device encryption poses for law enforcement – although it did not produce agreement on the severity of that problem or how to address it.

Meanwhile, Apple's iMessage, Facebook's WhatsApp, and other messaging services have introduced end-to-end encryption for data in motion across their services. This means that only the end users can read the content of messages in decrypted cleartext. As with device encryption, the end result is that providers cannot give law enforcement decrypted content, even in response to a warrant.

PROTECTING A FLOURISHING TECHNOLOGY INDUSTRY

Encryption

- Given the impasse over decryption legislation, and given that the debate itself has damaged relations between the government and the technology industry, the next administration should de-escalate the public debate over encryption.
- The FBI should support its argument for an encryption mandate by publishing more data about the precise contours of the technical challenge posed by encryption.
- To help the FBI cope with the status quo, Congress should scale up the FBI's resources for gaining access to encrypted devices and communications without compelled assistance from providers.
- This scaling up should also include resources to enable the FBI to create a centralized repository of expertise and technical assistance for the 15,000 state and local law enforcement agencies in the United States.

Risk Management in SIGINT Decisions

- Operations that, if exposed, would pose a significant risk to an American company or business sector should be approved by senior political appointees after a process that incorporates, to the greatest extent possible, external input about the scale of the risk.
- The government should create regularized channels for candid communication between NSA and the technology industry, such as creating an industry advisory board of corporate officials who hold security clearances.
- To the extent that a dialogue would, for some companies, raise concerns about appearing complicit in NSA practices, NSA should also establish a formalized one-way channel for receiving comment from American companies about the risks that signals-intelligence practices pose to their businesses and other issues of concern.
- Where the U.S. government wishes to obtain data held by a U.S. company, it should generally seek to access the data through the "front door" provided by U.S. domestic law rather than through overseas intelligence operations or liaison relationships.
- To the extent that the government contemplates operations that involve tampering with or introducing vulnerabilities into an American company's product before it reaches its end customer, any such operations should be approved by the National Security Advisor with input, where appropriate, from the Deputy National Security Advisor for International Economic Affairs, or another senior official with analogous responsibilities.
- The government should not, as a rule, pressure American technology companies to compromise their own products or hand over their source code.
- The government should not pressure American companies that sell to the government to disclose to it vulnerabilities that the company discovers before the company discloses them to other customers.
- The Vulnerabilities Equities Process should be formalized in an executive order.
- The executive order should, to the maximum extent consistent with national security, list all agencies that have a say in the process and should specifically state which agencies have a vote on whether to retain or disclose a vulnerability.
- In order to ensure that the process takes account of the broader interests of the U.S. technology sector, the Department of Commerce should have a regular seat at the table.
- The executive order should also describe the process to be followed in deciding whether to retain or disclose a vulnerability. In particular, it should clearly state the government's substantive standard for deciding whether a vulnerability's potential national security benefits outweigh the risks of retaining it.
- The executive order should also require that there be periodic review of whether a retained vulnerability should be disclosed.
- The executive order should provide for public annual reports containing as much detail about the process's operation as is consistent with national security, along with a classified annex for the relevant congressional committees.

iPhones protected by full-disk encryption have frustrated law enforcement. (Adrian Ilie/Creative Commons)

Encryption is becoming a serious challenge for law enforcement and counterterrorism. Law-enforcement agencies across the United States are accumulating piles of devices for which they have obtained or could obtain search warrants but which cannot be unlocked because of encryption. In Senate testimony last year, Manhattan District Attorney Cyrus Vance Jr. offered several specific examples of investigations thwarted by unbreakable encryption.[181] Government hacking, like the FBI's purchase of a "gray market" exploit in the San Bernardino case, may be an option in a few high-value cases. But it is difficult to scale and is not a realistic option for most of the 15,000 police departments across the country, which do not have the financial or technical resources of the FBI.

This is not just a law-enforcement problem; international terrorists are consciously using encrypted communications to enhance their operational security. Both ISIS and al Qaeda have made heavy use of Telegram, a Berlin-based app that touts its end-to-end encrypted "[s]ecret chats ... meant for people who want more secrecy than the average fella."[182] An ISIS operational-security manual specifically recommends that operatives use Telegram and other encrypted apps,[183] and ISIS recruiters commonly move to an encrypted platform after establishing contact with a potential recruit on social media.[184] The chief planner of last year's Paris attacks reportedly gave each operative "an email address to reach him on and a USB stick with an encryption key he was to download on his computer."[185] And those involved in the Paris plot reportedly used encrypted services, including WhatsApp and Skype, to communicate with operatives in Syria while they laid low between the Paris attacks and the subsequent attacks in Brussels.[186]

European allies, facing a wave of attacks planned or inspired by ISIS, are increasingly faulting encryption for obstructing terrorism investigations. For example, European officials blamed the failure to find those who planned the Paris attacks before they struck again on encrypted communications: "Everyone was trying to find these guys. ... They were able to elude us. But they were able to elude the Americans, too, and that shows you what a problem encryption is."[187] In the wake of repeated attacks in both countries, the interior ministers of France and Germany recently called for legislation requiring encryption providers to assist law enforcement in terrorism investigations.[188]

One common response is that law enforcement can use metadata, content stored in the cloud, or other information like geolocation data as a substitute for content made inaccessible by encryption.[189] Some even argue that these alternatives have created a "golden age of surveillance."[190] Government officials respond, however, that these are incomplete solutions. Metadata is often not as probative as content. Cloud backup may be unavailable or incomplete.[191] And government access to other forms of user data presents its own privacy challenges, which are only beginning to be confronted.

On the other hand, some of the solutions being proposed raise their own concerns. First, there is the risk that a decryption mandate would reduce the security of Americans' data. Requiring that companies retain the ability to decrypt data encrypted by their products would introduce a certain (albeit unquantified) degree of additional insecurity into those products. Adding complexity to software necessarily increases the risk that it will contain bugs for attackers to exploit. And requiring manufacturers to hold keys to devices they manufacture would create some risk of key theft – although an attacker would have to have both the key and physical possession of the device to capitalize on this.[192]

> ***There is the risk that a decryption mandate would reduce the security of Americans' data.***

It also bears noting that strong encryption's benefits are not limited to cybersecurity; it can also enhance *national* security, by shielding key U.S. government data and that of strategically important private actors from skilled adversaries. As Secretary of Defense Ash Carter has noted, the Department of Defense "is the largest user of encryption in the world, principally because our

troops need it. It helps keep our fighter jets and our sensor networks from getting hacked, it allows us to surprise our adversaries and it lets our people deployed around the world communicate securely with their families back home, from sailors aboard aircraft carriers to soldiers in Afghanistan."[193] In the private sector, strong encryption can help protect the intellectual property of defense contractors and other strategically important industries.[194] At the same time, it is unclear whether these national security needs call for encryption *that only the end user can unlock* – the feature most challenging for domestic law enforcement.

There are also serious concerns about the effect a decryption mandate would have on international human rights. Technologically advanced authoritarian states like Russia and China have powerful indigenous capabilities for surveilling their citizens and controlling the flow of information on the internet. Increasingly, however, technologically unsophisticated governments are also in on the game, as they can purchase high-tech monitoring systems and hacking tools from private companies.[195] China, appear intent on having access to their citizens' data regardless of what the United States does.[196]

This is not an artificial debate in which one side is completely wrong and the other is completely right; it is an authentically difficult policy conundrum in which various legitimate interests are in tension with one another. Unfortunately, some of the most prominent arguments in this debate have implied otherwise.

For example, senior law-enforcement officials have contended that the Fourth Amendment's "balance" requires that all evidence be amenable to search once police get a warrant.[200] The Fourth Amendment, however, merely *limits* the terms on which police can conduct searches; it does not require citizens to preserve evidence to facilitate those searches.

Meanwhile, opponents of a decryption mandate frequently argue that it is "mathematically impossible" to design a perfectly secure system for government access – or, as one put it, that a secure lawful-access mechanism is a "magic rainbow unicorn."[201] That may be true, but it mischaracterizes the argument. Supporters

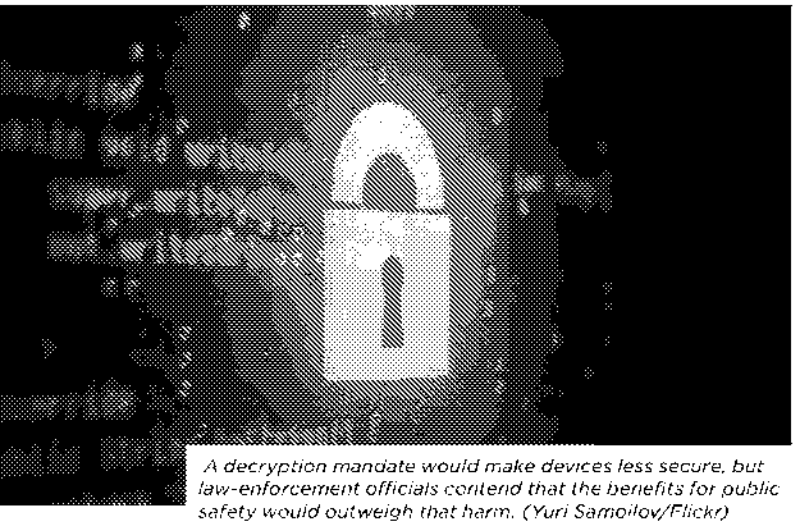
This is not an artificial debate in which one side is completely wrong and the other is completely right; it is an authentically difficult policy conundrum in which various legitimate interests are in tension with one another.

These developments challenge a longstanding principle of U.S. foreign policy: internet freedom, including secure communications for dissidents and journalists living in authoritarian countries. Each year, the State Department's Bureau of Democracy, Human Rights, and Labor (DRL) funds the development of secure communications technologies for use by dissidents overseas.[196] American companies and foundations have also supported the internet freedom agenda by funding technologies to enable secure internet browsing and communications.[197]

A U.S. decryption mandate would, to some hard-to-quantify extent, reduce the ability of vulnerable people living under authoritarian governments to communicate and browse the internet securely. U.S. companies are responsible for many, albeit not all, of the most secure communications technologies that are widely available to consumers. If the United States requires U.S. companies to retain the ability to decrypt data, it seems safe to assume that authoritarian governments would allow only iPhones with that exceptional-access mechanism into their markets.[198] On the other hand, powerful countries with large internal markets, such as Russia and

of such a law do not contend that a lawful-access mechanism would be perfectly secure; rather, they argue that any reduction in security would be manageable and justified by the benefits for public safety.[202] That is debatable, but it is not impossible. It would be informative to know how often comparable existing platforms have been penetrated in the past and what security flaws led to those breaches. Technologists should also undertake forward-looking, practical assessments of how great the reduction in security would be if a given approach to mandatory decryption were adopted.

Similarly, strong-encryption advocates frequently argue that any decryption mandate will be toothless because the truly "bad guys" would simply switch to non-U.S. products.[203] This would surely be true of terrorists, child pornographers, and other sophisticated criminals. But most Americans, including ordinary criminals who are not tech-savvy, would stick with the most convenient, user-friendly, and widely accessible products. In that scenario, unsophisticated or impulsive criminals would no longer benefit from unbreakable encryption. This would not eliminate the set of hard targets for law enforcement but would likely reduce it



A decryption mandate would make devices less secure, but law-enforcement officials contend that the benefits for public safety would outweigh that harm. (Yuri Samoilov/Flickr)

dramatically. And with a much smaller set of high-value targets, one-off solutions like placing malware on a suspect's computer or using zero-day exploits to hack a device[204] – which are too costly or labor-intensive to be used for a large number of routine cases – might be an adequate alternative.

Ideally, both sides would focus on developing the factual record to support their assertions. A pragmatic, factually oriented debate would be far more useful to most observers and members of Congress, who come to this debate willing to consider the arguments and legitimate concerns of both sides.

For now, there appears to be little prospect of a decisive resolution either way. Legislation like the Senate's Burr-Feinstein bill seems unlikely to pass absent a major terrorist attack or some other event that dramatically alters the political balance. The Obama administration declined to seek such legislation; indeed, a leaked National Security Council options memorandum on encryption did not even include "seek legislation" among the three options considered.[205]

Given this impasse, and given that the debate itself has damaged relations between the government and the technology industry, the authors recommend that the next administration, even if it maintains the Obama administration's wait-and-see posture, de-escalate the public debate over encryption. Deciding not to decide is a rational approach given that the relevant facts are not fully known and public opinion is not fully formed. That means taking steps to ensure that the entire government acts consistent with that approach. There is little sense in declining to seek decryption legislation yet simultaneously antagonizing industry by seeking to use existing laws to achieve the same ends. In a world of widespread strong encryption and no compelled-decryption law, government will need a collaborative relationship with industry to identify alternatives to encrypted data – for example, making optimal use of available cloud backups and metadata.[206] Government will also need industry's support to combat the use of social-media platforms to spread terrorist propaganda.[207] De-escalating this debate can create breathing room for quiet industry-government discussions.

As long as the present impasse prevails, policymakers should focus on developing the factual record and exploring the pros and cons of various courses of actions. A working group recently launched by the National Academies of Sciences, Engineering, and Medicine, made up of leading experts from academia, industry, and civil society, should help.[208] Another promising option would be a commission to study the issue and develop the factual record, as U.S. Rep. Michael McCaul and Sen. Mark Warner have proposed.[209] If Congress creates such a commission, its mandate should be limited to studying the scope of the problem, exploring the various technical alternatives, and considering possible harms to data security, privacy, human rights, U.S. technological leadership, and other important interests. Weighing those values against each other, on the other hand, calls for the type of sensitive value judgments that should be made by the people's elected representatives, as members of the House Energy and Commerce and Judiciary Committees have argued.[210]

> ***Government will need a collaborative relationship with industry to identify alternatives to encrypted data.***

Whether or not a commission is created, however, the FBI should support its argument for an encryption mandate by publishing more data about the precise contours of the technical challenge posed by encryption. Specifically, it should document the specific technical obstacles (e.g., device and operating-system versions) and surrounding circumstances (e.g., whether cloud backups and/or metadata were viable alternatives) encountered in cases where investigations have reportedly been impeded by encryption. The record that preceded the enactment of the Communications Assistance for Law Enforcement Act (CALEA) in 1994, which was far more quantitatively detailed than anything that has been produced on the encryption issue, is illustrative.[211]

Finally, the new administration and Congress should work to help the FBI and state and local law enforcement cope with the status quo. Among other things, this means scaling up the FBI's resources for gaining access to encrypted devices and communications without compelled assistance from providers. Germany, which has thus far not sought a decryption mandate, recently took similar steps: The government recently announced that it will create a new agency to help law enforcement and the domestic intelligence services break encryption and otherwise ensure that it is technically possible to carry out lawful surveillance.[212] In a world of widespread strong encryption, the most likely alternative to "back doors" or some other kind of decryption mandate is "lawful hacking" authorized by search warrants.[213] It may be an imperfect solution from a law-enforcement perspective, but it is the only solution that is feasible in the current political climate.

In a world of widespread strong encryption, the most likely alternative to "back doors" or some other kind of decryption mandate is "lawful hacking" authorized by search warrants.

This scaling up should also include resources to enable the FBI to create a centralized repository of expertise and technical assistance for state and local law enforcement. There are more than 15,000 law enforcement agencies in the United States – many of them small state or local departments without the resources to circumvent sophisticated encryption technologies or purchase vulnerabilities like that used to access the San Bernardino shooter's phone. The FBI's Criminal Justice Information Center serves as a national center of excellence and knowledge repository for fingerprint analysis; the Justice Department should explore and report to Congress how the Bureau could perform a similar role for communications technologies, and what resources it would need.

RISK MANAGEMENT IN SIGINT DECISIONS

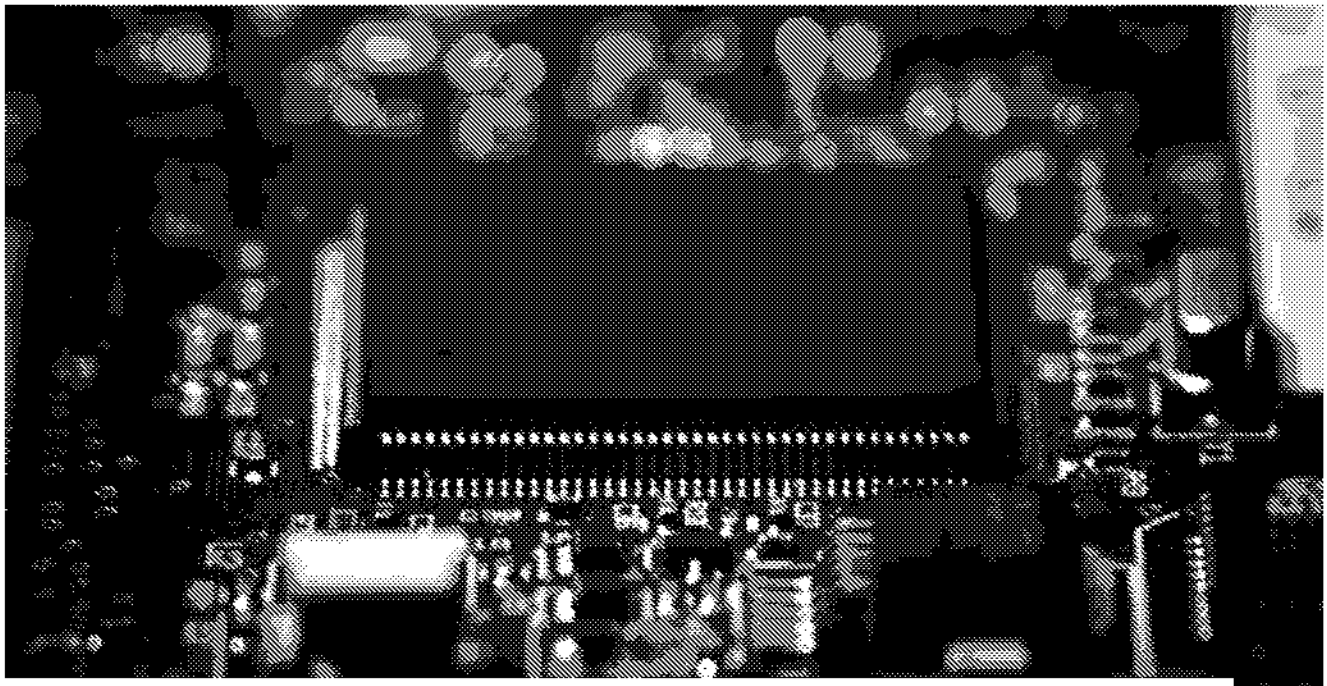
One of the indelible lessons of the post-Snowden period is that surveillance practices can pose a grave danger to the global business prospects of important American companies. In particular, surveillance practices that call into question the integrity or security of U.S. products endanger the technology industry's global competitiveness and give ammunition to foreign competitors, who may exploit NSA surveillance as a marketing tool.

Given the ubiquity of American technology, it is impossible to forbid altogether surveillance practices that implicate American products. But at a minimum, the government should do everything possible to ensure that (i) such operations are undertaken only where the national security ends justify the potential harms and (ii) the potential risks to American companies are accurately incorporated into the decisionmaking process. In the words of the President's Review Group, managing risk, including "risks to trade and commerce," is a "central task" of surveillance policy.[214]

There have been some positive steps in this direction. NSA Director Michael Rogers "determined one of the answers to" the NSA's reputational crisis "was to focus on strengthening and formalizing risk management."[215] NSA now has a "Chief Risk Officer" and has built an internal risk model that considers "disclosure, risk to U.S. foreign policy, risk to the U.S. technology sector, civil liberties and privacy."[216] (The model itself, and the weighting it assigns to each factor, are classified.) The Privacy and Civil Liberties Oversight Board recommended, and the intelligence community is reportedly developing, "a comprehensive methodology for assessing the efficacy and relative value of counterterrorism programs."[217] And the executive branch has reenergized the interagency Vulnerabilities Equities Process (VEP), which decides whether to exploit or disclose software vulnerabilities.[218]

While these steps are a promising beginning, more can and should be done to ensure that signals-intelligence practices collect needed information without creating unnecessary risks to the American technology industry. A good guiding principle is that operations that, if exposed, would pose a significant risk to an American company or business sector should be approved by senior political appointees after a process that incorporates, to the greatest extent possible, external input about the scale of the risk. The same is true of operations that, if revealed, pose strategic risks for U.S. foreign policy – a recognition embodied in President Obama's post-Snowden restrictions on surveilling foreign leaders.[219]

Unfortunately, such risk management appears to have fallen short in the pre-Snowden era. "While the



The Snowden disclosures undermined international confidence in the integrity of American hardware products. (Yuri Samoilov/Flickr)

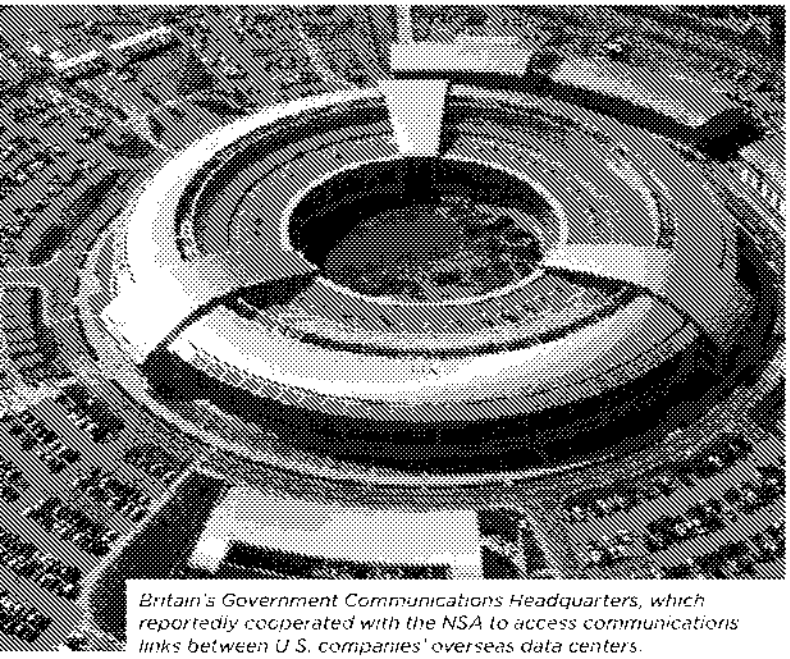
NSA excels at performing ... cost-benefit analysis at the tactical level," it does not seem to have adequately weighed "the risks of those efforts becoming front-page news."[220] Indeed, even when undertaking highly sensitive espionage on allied leaders, the intelligence community reportedly conducted no cost-benefit analysis that considered the risk that the operation could be exposed.[221] Senior administration officials with a broader political view and wider experience are better positioned to weigh economic and political risks than NSA officials focused on that agency's mission.

Industry is also understandably skeptical that the NSA has adequate information to accurately gauge risk to the U.S. technology sector, and to particular companies, when deciding whether an operation's overall costs exceed its benefits. Because the new risk model is classified, it is not publicly known how it assesses the risk to American companies' businesses and reputations or how much weight it assigns to that risk in the overall calculus. Companies worry that the NSA, given its institutional interests and limited understanding of their businesses, will give overriding weight to intelligence value while underestimating the risks to the technology industry and that sector's importance to the broader national interest.

To address this, the government should create regularized channels for candid communication between NSA and the technology industry. In addition to enhancing the government's understanding of risks to the industry, this channel could provide a forum for an ongoing exchange of views on issues of mutual concern, enhancing the quality and stability of public-private contacts on signals-intelligence issues. One way to do this would be to create an industry advisory board, potentially comprising corporate officials who hold security clearances.

To the extent that a dialogue would, for some companies, raise concerns about appearing complicit in NSA practices, NSA could also establish a formalized one-way channel for receiving comment from American companies about the risks that signals-intelligence practices pose to their businesses and other issues of concern.

Reports that the NSA had accessed data held by U.S. companies through clandestine intelligence operations overseas rather than the mechanisms provided by domestic law were a particularly significant source of post-Snowden friction.[222] It should be a selling point for U.S. companies that the data they hold is protected by the United States' legal regime for access by law enforcement and the intelligence community. That argument is undermined if the government collects such data in overseas operations not covered by the statutes and constitutional provisions that apply at home. Accordingly, where the U.S. government seeks data held by a U.S. company, it should generally seek to access the data through the "front door" provided by U.S. domestic law rather than through overseas intelligence operations or liaison relationships.[223]



Britain's Government Communications Headquarters, which reportedly cooperated with the NSA to access communications links between U.S. companies' overseas data centers. (GCHQ | Crown Copyright)

To the extent that the government contemplates operations that involve tampering with an American company's product without the company's consent, any such operations would pose a significant potential risk to the U.S. technology industry.[224] The backlash that followed the release of the infamous photo depicting a Cisco box illustrates how damaging the perception of NSA tampering can be, both for particular companies and for confidence in American technology more broadly.[225] If American technology products are less trusted abroad, American technological leadership and American workers will ultimately suffer.

To ensure that such operations are undertaken only when strictly necessary, we recommend that operations that involve tampering with or introducing vulnerabilities into an American company's product before it reaches its end customer, to the extent that the government contemplates such operations, should be approved by the National Security Advisor, with input, where appropriate, from the Deputy National Security Advisor for International Economic Affairs or another senior official with analogous responsibilities.

While it is hard to define with precision what operations should be subject to this requirement, the basic principle is the front-page test: If disclosure of the operation would undermine trust in the security and integrity of an American company's product, the operation should undergo high-level review and be formally approved by politically accountable officials who take into account the nation's security and economic interests. Unlike most recommendations in this report, this should probably be implemented quietly, without public fanfare, as the harm of reminding foreign customers that the government may occasionally undertake such operations may outweigh any remedial effect. As such, this change is probably best viewed as prophylaxis against future disclosures rather than remediating past harms.

More broadly, the government should not, as a rule, pressure American technology companies to compromise their own products or hand over their source code. Many foreigners believe that the U.S. government routinely obtains American companies' source code or that American technology products are pervasively compromised by the NSA. Non-U.S. companies have exploited the resulting skepticism to gain an advantage over their American competitors. Some hardened skeptics will never be persuaded, but frequent repetition by high-level officials that this is not U.S. policy can help make this belief less widespread.

Similarly, the government should not pressure American companies that sell to the government to disclose to it vulnerabilities that the company discovers before the company discloses them to other customers. This practice, which would allow the government to exploit vulnerabilities before they are patched by the company's other customers, would similarly undermine foreign customers' faith in American products.

THE VULNERABILITIES EQUITIES PROCESS

Some cyber operations exploit vulnerabilities that already exist but are not known to the company – which means that they cannot be patched.[226] These are known as "zero days" because the developer has had zero days to address them. Such offensive operations do not create new vulnerabilities, but the decision to exploit existing vulnerabilities rather than disclose them to the manufacturer necessarily allows them to persist, leaving ordinary users of the flawed product at risk.[227] One prominent example is the recent leak of a trove exploit code, believed by some analysts to have been exfiltrated from the NSA, by a group calling itself the Shadow Brokers.[228] The exploits reportedly incorporate zero-day vulnerabilities in networking products made by several American companies, including Cisco and Juniper – products "used by both private and government organizations around the world."[229]

On the other hand, there are instances in which the benefits of retaining a vulnerability outweigh the security costs of allowing it to persist. For example, the FBI's takedown of the notorious child-pornography

site "Playpen," which rescued "at least 26 child victims" from ongoing abuse, relied on a vulnerability in the Tor browser, although it is not known whether that flaw was a zero-day or was previously known.[230] Law enforcement and counterterrorism will only become more reliant on vulnerabilities as user-controlled strong encryption spreads.[231] If providers cannot access the content of encrypted messages, "the only way for law enforcement to read them is on the device, by essentially placing itself in the position of the end user."[232] And that will sometimes mean exploiting a vulnerability to gain access to the device.

> ***There are instances in which the benefits of retaining a vulnerability outweigh the security costs of allowing it to persist.***

In short, there is no way around the need for a case-by-case weighing of the interests at stake. In theory, the Vulnerabilities Equities Process created and later reenergized by the Obama administration reflects that need.[233] With the caveat that "there are no hard and fast rules," the White House Cybersecurity Coordinator laid out in a widely cited blog post nine factors relevant to the decision whether to disclose or retain a vulnerability.[234] That post also said that the process "is biased toward responsibly disclosing" software bugs, which accords with a recommendation of the President's Review Group.[235] NSA has said that it discloses 91 percent of the vulnerabilities it finds, although this fact alone is relatively uninformative absent more information about whether that 91 percent includes the most significant vulnerabilities and how long the NSA holds on to them before disclosing them.[236] A document declassified earlier this year provides substantial additional information about how the process is structured, albeit with extensive redactions.[237]

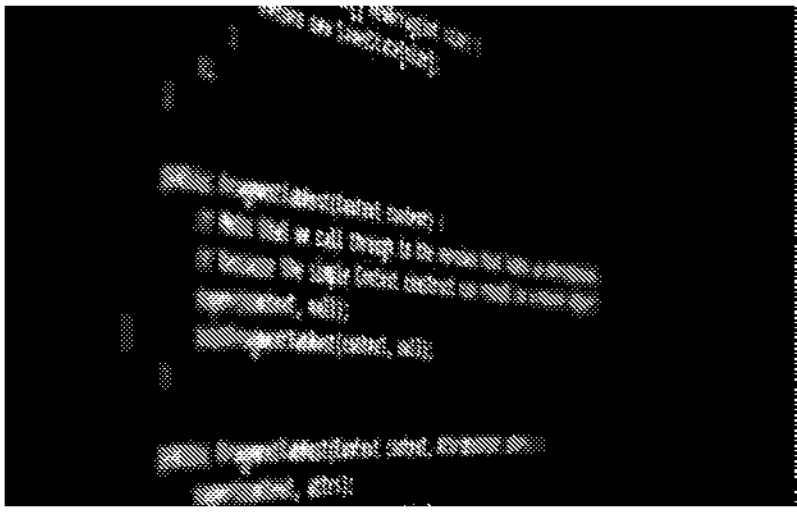
In practice, however, the process is widely perceived as insufficiently transparent and as likely to overvalue government interests relative to those of users and manufacturers. Most notably, the composition of the interagency Equities Review Board that decides by majority whether to withhold or disclose vulnerabilities remains classified.[238]

It is vital, as the White House Cyber Coordinator has noted, that Americans and the companies whose products are affected "have confidence in the integrity of the process" that the government "use[s] to make these decisions."[239] Today, however, "there is insufficient public information to evaluate whether the process is fairly designed ... and a lack of clarity regarding who and what is governed by it."[240]

A reform agenda for the VEP should aim to "generate public legitimacy through transparency and accountability."[241] The first step in enhancing the VEP's credibility would be formalizing the process in an executive order as part of a broader reset of the government's approach to commercial technology and risk management. As former White House cybersecurity officials Ari Schwartz and Rob Knake have explained, the current interagency agreement "does not carry the weight of an executive order signed by the president," so "there are few consequences for agencies that choose not to participate in the process."[242]

The executive order should, to the maximum extent consistent with national security, list all agencies that have a say in the process and should specifically state which agencies have a vote on whether to retain or disclose a vulnerability. To ensure that the process takes account of the broader interests of the U.S. technology sector, the Department of Commerce should have a regular seat at the table.

The executive order should also describe the "process to be followed in making a disclosure decision."[243] In particular, it should clearly state the government's substantive standard for deciding whether a vulnerability's potential national security benefits outweigh the risks of retaining it. Of course, those who apply this standard



In some instances, the benefits of retaining a vulnerability for law enforcement, foreign intelligence, or military uses will outweigh the cybersecurity risks of allowing it to remain unpatched.
(Yuri Samoilov/Flickr)

will have to apply their own judgment to determine the ultimate outcome in any given case. But short of an outright ban on retaining vulnerabilities – which would endanger national security and public safety – there is no way to structure this process that avoids relying on the case-by-case discretion of those at the table.

The executive order should also require that there be periodic review of whether a retained vulnerability should be disclosed.[244] We do not believe, however, that there must be a prescribed period after which every retention decision is reviewed, other than perhaps a presumptive outer limit. As with the retention decision itself, the facts of the case – namely, the intended use and the nature of the vulnerability – may themselves suggest what a natural period for reviewing a given decision would be. When the VEP decides that a vulnerability should be retained, the agencies involved should also agree to a period after which the decision will be reviewed.

Public reports, even at a high level of generality, will enhance democratic accountability and public oversight, and thus the credibility of the process.

Finally, the executive order should provide for public annual reports containing as much detail about the process's operation as is consistent with national security, along with a classified annex for the relevant congressional committees. Under the existing process, the program's executive secretariat (at NSA) prepares and disseminates what appear to be quite detailed annual reports, but these are distributed only to the participating agencies.[245] Public reports, even at a high level of generality, will enhance democratic accountability and public oversight, and thus the credibility of the process.

These changes will not satisfy those who believe that retaining vulnerabilities is never, or almost never, appropriate. If, however, it remains government policy to retain some number of useful vulnerabilities for intelligence and law-enforcement purposes, these recommendations will do much to ensure that the process for making those decisions is relatively transparent and as credible as possible.

Mitigating the International Consequences of Surveillance Policy

The recommendations in this section address the international effects of U.S. surveillance policy. That includes diplomatic consequences, harms to the American technology sector's international prospects and preeminence, and effects on U.S. "soft power" and global influence.

The Snowden revelations triggered immediate repercussions in each of these areas. Surveillance against foreign leaders, including Germany's Angela Merkel and Brazil's Dilma Rousseff, strained diplomatic ties with affected countries.[246] U.S. companies encountered newfound skepticism from foreign customers.[247] The European Court of Justice's decision invalidating the U.S.-EU Safe Harbor agreement plunged transatlantic data transfers, and the billions of dollars in commerce dependent on them, into uncertainty.[248] Public trust of the United States declined in important allied countries.[249] Authoritarian states seized the opportunity to suggest a false moral equivalency between the United States' surveillance practices and their own.

The Obama administration took a number of important steps to attempt to repair the international consequences of the leaks: It created a new "protected list" placing certain allied leaders' private communications off-limits for the NSA.[250] It created a bilateral Cyber Dialogue with Germany, providing a forum to work through major post-Snowden disagreements.[251] It negotiated the new Privacy Shield agreement to replace Safe Harbor. Most importantly, Presidential Policy Directive 28 recognized that surveillance policy should respect the privacy interests of non-U.S. persons and required intelligence community elements to adopt policies and procedures to do so. This is a historic commitment – one matched, as far as we are aware, by no other country.

With these reforms on the books, the United States has a comparatively good story to tell on legal and institutional control over its intelligence community. Unfortunately, the actions the United States took in reaction to the post-Snowden blowback are not widely known among European publics. And European institutions have continued to pressure the United States over surveillance despite the fact that U.S. law and policy governing electronic surveillance and government access to data are stronger than analogous European restrictions. To some extent, this reflects European governing institutions' separation between national security and data privacy, both at the European and national levels. Data privacy and cross-border data transfers are subject to European Union regulation, while national security is the exclusive province of national governments. On the

MITIGATING THE INTERNATIONAL CONSEQUENCES OF SURVEILLANCE POLICY

Surveillance Diplomacy and PPD-28

- The next administration should offer to hold a political dialogue, among willing allies with similar rule-of-law cultures, on norms to govern surveillance of one another's citizens and institutions.
- This dialogue should seek to exchange high-level, public, political (rather than legal) commitments analogous to the public commitments the United States has already made, most notably in PPD-28.
- These discussions should also include mutual, public, high-level commitments about the purposes and boundaries of "liaison" cooperation between one another's intelligence services – in particular, the circumstances in which they will exchange information about one another's citizens.
- In order to encourage allied governments to enter into such discussions and extend appropriate privacy protections to the American people, the United States should make clear to allied publics and their governments that while it is prepared to commit itself to protect their privacy, the American people's privacy deserves equivalent respect and it expects such protections to be reciprocated.
- The next administration should reaffirm that PPD-28's basic recognition that signals-intelligence activities must consider the basic dignity and privacy of all people, and the fundamental commitments of Section 1 of PPD-28 (signals-intelligence activities must be be authorized by law; no use for discrimination or suppressing dissent; no espionage for commercial advantage of U.S. companies; narrow tailoring), will remain applicable to all countries and their citizens without regard to their own governments' policies.
- The new administration should announce that after one year, the heightened commitments in PPD-28 Sections 2 and 4 will be guaranteed only to citizens of countries that agree to extend comparable protection to Americans. There is no reason why other countries, and particularly U.S. allies, should resist extending to Americans the same consideration that the U.S. government grants to their citizens.
- The next administration should also offer to elevate these commitments to an executive order for countries that make credible reciprocal promises.
- The United States should insist that European Union member states grant to Americans the same judicial-redress rights and access to a surveillance "ombudsperson" that the United States extended to Europeans under Privacy Shield.
- The United States should demand that allied countries publicly commit not to spy on one another's nationals for the economic benefit of domestic companies – a practice the United States has long forsworn but some close allies have not.
- The next administration should also make clear that it will consider excluding from any list of allied leaders whose personal communications are off-limits from surveillance the leaders of any country that refuses to publicly renounce economic espionage against American companies.
- The next administration and Congress should establish regularized, formal exchanges between congressional, judicial, and executive branch compliance and oversight bodies, including the Privacy and Civil Liberties Oversight Board, and their foreign counterparts.

Public Diplomacy

- The United States should explain, in a modest and factual manner, the many ways in which the U.S. intelligence community supports Europe in its fight against terrorism.
- The intelligence community should, with as much specificity as is consistent with national security, offer greater detail about how much and what kind of counterterrorism data the United States shares with European partners, as well as the types of information it receives from them.
- The next administration should also consider raising the profile of joint counterterrorism efforts by making American ambassadors and senior national security officials available to discuss them with local media, and asking European counterparts to publicly acknowledge the cooperation.

Privacy Shield

- While legal challenges are pending, U.S. officials should seek to foster a climate conducive to ensuring that Privacy Shield passes judicial muster.
- This includes continuing to make the case that U.S. and European privacy protections are, at a minimum, "essentially equivalent."

- U.S. officials should also seek to publicly reinforce the significance of the new ombudsperson mechanism and the Judicial Redress Act.
- Consumer-protection officials should work to publicly demonstrate that Privacy Shield's consumer protections are being rigorously enforced.
- American ambassadors in Europe and visiting U.S. government principals should be encouraged to highlight U.S. privacy protections and emphasize that in the United States, as in Europe, the right to privacy is a fundamental right.
- The next administration should begin to consider what the United States' response will be, other than further concessions, if Privacy Shield is struck down.
- It should also begin communicating quietly to European partners that while the United States respects their legal institutions, shares their values, and has taken every reasonable measure to help European partners satisfy the Court of Justice, the United States has a "Plan B" and will not respond to another flawed, Schrems-like decision with more unilateral concessions.
- To amplify this message, Congress should consider legislation providing that if a judicial decision restricts data transfers from Europe to the United States, the same limitations will apply to data transfers from the United States to Europe by European companies.

Cross-Border Data Requests

- If the Justice Department's proposal does not pass during the current Congress, the next administration should seek, and Congress should enact, similar legislation authorizing executive agreements on cross-border data requests.
- Once the enabling legislation is enacted, the executive branch should move quickly to conclude executive agreements with countries with similar human-rights and rule-of-law standards.
- Legislation creating an alternative to the Mutual Legal Assistance system should be accompanied by parallel efforts to streamline the existing system.

national level, data-protection authorities are politically independent but lack authority over their own governments' national security practices.

The upshot is that the European institutions that criticize the U.S. government's surveillance practices and penalize American companies have no official responsibility to reconcile their criticisms with their own governments' comparable practices. Indeed, under European and national law, they often have no legal *authority* to do so. Even more frustrating for U.S. national security officials is that European security agencies quietly ask their American counterparts for intelligence produced by U.S. surveillance practices even as the privacy officials of the same governments are publicly blasting those practices – sometimes, we have heard, on the same day. Put simply, in many European governments, one hand does not know, or does not wish to know, what the other hand is doing.

This dissonance between European privacy policy and national security policy has hurt U.S. national interests – most notably, in the disruptive Safe Harbor decision. U.S. policy should seek to alter this status quo in three ways. First, it should seek to encourage, in an appropriate and amicable way, what should be a favorable comparison between U.S. and European legal restrictions applicable to electronic surveillance. Second, it should incentivize European governments to reconcile their own interest in preserving transatlantic data flows and U.S. investment in Europe with their data-protection authorities' and courts' apparent urge to use commerce in data as leverage to pressure the United States over surveillance. And third, it should seek to raise awareness among European publics of the ways in which the U.S. intelligence community supports their security from terrorist attacks and other threats.

Importantly, this does not mean limitless apologies or one-sided concessions. To the extent that reasonable *mutual* concessions would help further these aims, the next President should seek them. But the next administration will also be called, respectfully but firmly, to defend the United States' record and identify appropriate ways to ensure that important national interests are not imperiled by the decisions of European institutions.

SURVEILLANCE DIPLOMACY AND PPD-28

President Obama's Presidential Policy Directive 28 makes broader commitments to protect the privacy interests of foreigners in signals-intelligence collection than the policy or law of any other country of which we are aware. The closest comparable statement we have found is in Germany's recent law regulating domestic collection of foreign-foreign communications. That law

contains special protections for EU institutions, EU member states, and EU citizens, but no heightened protection for Americans.

The United States' legal and oversight regime governing domestic intelligence collection – including domestic collection against foreigners – is also equivalent to or stronger than the systems in place in leading European countries.[252] For example, only two of the leading EU member states surveyed in a review by the law firm Sidley Austin "require judicial authorization for intelligence surveillance, and most place such authorization in the hands of government ministers."[253] France, Germany, the United Kingdom, and the Netherlands all "explicitly permit certain types of surveillance that are not targeted at identified suspected individuals"[254] – that is, arguably, the type of "generalized" collection to which the Court of Justice objected in the *Schrems* decision. None of these countries' laws explicitly require minimization, and retention limits apply only to a few narrow categories of data.[255]

By contrast, in the United States all intelligence surveillance under Title I of the Foreign Intelligence Surveillance Act and criminal surveillance under the Wiretap Act (Title III) requires an individualized judicial order based on probable cause. Domestic surveillance of non-U.S. persons overseas under Section 702 requires individualized targeting, is subject to annualized judicial oversight by the Foreign Intelligence Surveillance Court, and is governed by minimization procedures that must be submitted by each participating agency and approved by the court. Even data on foreigners collected overseas is subject to a presumptive five-year retention period.[256] The United States also has robust congressional intelligence committees, "significant internal compliance and auditing mechanisms" within the executive branch, "embedded privacy and civil liberties officials and powerful and autonomous inspectors general," and the independent Privacy and Civil Liberties Oversight Board.[257]

American national security experts frequently lament that European privacy advocates criticize U.S. practices while being unaware of, or overlooking, the fact that their own intelligence agencies do similar things but are subject to fewer legal constraints and less oversight than their American counterparts. In the recent Privacy Shield negotiations, for example, EU negotiators demanded and obtained expanded rights of judicial redress in the United States for EU citizens and the creation of a State Department ombudsperson to receive Europeans' complaints about U.S. intelligence practices. Yet Americans receive none of these protections in the European Union – indeed, to the authors' knowledge, they were not offered.

Even more troubling, the United States' existing, unreciprocated concessions are not widely known abroad and have generated little goodwill for the United States. For example, one German expert told us that most Germans are "totally unaware" of PPD-28 – arguably the most significant commitment ever made by a major power to the privacy interests of foreigners. The United States should welcome a comparison between its legal and oversight regime and that of its European allies.

Fortunately, this should be an opportune time for a more mature, two-way transatlantic dialogue about surveillance. The political dynamics surrounding surveillance issues in Europe have been subtly changing, even before recent terrorist attacks. In Germany, a leader on data-privacy issues, a parliamentary committee created to investigate the NSA's activities ended up uncovering an array of controversial activities by Germany's own foreign intelligence service, the *Bundesnachrichtendienst*. This has triggered an unprecedented period of public debate and reflection about espionage and oversight. Meanwhile, in the wake of repeated terrorist attacks, public opinion in key European countries has swung dramatically toward expanded surveillance powers. France has been under a state of emergency for almost a year. In July, the United Kingdom's House of Commons passed the Investigatory Powers Bill, which gives authorities significant new surveillance powers and requires companies to help authorities break encryption in some situations.[258] Most recently, in the wake of several terrorist attacks, Germany's governing coalition has proposed a tough new set of counterterrorism measures.[259] In a Europe under regular attack by ISIS, governments are likely to conduct more surveillance and share information more widely.

The United States' legal and oversight regime governing domestic intelligence collection – including domestic collection against foreigners – is equivalent to or stronger than the systems in place in leading European countries.

Changing dynamics in Europe provide an opening for a more honest, less adversarial transatlantic dialogue on surveillance policy. (Pete Souza/Official White House Photo)

These developments have created an opportunity for a more productive, less adversarial transatlantic discussion on surveillance policy – including an honest comparison of legal and oversight regimes. The question for the next administration is how to encourage this comparison and raise awareness of the United States' record in a manner that is seen as productive and collegial rather than boastful and adversarial. One reason the commitments in PPD-28 are not widely appreciated is that they were offered as unilateral concessions rather than reciprocal exchanges between partners. Put differently, these concessions may well be more widely valued and known in Europe if Europeans were asked to give something in return.

To that end, the next administration should offer to hold a political dialogue, among willing allies with similar rule-of-law cultures, on norms to govern surveillance of one another's citizens and institutions. This differs from the recommendation of the President's Review Group that the United States seek to enter into a "very few new" bilateral "understandings or arrangements regarding intelligence collection guidelines and practices with respect to each other's citizens," analogous to the so-called Five Eyes arrangement among the United States, the U.K., Canada, Australia, and New Zealand.[260] The discussions proposed here would entail neither the detailed commitments nor the intensive intelligence coordination of the Five Eyes arrangement. Nor would they result in the type of "no-spy" agreement that Germany reportedly sought after the Snowden disclosures.

Rather, these would be high-level, public, political (rather than legal) commitments analogous to the public commitments the United States has already made, most notably in PPD-28.[261] For example, the United States should ask partners to mutually agree:

- To incorporate in their signals-intelligence practices protections for the privacy interests of one another's citizens.[262]
- To publish, with the maximum detail consistent with national security, agency procedures implementing such protections, including minimization requirements limiting the dissemination and retention of personal information of one another's citizens.[263]
- To establish a presumptive time limit for retaining the personal information of one another's citizens.[264]
- To agree to limitations on the use of signals intelligence collected in bulk.[265]
- To designate a senior official to serve as a point of contact for implementation of these commitments and other concerns related to signals-intelligence practices.[266]

- To require individualized judicial approval for electronic surveillance of one another's citizens when on the other country's territory.[367]

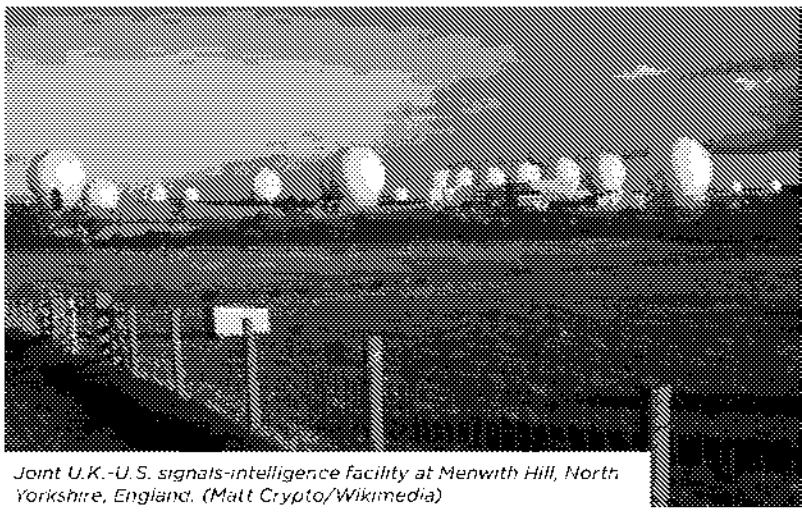
These negotiations would be an opportunity for the United States to demonstrate its good faith and strong bona fides on these issues, but also to subtly invite a comparison between its own practices and those of its allies. If U.S. allies are as committed to privacy as they contend, they should be eager to sign on to these commitments. If not, they should explain to their publics and the world why they refuse to.

These discussions should also include mutual, public, high-level commitments about the purposes and boundaries of "liaison" cooperation between one another's intelligence services – in particular, the circumstances in which they will exchange information about one another's citizens. While cross-border spying receives the most attention, people ultimately have the most to fear from their own governments, who after all wield direct coercive power over their lives, liberty, and property. Limits on such cooperation exist, but most are classified. More transparency would increase the democratic legitimacy of such cooperation and help dispel suspicions that services use liaison cooperation to evade their own domestic legal restrictions.

It is possible that other governments will be reluctant to enter into the type of discussions we envision here. To ensure that allied governments are adequately motivated to enter into such discussions and extend appropriate privacy protections to the American people, the United States should make clear to allied publics and their governments that while it is prepared to commit itself to protect their privacy, the American people's privacy deserves equivalent respect and it expects such protections to be reciprocated.

The new president's review of PPD-28 will provide an opportunity to give effect to this demand for reciprocity. PPD-28's basic recognition that signals-intelligence activities must consider the basic dignity and privacy of all people, and the fundamental commitments of Section 1 of PPD-28 (signals-intelligence activities must be be authorized by law; no use for discrimination or suppressing dissent; no espionage for commercial advantage of U.S. companies; narrow tailoring), should remain applicable to all countries and their citizens.

As for the heightened commitments in PPD-28 Sections 2 and 4 – for example, limits on how long intelligence agencies can retain non-U.S. persons' data – the new administration should announce that after one year, these protections will be conditioned on other governments' extending comparable protection



Joint U.K.-U.S. signals-intelligence facility at Menwith Hill, North Yorkshire, England. (Matt Crypto/Wikimedia)

to Americans. There is no reason why other countries, particularly U.S. allies, should resist extending to Americans the same consideration that the United States grants to their citizens. Indeed, the desire to retain PPD-28's protections should help stimulate in allied countries the political will to do so. The next administration should also offer to elevate PPD-28's commitments to an executive order for countries that make credible reciprocal promises.

Some might argue that adding conditionality to PPD-28 would be damaging for privacy standards globally. We understand this argument and appreciate the importance of PPD-28 for the United States' global moral authority on surveillance practices. Our hope, however, is that if this proposal were adopted, there would not be any rollback of PPD-28 because other countries would choose to retain the protection of all of its provisions by making reciprocal commitments to the American people.

Indeed, making these commitments reciprocal would substantially *enhance* privacy, for several reasons. If, as we expect, a significant number of countries accept this reciprocity and make the necessary commitments, it would be a substantial victory for privacy and surveillance under law around the world. Americans would gain new privacy protections from other governments. Citizens of other countries would gain new insights about their own governments' surveillance practices. Elevating PPD-28 to an executive order (at least for reciprocating countries) would also add a degree of permanence, enhancing its public credibility. Finally, one might argue that it would inappropriately disserve Americans' privacy to preserve these concessions for foreign citizens without using the leverage they provide to elicit equivalent protections for Americans.

There are other commitments that the authors do not believe can be made conditional, but which the United States should nonetheless make clear to its allies that it expects them to reciprocate. First, the United States should insist that EU member states grant to Americans the same judicial-redress rights and access to a surveillance ombudsperson that the United States extended to Europeans under Privacy Shield. There is no defensible ground for granting these protections to Europeans but not Americans. If the European Union wishes to deny Americans the same protections it has demanded for its own citizens, the United States should at least ensure that it is forced to publicly defend this inequity.

Second, as part of the bilateral and potentially multilateral discussions we envision, the United States should demand that allied countries publicly commit not to spy on one another's nationals for the economic benefit of domestic companies – a practice the United States has long forsworn but that some close allies have not. For example, former Secretary of Defense Robert Gates has "singled out France as particularly aggressive in its use of economic espionage."[268] The United States should not be harangued into unilateral privacy concessions by countries whose surveillance practices include "stealing American defense technology" and "bugging American business executives."[269] The next administration should also make clear that it will consider excluding from any list of allied leaders whose personal communications are off-limits from surveillance the leader of any country that refuses to publicly renounce such economic espionage against American companies. Even China has publicly promised not to conduct economic espionage for commercial advantage. It is not unreasonable to ask the same of U.S. allies.

Finally, it is not realistic or practical for the reciprocal commitments we envision to be legally binding or enforced by judicial review. For the type of high-level political commitments envisioned here, equivalently high-level political safeguards should be adequate to hold countries to their commitments, broadly speaking. The most basic protection is that such reciprocal commitments should only be made with countries that have rule-of-law and governance cultures in which such commitments are taken seriously and internally enforced. However, to reassure participating countries' publics that both countries are implementing their commitments, the next administration and Congress should establish regularized, formal exchanges between congressional, judicial, and executive branch compliance and oversight bodies, including the Privacy and Civil Liberties Oversight Board, and their foreign counterparts.

PUBLIC DIPLOMACY

Another persistent frustration we encountered among American national security officials is the discrepancy between their European counterparts' view of U.S. signals-intelligence and counterterrorism practices and European *publics'* view. European counterterrorism efforts rely heavily on data provided by the U.S. intelligence community: The United States reportedly sends to Europe vastly more counterterrorism intelligence than Europe sends back. Yet European publics hear an account of U.S. surveillance practices, including from their government officials, that is almost relentlessly negative. One senior European security official told the authors that her country's citizens do not understand the scale of American counterterrorism intelligence sharing "at all."

This has produced a warped understanding of the consequences of U.S. intelligence practices, in which privacy costs are highlighted and security gains largely ignored. Yet with jihadist attacks striking at Europe's heart, the political dynamics are changing. European leaders who three years ago felt the need to distance themselves from U.S. intelligence practices are now willing to publicly highlight enhanced intelligence sharing with the United States.[270] The United States should take this opportunity to explain, in a modest and factual manner, the many ways in which the U.S. intelligence community supports Europe in its fight against terrorism. For example, after the terrorist attacks in Paris in November 2015, the White House deployed American counterterrorism experts to European capitals "to help Western European allies shore up their defenses and borders."[271] The Brussels attacks in March and subsequent attacks in France and Germany illustrate how vital this support remains. Unfortunately, this assistance was, as *The New York Times* wrote, "little-noticed."[272]

This support is the right thing to do and should persist regardless of whether it is publicly appreciated. Yet it is in the U.S. national interest that European publics become aware of how U.S. intelligence cooperation – including intelligence generated by the NSA's electronic surveillance – helps protect them from terrorism. Skepticism about U.S. intelligence practices continues to harm the United States, as the invalidation of the Safe Harbor agreement demonstrates. Greater European public awareness of these benefits can help reduce that damaging skepticism.

Of course, a public relations tour trumpeting U.S. counterterrorism assistance would be distasteful and counterproductive. And the United States should not imply that counterterrorism is the *only* purpose of U.S.

signals-intelligence collection. That is not true, and U.S. officials would lose credibility by suggesting it. That said, counterterrorism is a central purpose, and there are ways to raise European publics' awareness of how U.S. intelligence supports their security without boasting or overstating the case. At a minimum, the intelligence community should, with as much specificity as is consistent with national security, offer greater detail about how much and what kind of counterterrorism data the United States shares with European partners, as well as the types of information it receives from them.

awareness of the relative strength of the legal restrictions on intelligence activities in the United States and Europe. The effect on the legal proceedings involving Privacy Shield would be another important benefit of such an initiative.

U.S. officials should also seek to publicly reinforce the significance of the new ombudsperson mechanism and the Judicial Redress Act, which extends to Europeans the rights Americans enjoy under the 1974 Privacy Act.[276] Consumer-protection officials should work to publicly demonstrate that Privacy Shield's consumer protections are being rigorously enforced.[277] And American ambassadors in Europe and

It is in the U.S. national interest that European publics become aware of how U.S. intelligence cooperation – including intelligence generated by the NSA's electronic surveillance – helps protect them from terrorism.

The next administration should also consider raising the profile of joint counterterrorism efforts by making American ambassadors and senior national security officials available to discuss them with local media, and asking their European counterparts to publicly acknowledge the cooperation. Public commitments regarding the purposes of intelligence cooperation and exchanges between data-protection authorities and oversight officials, both recommended elsewhere in this section, should help mitigate potential civil-liberties concerns arising from this cooperation.

visiting U.S. principals should be encouraged to highlight U.S. privacy protections and emphasize that in the United States, as in Europe, "the right to privacy is a personal and fundamental right."[278]

Unfortunately, however, even with the best efforts of U.S. officials there remains a real prospect that Privacy Shield, like Safe Harbor, will be invalidated by the Court of Justice of the European Union. The Article 29 Working Party of European data-protection authorities, for example, has expressed concern about various aspects of the final agreement.[279] The next administration should begin to consider what the United States' response will be, other than further concessions, if Privacy Shield is struck down. The administration should also begin communicating quietly to European partners that while the United States respects their legal institutions, shares their values, and has taken every reasonable measure to help European partners satisfy the Court of Justice, the United States has a "Plan B" and will not respond to another flawed, *Schrems*-like decision with more unilateral concessions.

To amplify this message, Congress should consider legislation providing that if a judicial decision restricts data transfers from Europe to the United States, the same limitations will apply to data transfers from the United States to Europe by European companies. Traditionally, American companies have been far more data-driven – and thus more dependent on such transfers – than European companies. But as traditional industrial companies increasingly become data companies as well, this imbalance is waning. European companies such as Daimler, Mercedes, Audi, Airbus, and Siemens will be increasingly reliant on data flowing back from their products in the United States to Europe. U.S. law should reflect the fact that both sides have a strong incentive to ensure continued data flows.

PRIVACY SHIELD

Earlier this year, the United States and the European Union concluded the new Privacy Shield agreement to replace Safe Harbor. It is to be hoped that Privacy Shield will survive the European judicial review process that is now underway.[273] Billions of dollars in transatlantic commerce depend on transatlantic data transfers, and operating without the safety of Safe Harbor has proved disruptive and costly for U.S. companies. Data-protection authorities in various European companies have leapt at the opportunity to pursue enforcement actions against American companies. Some are now attacking companies' ability to use a fallback tool, standard contractual clauses, to comply with European regulations.[274]

During this period, U.S. officials should seek to foster a climate conducive to ensuring that Privacy Shield passes judicial muster. This means continuing to make the case, as government officials such as the General Counsel of the Office of the Director of National Intelligence and private actors including Peter Swire and Sidley Austin have done, that U.S. and European privacy protections are, at a minimum, "essentially equivalent," as EU law requires.[275] The diplomatic initiatives outlined here would help raise

CROSS-BORDER DATA REQUESTS

A final key issue is how law-enforcement agencies access data stored outside of their home country when needed for criminal investigations. There are two sides to this issue: how foreign governments access data held in the United States, and how the U.S. government accesses data stored abroad.

The question of foreign-government access to data stored in the U.S. has been percolating for several years as foreign governments have grown progressively more dissatisfied with the status quo. There are several reasons for this frustration. First, because American companies are so predominant in digital communications and social networking, they hold a huge amount of data about foreign nationals – much of which is stored in the United States. Second, U.S. law prohibits service providers from disclosing the contents of their customers' communications directly to a foreign government, even if served with valid legal process from that government.[280] (Providers are allowed to respond to foreign-government requests for stored metadata, although they are not obligated to do so.) Rather, foreign governments are told that they must make a diplomatic request for this information, employing what is known as the Mutual Legal Assistance (MLA) process. Unfortunately, that process is notoriously slow and bureaucratic.[281] The President's Review Group reported that MLA requests "appear to average approximately 10 months to fulfill, with some requests taking considerably longer."[282]

Foreign governments are naturally dissatisfied with a status quo that frustrates their time-sensitive investigations, particularly when they are investigating their own residents in connection with local crime and the only U.S. link to the data is that it happens to be stored here. As the President's Review Group noted, lengthy Mutual Legal Assistance "delays provide a rationale for new laws that require e-mail and other records to be held in the other country," "contributing to the harmful trend of [data] localization laws."[283] Alternatively, foreign governments can simply insist that U.S. companies comply with their laws even if those laws conflict directly with the companies' obligations in the United States. This leaves companies in an untenable bind. For example, when Microsoft "refused to violate U.S. law by complying with unilateral and extraterritorial Brazilian orders, government authorities in Brazil have levied fines against [Microsoft's] local subsidiary and in one case even arrested and criminally charged a local employee" of the company.[284] These delays also give foreign governments an incentive to go outside the legal system and take data surreptitiously – for example, by hacking.

To address these problems, the Justice Department recently proposed amending the Electronic Communications Privacy Act to allow American companies to respond directly to certain requests "to disclose electronic data [to] foreign governments investigating serious crime, including terrorism."[285] The legislation would permit eligible foreign governments to take these requests directly to providers rather than using the MLA process. This proposal contains several important privacy-protective limitations. It applies only to non-U.S. persons abroad; requests must be reviewed by a judge or other independent overseer; and requests must be targeted and of limited duration (that is, it forbids bulk collection).[286] Perhaps most important, however, is that to be eligible to benefit from the legislation, a foreign government will have to (i) be certified by the Attorney General and Secretary of State as satisfying various human-rights and rule-of-law standards, (ii) enter into an executive agreement with the United States, (iii) adopt privacy-protective minimization procedures limiting how data acquired through the agreement can be used, and (iv) agree to periodic compliance reviews by the United States.[287] The agreements will also be reciprocal, meaning that U.S. law enforcement would be able to make direct requests for data held by providers based in the other country, subject to analogous privacy restrictions.

The United States and the United Kingdom have reportedly been negotiating an executive agreement allowing U.K. authorities to request data from U.S. companies in qualifying investigations.[288] The legislation recently proposed by the Department of Justice is a necessary prerequisite for that agreement and others like it.

As academics Jennifer Daskal and Andrew Woods have argued, this legislation and the system of executive agreements it would permit would be significantly more privacy-protective than the status quo, particularly over the long term.[289] If foreign governments continue to be denied data that they reasonably seek for legitimate law-enforcement investigations, the inexorable result will be widespread data-localization laws and stepped-up efforts to surreptitiously access data outside of legal channels. That is, foreign governments will gain direct access to this data without any of the privacy commitments required by the draft legislation – and in a manner that is destructive for an open and free internet and for American technology companies with cross-border business models (virtually all of them).

If the Justice Department's proposal does not pass during the current Congress, the next administration should seek, and Congress should enact, similar

legislation authorizing executive agreements on cross-border data requests. Once the enabling legislation is enacted, the executive branch should move quickly to conclude executive agreements with countries with similar human-rights and rule-of-law standards.

Even with those agreements in place, however, many requests will still have to go through the traditional Mutual Legal Assistance process – and the number of MLA requests from foreign governments has been steadily rising in recent years. Accordingly, legislation creating an alternative to the Mutual Legal Assistance system should be accompanied by parallel efforts to streamline the existing system. These could include increased funding for the MLA process, an online portal and docket for MLA requests, and annual reports on the volume of MLA requests and how long they take to process.[290]

The other key issue is U.S. law enforcement's ability to access data stored outside the United States. In a widely followed case involving customer emails Microsoft had stored in Ireland, the U.S. Court of Appeals for the Second Circuit held that the government cannot force U.S.-based companies to produce customer communications stored outside the United States – even if they can access the data from the United States and the request is supported by probable cause, the standard for a search warrant under the Fourth Amendment.[291] The effect is that the U.S. government now has to use the cumbersome MLA process to obtain customer data stored overseas. In some cases, law enforcement may not be able to access the data at all – either because the relevant country does not have a functioning MLA system, or because that country does not have jurisdiction over the person or entity that can actually access the data.[292]

The Justice Department is seeking review of the *Microsoft* decision but has already announced that it intends to seek legislation addressing the decision's consequences. The parallel timing of the two issues – foreign governments' access to data held in the United States, and the U.S. government's access to data held abroad – provides an opportunity for a broader rationalization of the legal regime governing cross-border access to data. Among countries with comparable rule-of-law standards, law-enforcement access to data should turn on the location and nationality of the subject of the investigation rather than where the data happens to be stored. That principle would align access to data with real-world law-enforcement responsibilities.[293] And it would avoid creating incentives for individuals, companies, and governments to redirect data flows in ways that harm performance, functionality, and the integrity of stored data.

In practice, this could mean combining the Justice Department's proposed cross-border-data-sharing legislation with a measure giving U.S. law-enforcement agencies qualified authority to obtain warrants for data stored abroad. And because both of these measures would amend the Electronic Communications Privacy Act, they could be packaged with long-delayed legislation requiring a warrant to access the contents of Americans' stored communications and imposing reasonable limits on nondisclosure orders, which prevent companies from notifying their customers that the government is seeking their data.[294] That package should be able to pass even today's polarized Congress and would yield benefits for international comity, the U.S. technology sector, and individual privacy.

The parallel timing of the two issues – foreign governments' access to data held in the United States, and the U.S. government's access to data held abroad – provides an opportunity for a broader rationalization of the legal regime governing cross-border access to data.

Conclusion

The reform agenda outlined in this report would strengthen privacy and civil liberties, improve oversight, and enhance transparency and democratic accountability. At the same time, the authors have consciously dubbed this a *pragmatic* agenda for surveillance policy. With the United States and its allies facing a grave terrorist threat and many other pressing international challenges, it is not realistic or responsible to eliminate lawful intelligence tools that are critical to U.S. national security.

On the international front, this agenda leads with good faith efforts to find mutual agreement on controversial surveillance-policy issues. This should help rebuild diplomatic capital damaged by the Snowden leaks and protect the U.S. technology industry's ability to do business abroad. Yet this approach also recognizes the need to firmly defend U.S. interests if other powers reject these overtures or prefer to leverage surveillance disputes to serve their own interests.

The next president will take office at a time of serious terrorist threat *and* substantial public and international skepticism about U.S. surveillance practices. An approach to surveillance policy that does not adequately account for both of these factors would, at a minimum, require a heavy expenditure of the new president's scarce political capital. By contrast, a principal virtue of our approach is that instead of expending political capital, it would expand it by helping the new president establish trust and credibility with the American people, international partners, and the U.S. technology industry. And it would do so without endangering important national security capabilities.

There is a one final reason why the next president would be wise to proactively undertake a pragmatic surveillance-reform agenda like that proposed here. The Snowden disclosures were the most significant national security leaks of the digital age, but they were neither the first nor the last of their kind. The recent "Shadow Brokers" leak is yet more evidence that nothing – not even the most highly classified program – is truly secret anymore.[395] If the new administration is hit with a wave of unexpected revelations, having launched a pragmatic but forward-leaning push for surveillance reform will to some extent help protect the president from any backlash. For the good of the country – and to protect itself – the new administration should act swiftly to demonstrate its commitment to pragmatic surveillance reform.

The next president will take office at a time of serious terrorist threat and substantial public and international skepticism about U.S. surveillance practices.

Endnotes

1. Bruce Schneier, "Cisco Shipping Equipment to Fake Addresses to Foil NSA Interception," Schneier on Security blog on Schneier.com, March 20, 2015, https://www.schneier.com/blog/archives/2015/03/cisco_shipping_.html.

2. President Barack Obama, "Remarks by the President on Review of Signals Intelligence" (Department of Justice, Washington, Jan. 17, 2014), https://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.

3. Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies (December 12, 2013), 75, https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.*

4. Ibid., 31–32. Internal NSA audits publicized in 2013 uncovered "a couple" instances "in the past decade" in which officers had misused agency systems to surveil former love interests – a practice colloquially known as "LOVINT." Siobhan Gorman, "NSA Officers Spy on Love Interests," *The Wall Street Journal*, August 23, 2013, http://blogs.wsj.com/washwire/2013/08/23/nsa-officers-sometimes-spy-on-love-interests/?cb=logged0.17765718392901975. Each of the miscreants "was punished either with an administrative action or termination." Ibid.

5. Yochai Benkler, "We cannot trust our government, so we must trust the technology," *The Guardian*, February 22, 2016, https://www.theguardian.com/us-news/2016/feb/22/snowden-government-trust-encryption-apple-fbi.

6. Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies*, 6.

7. See, for example, Dena Levitz, "It's harder to build a new 'Silicon Valley' than cities think," *The Washington Post*, August 12, 2015, https://www.washingtonpost.com/posteverything/wp/2015/08/12/every-city-wants-to-create-its-own-silicon-valley-this-is-bad-for-innovation/; Carles .Buzz [sic], "We All Live in Silicon Somewhere," Motherboard.Vice.com, March 4, 2016, http://motherboard.vice.com/read/we-all-live-in-silicon-somewhere; and Shane Dingman, "What Israel's startup scene can teach the world," *The Globe and Mail*, January 22, 2016, http://www.theglobeandmail.com/report-on-business/small-business/startups/what-israels-startup-scene-can-teach-the-world/article28329835/. ("There is immense, enormous curiosity about this phenomen[on] ... this mania of creating startups.")

8. See, for example, Ben FitzGerald et al., "Open Source Software and the Department of Defense" (Center for a New American Security, August 2016), https://www.cnas.org/publications/reports/open-source-software-and-the-department-of-defense.

9. Eric Jhonsa, "Amazon, Microsoft and Google Are Breaking Away From the Pack in Cloud Infrastructure," TheStreet.com, August 6, 2016, https://www.thestreet.com/story/13667086/1/amazon-microsoft-and-google-are-breaking-away-from-the-pack-in-cloud-infrastructure.html.

10. Frank Konkel, "CIA Official: 'Cloud Has Been a Godsend,'" Nextgov.com, August 12, 2016, http://www.nextgov.com/cloud-computing/2016/08/cia-official-cloud-has-been-godsend/130716/.

11. Ibid.

12. Frank Konkel, "Amazon Launches Cloud Marketplace for Spy Agencies," Nextgov.com, April 27, 2016, http://www.nextgov.com/cloud-computing/2016/04/amazon-launches-cloud-marketplace-spy-agencies/127833/; *cf.* AWS Marketplace, https://aws.amazon.com/marketplace.

13. Ibid.

14. Christopher Stewart and Mark Maremont, "Twitter Bars Intelligence Agencies From Using Analytics Service," *The Wall Street Journal*, May 8, 2016, http://www.wsj.com/articles/twitter-bars-intelligence-agencies-from-using-analytics-service-1462751682.

15. Ibid.

16. Ibid.

17. Ryan Browne, "Top intelligence official: ISIS to attempt U.S. attacks this year," CNN.com, February 9, 2016, http://www.cnn.com/2016/02/09/politics/james-clapper-isis-syrian-refugees/; and Mark Landler, "North Korea Nuclear Threat Cited by James Clapper, Intelligence Chief," *The New York Times*, February 9, 2016, http://www.nytimes.com/2016/02/10/world/asia/north-korea-nuclear-effort-seen-as-a-top-threat-to-the-us.html.

18. See Part IV.B.

19. Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies*, 45 ("reject[ing]" the view that society must "choose between" these values).

20. See, for example, text accompanying notes 97–112.

21. James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts," *The New York Times*, December 16, 2005, http://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html.

22. Public Law 110-55, *Protect America Act of 2007*, August 5, 2007; and Public Law 110-261, *FISA Amendments Act of 2008*, July 10, 2008.

23. *ACLU v. Clapper*, No. 14-42-cv, slip op. at 54 (2d Circuit, May 7, 2015) (quoting 50 U.S.C. § 1861(b)(2)(A)).

24. Ibid.

25. Ibid., 59.

26. Ellen Nakashima, "Top spy bemoans loss of key information-gathering program," *The Washington Post*, September 9, 2015, https://www.washingtonpost.com/world/national-security/top-spy-bemoans-loss-of-key-intelligence-program/2015/09/09/a214bda4-5717-11e5-abe9-27d53f250b11_story.html.

27. Schneier, "Cisco Shipping Equipment to Fake Addresses" and text accompanying endnote 52.

28. Barton Gellman and Ashkan Soltani, "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say," *The Washington Post*, October 30, 2013, https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

29. See, for example, Brad Smith, General Counsel, Microsoft, "Protecting customer data from government snooping," December 4, 2013, http://blogs.microsoft.com/blog/2013/12/04/protecting-customer-data-from-government-snooping/; and Robert Weber, General Counsel, IBM, "A Letter to Our Clients About Government Access to Data," March 14, 2014, http://asmarterplanet.com/blog/2014/03/open-letter-data.html.

30. Google, "Transparency Report: Legal Process," https://www.google.com/transparencyreport/userdatarequests/legalprocess/; Apple, "Privacy: Government Information Requests," https://www.apple.com/privacy/government-information-requests ("When we receive information requests, we require that it be accompanied by the appropriate legal documents such as a subpoena or search warrant."); Facebook, "Information for Law Enforcement Authorities," https://www.facebook.com/safety/groups/law/guidelines/ ("We disclose account records solely in accordance with our terms of service and applicable law, including the federal Stored Communications Act. ..."); and Microsoft, *Principles, Policies and Practices FAQ*, https://www.microsoft.com/about/csr/transparencyhub/pppfaq/. ("If a government wants customer data, it needs to follow applicable legal process -- meaning, it must serve us with a warrant or court order for content or a subpoena for subscriber information or other non-content data.")

31. *Microsoft v. United States*, No. 14-2985 (2d Circuit, July 14, 2016).

32. Apple, "Legal Process Guidelines: U.S. Law Enforcement" (September 29, 2015), 9, http://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf.

33. "German Trust in United States Plummets," Spiegel.de, November 8, 2013, http://www.spiegel.de/international/germany/nsa-spying-fallout-majority-of-germans-mistrust-united-states-a-932492.html.

34. William Jordan, "World's Most Admired 2015: Angelina Jolie and Bill Gates," YouGov.co.uk, January 30, 2015, https://yougov.co.uk/news/2015/01/30/most-admired-2015/.

35. Ben Scott, "Transatlantic Digital Dialogue: Rebuilding Trust through Cooperative Reform" (The German Marshall Fund of the United States, November 5, 2015), http://www.gmfus.org/publications/transatlantic-digital-dialogue-rebuilding-trust-through-cooperative-reform.

36. See, for example, Robert Litt, "Europe's court should know the truth about US intelligence," *Financial Times*, October 5, 2015, http://www.ft.com/cms/s/0/90be63f4-6863-11e5-a57f-21b88f7d973f.html.

37. See Part IV.C.

38. Julia Fioretti and Dustin Volz, "Privacy group launches legal challenge against EU-U.S. data pact," Reuters, October 27, 2016, http://mobile.reuters.com/article/idUSKCN12Q2JK.

39. Richard Fontaine, "Bringing Liberty Online: Reenergizing the Internet Freedom Agenda in the Post-Snowden Era" (Center for a New American Security, September 2014), https://www.cnas.org/publications/reports/bringing-liberty-online-reenergizing-the-internet-freedom-agenda-in-a-post-snowden-era.

40. Ibid.; and Adam Klein, "Decryption Mandates and Global Internet Freedom: Toward a Pragmatic Approach," Aegis Paper Series No. 1608 (Hoover Institution, September 2016), https://www.scribd.com/document/325067103/Decryption-Mandates-and-Global-Internet-Freedom-Toward-a-Pragmatic-Approach#from_embed.

41. Fontaine, "Bringing Liberty Online: Reenergizing the Internet Freedom Agenda in the Post-Snowden Era," 3.

42. Ibid., 4.

43. Claire Cain Miller, "Revelations of N.S.A. Spying Cost U.S. Tech Companies," *The New York Times*, March 21, 2014, http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html; and Danielle Kehl et al., "Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom & Cybersecurity" (New America's Open Technology Institute, July 2014), https://static.newamerica.

org/attachments/534-surveillance-costs-the-nsas-impact-on-the-economy-internet-freedom-cybersecurity/Surveilance_Costs_Final.pdf.

44. Ibid., 10; and Alonso Soto and Brian Winter, "Saab wins Brazil jet deal after NSA spying sours Boeing bid," Reuters, December 18, 2003, http://www.reuters.com/article/brazil-jets-idUSL2N0JX17W20131219#DeFikOkt1LmAZOQG.97. #of 27 icy LandscaeAngela Merke'alogous electronic messagesto localize ata before it is encrypted or after it is decrypt

45. Daniel Castro and Alan McQuinn, "Beyond the USA Freedom Act: How U.S. Surveillance Still Subverts U.S. Competitiveness" (Information Technology & Innovation Foundation, June 2015), http://www2.itif.org/2015-beyond-usa-freedom-act.pdf?_ga=1.114044933.369159037.1433787396.

46. Ibid., 7.

47. Sam Schechner, "U.S. Tech Firms Dominate Cloud Services in Western Europe," *The Wall Street Journal*, August 4, 2016, http://www.wsj.com/articles/u-s-tech-firms-dominate-cloud-services-in-western-europe-1470303004.

48. U.S. Department of Commerce Economics & Statistics Administration, *New BEA Estimates of International Trade in Digitally Enabled Services* (May 24, 2016), http://www.esa.doc.gov/economic-briefings/new-bea-estimates-international-trade-digitally-enabled-services.

49. See, for example, Ginni Rometty, "Competitive Advantage in an Era of Innovation" (Lisbon Council, Brussels, December 7, 2013) (listing examples), 2-4, http://www.lisboncouncil.net/news-a-events/495-ibms-rometty-on-competitive-advantage-in-an-era-of-innovation.html.

50. See, for example, Deutsche Telekom, "Deutsche Telekom to act as Data Trustee for Microsoft Cloud in Germany," November 11, 2015, https://www.telekom.com/media/company/293260.

51. See, for example, Jeremy Kahn, "Amazon's Pitch to Europe: Your Data Is Safe From American Spies," Bloomberg Technology, January 7, 2016, https://www.bloomberg.com/news/articles/2016-01-07/amazon-s-pitch-to-europe-your-data-is-safe-from-american-spies.

52. Schneier, "Cisco Shipping Equipment to Fake Addresses."

53. Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies*.

54. Ibid., 17.

55. Ibid., 36.

56. Ibid., 21.

57. Warren Strobel, "Obama prepares to boost U.S. military's cyber role: sources," Reuters, August 7, 2016, http://www.reuters.com/article/us-usa-cyber-idUSKCN10G254.

58. Available at http://fas.org/irp/offdocs/ppd/ppd-28.pdf.

59. PPD-28 § 1(a).

60. PPD-28 § 1(c).

61. PPD-28 § 4 (emphasis added).

62. Lauren Bateman, "NSA, CIA, and FBI Implementation of PPD-28," Lawfare, February 9, 2015, https://www.lawfareblog.com/nsa-cia-and-fbi-implementation-ppd-28.

63. PPD-28 § 4.

64. PPD-28 § 2.

65. PPD-28 § 4(d); and "Designation of the Senior Coordinator for International Information Technology Diplomacy," U.S. Department of State, press release, March 5, 2014, http://www.state.gov/r/pa/prs/ps/2014/03/223001.htm.

66. PPD-28 § 3.

67. Office of the Director of National Intelligence, *Signals Intelligence Reform: 2015 Anniversary Report*, http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties#p-pd-28.

68. Public Law 114-23, *USA FREEDOM Act of 2015*, June 2, 2015.

69. Privacy and Civil Liberties Oversight Board, *Recommendations Assessment Report* (January 29, 2015), https://pclob.gov/library/Recommendations_Assessment-Report.pdf.

70. 50 U.S.C. § 1861(b)(2)(C), "Access to certain business records for foreign intelligence and international terrorism investigations" (emphasis added).

71. Ibid.; 50 U.S.C. § 1861(c)(2)(F)(iii)-(iv).

72. The act also prohibited the use of FISA's pen register/trap-and-trace provisions for bulk collection. Public Law 114-23, Sections 201, 501.

73. 50 U.S.C. § 1803(i), "Designation of judges."

74. United States Foreign Intelligence Surveillance Court, *Memorandum Opinion and Order (November 6, 2015)*, https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf.

75. 50 U.S.C. § 1872(a), "Declassification of significant decisions, orders, and opinions."

76. Public Law 114-23, Section 602, codified at 50 U.S.C. § 1873(b), "Annual reports."

77. Public Law 114-23, Section 602, codified at 50 U.S.C. § 1873(a).

78. Public Law 114-23, Section 603, codified at 50 U.S.C. § 1874, "Public reporting by persons subject to orders."

79. See, for example, *In re Motion for Declaratory Judgment to Disclose Aggregate Data Regarding FISA Orders and Directives*, No. 13-06, Motion of Facebook, Inc. (FISC, Sept. 9, 2013) , http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-06%20Motion-3.pdf. ("Despite Facebook's efforts to push for more transparency, which have included extensive discussions with government officials, the U.S. government has taken the position that Facebook is prohibited from disclosing the specific number and type of any such requests as well as even aggregate numbers of any national security requests within ranges.")

80. *Cf.* "The Global Principles on National Security and the Right to Information (Tshwane Principles)," Paragraph 10E (June 12, 2013), https://www.opensocietyfoundations.org/sites/default/files/global-principles-national-security-10232013.pdf. ("The overall legal framework concerning surveillance of all kinds, as well as the procedures to be followed for authorizing surveillance, selecting targets of surveillance, and using, sharing, storing, and destroying intercepted material, should be accessible to the public.")

81. 50 U.S.C. § 1881a, "Procedures for targeting certain persons outside the United States other than United States persons."

82. Office of the Director of National Intelligence, *Statistical Transparency Report Regarding Use of National Security Authorities - Annual Statistics for Calendar Year 2015* (May 2, 2016), https://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2015.

83. Office of the Director of National Intelligence, *Statistical Transparency Report Regarding Use of National Security Authorities - Annual Statistics for Calendar Year 2014* (April 22, 2015), https://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2014 (92,707 targets under Section 702).

84. Office of the Director of National Intelligence, *Statistical Transparency Report Regarding Use of National Security Authorities - Annual Statistics for Calendar Year 2015.*

85. National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (2004), 395.

86. Congress later revised the board's organic statute in the implementing recommendations of the 9/11 Commission Act of 2007.

87. Privacy and Civil Liberties Oversight Board, *Recommendations Assessment Report.*

88. Privacy and Civil Liberties Oversight Board, *Recommendations Assessment Report*, 15; and Rachel L. Brand, Member, Privacy and Civil Liberties Oversight Board, testimony to the Committee on the Judiciary, U.S. Senate, May 10, 2016, 7.

89. Privacy and Civil Liberties Oversight Board, *Recommendations Assessment Report*, 20.

90. Letter from Robert Litt to Justin Antonipillai, Counselor, Department of Commerce, and Ted Dean, Deputy Assistant Secretary, International Trade Administration (February 22, 2016), 7, http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-6_en.pdf.

91. Office of the Director of National Intelligence, *Principles of Intelligence Transparency for the Intelligence Community* (February 2015), http://www.dni.gov/index.php/intelligence-community/intelligence-transparency-principles.

92. At http://icontherecord.tumblr.com/.

93. See, for example, "Joint Statement on U.S.-Germany Cyber Bilateral Meeting," U.S. Department of State, press release, March 24, 2016, https://www.state.gov/r/pa/prs/ps/2016/03/255082.htm.

94. Adam Entous and Danny Yadron, "Some Senior U.S. Officials Not Comfortable With Obama's Curbs on NSA Spying on Leaders," *The Wall Street Journal*, December 30, 2015, http://www.wsj.com/articles/some-senior-u-s-officials-not-comfortable-with-obamas-curbs-on-nsa-spying-on-leaders-1451506801.

95. John Kerry, "Remarks to the Freedom Online Coalition Conference" (via teleconference, April 28, 2014), http://www.state.gov/secretary/remarks/2014/04/225290.htm; and Scott Busby, Deputy Assistant Secretary for Democracy, Human Rights, and Labor, "Remarks on Internet Freedom" (RightsCon, San Francisco, March 4, 2014), http://www.humanrights.gov/dyn/state-department-on-internet-freedom-at-rightscon.html.

96. Joby Warrick and Karen DeYoung, "Obama Reverses Bush Policies On Detention and Interrogation," *The Washington Post*, January 23, 2009, http://www.washingtonpost.com/wp-dyn/content/article/2009/01/22/AR2009012201527.html.

97. Julian Hattem, "Surprise resignation threatens to hobble privacy watchdog," *The Hill*, April 8, 2016, http://thehill.com/policy/national-security/275545-surprise-vacancy-threatens-privacy-watchdog.

98. *Riley v. California*, 134 S. Ct. 2473 (2014).

99. 18 U.S.C. § 2703, "Required disclosure of customer communications or records"; and Richard M. Thompson II and Jared P. Cole, "Stored Communications Act: Reform of the Electronic Communications Privacy Act (ECPA)," R44036 (Congressional Research Service, May 19, 2015), https://www.fas.org/sgp/crs/misc/R44036.pdf.

100. Peter J. Henning, "The Fight Over Privacy and Secrecy in Government Investigations," *The New York Times*, May 16, 2016, http://www.nytimes.com/2016/05/17/business/

dealbook/the-fight-over-privacy-and-secrecy-in-government-investigations.html ("Why the different level of protections based on the age of the communications? Thirty years ago, Congress considered any messages over 180 days old to be abandoned, and therefore subject to reduced protection. This distinction does not make much sense now. ... ").

101. *Cf.* Digital Due Process, "ECPA Reform: Why Now?," http://www.digitalddueprocess.org. ("A particular kind of information (for example, the content of private communications) should receive the same level of protection regardless of the technology, platform or business model used to create, communicate or store it" and "regardless of how old the communication is and whether it has been 'opened' or not.")

102. *United States v. Warshak*, 631 F.3d 266 (6th Circuit, 2010).

103. *Cf. Kyllo* v. United States, 533 U.S. 27 (2001) (use of remote thermal imager to gather information about interior of a home constitutes a Fourth Amendment search).

104. H.R. 699, 114th Congress.

105 Ibid., § 4.

106. Roll Call 167, 114th Congress, 2d Session, http://clerk.house.gov/evs/2016/roll167.xml.

107. *United States v. Warshak*.

108. House Committee on the Judiciary, Report Accompanying the Email Privacy Act, H.R. Rep. No. 114-528 (2016), 9. ("Soon after the [*Warshak*] decision, the Department of Justice began using warrants for email in all criminal cases. That practice became Department policy in 2013.")

109. See, for example, Center for Democracy & Technology, "Correcting the Record: The ECTR 'Fix,'" June 27, 2016, https://cdt.org/insight/correcting-the-record-the-ectr-fix/.

110. Susan Hennessey, "DOJ Responses to FAQs on Use of National Security Letters to Obtain Electronic Communication Transaction Records," Lawfare, October 28, 2016, https://www.lawfareblog.com/doj-responses-faqs-use-national-security-letters-obtain-electronic-communication-transaction-records.

111. Letter from SEC Commissioners to Sen. Charles Grassley (May 11, 2016), http://src.bna.com/eXr.

112. Julie Brill, "It's time to update the Electronic Communications Privacy Act (ECPA)," *The Hill*, May 25, 2016, http://thehill.com/blogs/congress-blog/technology/281106-its-time-to-update-the-electronic-communications-privacy-act.

113. Chase Gunter, "Lawmakers seek controls for access to geolocation data," *FCW* (March 2, 2016), https://fcw.com/articles/2016/03/02/oversight-geolocation.aspx.

114. *Cf.* Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values (May 2014)*, https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf/.

115. See, for example, *Gunter*, "Lawmakers seek controls for access to geolocation data."

116. Mark Mazzetti and Scott Shane, "A Saudi Imam, 2 Hijackers and Lingering 9/11 Mystery," *The New York Times*, June 17, 2016, http://www.nytimes.com/2016/06/18/world/middleeast/saudi-arabia-sept11-classified-28-pages.html.

117. Mark Mazzetti, "In 9/11 Document, View of a Saudi Effort to Thwart U.S. Action on Al Qaeda," *The New York Times*, July 15, 2016, http://www.nytimes.com/2016/07/16/us/28-pages-saudi-arabia-september-11.html.

118. U.S. Department of State, *Treaty on Open Skies*, http://www.state.gov/t/avc/trty/102337.htm.

119. See generally Elizabeth Goitein, "The New Era of Secret Law" (Brennan Center for Justice, 2016), https://www.brennancenter.org/sites/default/files/publications/The_New_Era_of_Secret_Law.pdf.

120. "The Global Principles on National Security and the Right to Information (Tshwane Principles)."

121. Dakota Rudesill, "Coming to Terms with Secret Law," *Harvard National Security Journal*, 7 no. 1 (2015), 241, http://harvardnsj.org/wp-content/uploads/2016/05/Rudesill-Secret-Law.pdf.

122. 50 U.S.C. § 1881a.

123. Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (July 2, 2014), https://www.pclob.gov/library/702-Report.pdf.

124. bid., 2 (emphasis added).

125. Ibid., 10 (emphasis added).

126. Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, 10.

127. Office of the Director of National Intelligence, *Statistical Transparency Report Regarding Use of National Security Authorities - Annual Statistics for Calendar Year 2015*.

128. Matthew G. Olsen, Former Director of the National Counterterrorism Center, testimony to the Committee on the Judiciary, U.S. Senate, May 10, 2016, https://www.judiciary.senate.gov/imo/media/doc/05-10-16%20Olsen%20Testimony.pdf.

129. "The National Security Agency: Missions, Authorities, Oversight and Partnerships," National Security Agency, press room statement, August 9, 2013, https://www.nsa.gov/

news-features/press-room/statements/2013-08-09-the-nsa-story.shtml.

130. See, for example, United States Foreign Intelligence Surveillance Court, *Memorandum Opinion and Order.*

131. Office of the Director of National Intelligence, *Release of 2015 Section 702 Minimization Procedures* (August 11, 2016), https://icontherecord.tumblr.com/tagged/section-702.

132. Chris Inglis and Jeff Kosseff, "In Defense of FAA Section 702," Aegis Paper Series No. 1604, (Hoover Institution, 2016), 16, http://www.hoover.org/sites/default/files/research/docs/ingliskosseff_defenseof702_final_v3_digital.pdf.

133. Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, 59.

134. See, for example, Elizabeth Goitein, "The FBI's Warrantless Surveillance Back Door Just Opened a Little Wider," JustSecurity.org, April 21, 2016, https://www.justsecurity.org/30699/fbis-warrantless-surveillance-door-opened-wider/.

135. United States Foreign Intelligence Surveillance Court, *Memorandum Opinion and Order.*

136. Brand, testimony to the Committee on the Judiciary, 9.

137. Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, 56.

138. Privacy and Civil Liberties Oversight Board, *Recommendations Assessment Report*, 23–26.

139. Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, 147.

140. Letter from House Judiciary Committee Members to DNI James Clapper (April 22, 2016), https://assets.documentcloud.org/documents/2811050/Letter-to-Director-Clapper-4-22.pdf; and letter from privacy groups to DNI James Clapper (October 29, 2015), https://www.brennancenter.org/sites/default/files/analysis/Coalition_Letter_DNI_Clapper_102915.pdf.

141. Foreign Intelligence Surveillance Court, 2011 702 Certification Op. 34 n.32 (October 3, 2011) (per Bates, J.).

142. Letter from I. Charles McCullough III, Inspector General of the Intelligence Community, to Sens. Ron Wyden and Mark Udall (June 15, 2012), https://www.wired.com/images_blogs/dangerroom/2012/06/IC-IG-Letter.pdf.

143. Brand, testimony to the Committee on the Judiciary, 10; and United States Foreign Intelligence Surveillance Court, *Memorandum Opinion and Order*, 78.

144. Ibid., 59 (FBI records "do not identify whether the query terms are U.S. person identifiers").

145. Brand, testimony to the Committee on the Judiciary, 9.

146. "ODNI General Counsel Robert Litt Speaks on Intelligence Surveillance Reform at the Brookings Institute" (February 4, 2015), https://icontherecord.tumblr.com/post/110099240063/video-odni-general-counsel-robert-litt-speaks-on.

147. Ibid., note *.

148. Jake Laperruque, "Updates to Section 702 Minimization Rules Still Leave Loopholes," Center for Democracy & Technology, February 9, 2015, https://cdt.org/blog/updates-to-section-702-minimization-rules-still-leave-loopholes/.

149. *United States v. Nosal*, Nos. 14-10037, 10275 (9th Circuit, July 5, 2016).

150. 50 U.S.C. § 1806(c), "Use of information"; and 50 U.S.C. § 1881e(a).

151. Patrick C. Toomey, "Why Aren't Criminal Defendants Getting Notice of Section 702 Surveillance — Again?," JustSecurity.org, December 11, 2015, https://www.justsecurity.org/28256/arent-criminal-defendants-notice-section-702-surveillance-again/.

152. United States Foreign Intelligence Surveillance Court, *Memorandum Opinion and Order*; and accompanying text.

153. 50 U.S.C. § 1803(i)(2).

154. Letter from Litt to Antonipillai *and accompanying text.*

155. See, for example, Hattem, "Surprise resignation threatens to hobble privacy watchdog"; and David Medine, "The Right New Agency at the Right Time," *The Hill*, June 29, 2016, http://thehill.com/blogs/congress-blog/judicial/285184-the-right-new-agency-at-the-right-time.

156. 42 U.S.C. § 2000ee(j)(1), "Privacy and Civil Liberties Oversight Board."

157. Privacy and Civil Liberties Oversight Board, "James X. Dempsey," https://www.pclob.gov/about-us/board/dempsey.html.

158. Privacy and Civil Liberties Oversight Board, "Rachel L. Brand," https://www.pclob.gov/about-us/board/brand.html; and 42 U.S.C. § 2000ee(h)(4).

159. S. 3017, Intelligence Authorization Act for Fiscal Year 2017, 114th Cong., § 602.

160. 5 U.S.C. § 552b, "Open meetings."

161. 42 U.S.C. § 2000ee(f).

162. Patricia Wald, *Senator Chuck Grassley: Questions for the Record*, 5, https://www.judiciary.senate.gov/imo/media/doc/Wald-Reappoint-Responses-to-Grassley.pdf.

163. S. 3017 § 603, "Protection of the privacy and civil liberties of United States persons" (emphasis added).

164. See, for example, PPD-28 §5(b).

165. Center for Democracy & Technology et al., "Coalition Letter Opposing Provision of Intelligence Authorization Act on PCLOB" (*June 24, 2016*), https://cdt.org/insight/coalition-letter-opposing-provision-of-intelligence-authorization-act-on-pclob/.

166. *Cf.* S. 3017, Intelligence Authorization Act for Fiscal Year 2017, § 601.

167. See, for example, Glenn Kessler, "Edward Snowden's claim that he had 'no proper channels' for protection as a whistleblower," *The Washington Post*, March 12, 2014, https://www.washingtonpost.com/news/fact-checker/wp/2014/03/12/edward-snowdens-claim-that-as-a-contractor-he-had-no-proper-channels-for-protection-as-a-whistleblower/.

168. Public Law 105-272, *Intelligence Authorization Act for Fiscal Year 1999*, October 20, 1998, Title VII; 50 U.S.C. § 3033, "Inspector general of the intelligence community"; and 50 U.S.C. §3234, "Prohibited personnel practices in the intelligence community."

169. The White House, *Presidential Policy Directive 19: Protecting Whistleblowers with Access to Classified Information* (October 10, 2012), http://fas.org/irp/offdocs/ppd/ppd-19.pdf; and Kessler, "Edward Snowden's claim that he had 'no proper channels' for protection as a whistleblower" (quoting Dan Meyer, Executive Director for Intelligence Community Whistleblowing and Source Protection; Office of the Intelligence Community Inspector General).

170. Joe Davidson, "Senate report hits 'inferior' FBI whistleblower procedures, citing 'numerous deficiencies,'" *The Washington Post*, June 2, 2016, https://www.washingtonpost.com/news/powerpost/wp/2016/06/02/senate-report-hits-inferior-fbi-whistleblower-procedures-citing-numerous-deficiencies/.

171. S. 2390, 114th Congress.

172. Senate Report 114-261, (May 25, 2016), 8, https://www.congress.gov/114/crpt/srpt261/CRPT-114srpt261.pdf.

173. 5 U.S.C. § 7211, "Employees' right to petition Congress."

174. 5 U.S.C. § 1213, "Provisions relating to disclosures of violations of law, gross mismanagement, and certain other matters."

175. Steven Titch, "Has the NSA Poisoned the Cloud?," Policy Study No. 17 (R Street Institute, January 2014), http://www.rstreet.org/wp-content/uploads/2014/01/RSTREET17.pdf.

176. Nicholas Weaver, "Band-Aids Can't Fix Bullet Holes: Silicon Valley and the NSA," Lawfare, September 30, 2015, https://www.lawfareblog.com/band-aids-cant-fix-bullet-holes-silicon-valley-and-nsa. ("The NSA committed at least three major acts: the battle over FISA orders against Yahoo, sabotaging US products in transit, and the bulk surveillance of Yahoo and Google's internal networks, that all represent not just attacks on Silicon Valley companies, but attacks on the very business models these companies operate on.")

177. Nathan Ingraham, "Google's Eric Schmidt: 'the solution to government surveillance is to encrypt everything,'" TheVerge.com, November 21, 2013, http://www.theverge.com/2013/11/21/5130472/googles-eric-schmidt-encrypt-everything-to-prevent-government-surveillance.

178. Danny Yadron, "Google's Schmidt Fires Back Over Encryption," *The Wall Street Journal*, October 8, 2014, http://www.wsj.com/articles/googles-schmidt-says-encrypted-phones-wont-thwart-police-1412812180.

179. Under *Riley v. California*, 134 S. Ct. 2473 (2014), law enforcement officers must obtain a search warrant to access data stored on an arrestee's cellphone.

180. Apple, "Privacy: Government Information Requests."

181. Cyrus R. Vance Jr., New York County District Attorney, "Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy," Written Testimony to the Committee on the Judiciary, U.S. Senate, July 8, 2015, http://www.judiciary.senate.gov/imo/media/doc/07-08-15%20Vance%20Testimony.pdf; and Manhattan District Attorney's Office, *Report on Smartphone Encryption and Public Safety* (November 2015), http://manhattanda.org/sites/default/files/11.18.15%20Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety.pdf.

182. Telegram FAQ, https://telegram.org/faq#q-what-is-telegram-what-do-i-do-here.

183. Kim Zetter, "Security Manual Reveals the OPSEC Advice ISIS Gives Recruits," *Wired* (November 19, 2015), http://www.wired.com/2015/11/isis-opsec-encryption-manuals-reveal-terrorist-group-security-protocols/.

184. See, for example, Warren Richey, "Terror on Twitter: How Islamic State uses social media to draw recruits," *The Christian Science Monitor*, June 3, 2015, http://www.csmonitor.com/USA/Justice/2015/0603/Terror-on-Twitter-How-Islamic-State-uses-social-media-to-draw-recruits-video.

185. Rukmini Callimachi et al., "How the Paris Attackers Honed Their Assault Through Trial and Error," *The New York Times*, November 30, 2015, http://www.nytimes.com/2015/12/01/world/europe/how-the-paris-attackers-honed-their-assault-through-trial-and-error.html.

186. Sebastian Rotella, "ISIS via WhatsApp: 'Blow Yourself Up, O Lion,'" ProPublica, July 11, 2016, https://www.propublica.org/article/isis-via-whatsapp-blow-yourself-up-o-lion.

187. Ibid.

188. "Paris, Berlin want access to encrypted apps to fight terror," Deutsche Welle, August 23, 2016, http://www.dw.com/en/paris-berlin-want-access-to-encrypted-apps-to-fight-terror/a-19495759.

189. Urs Gasser et al., "Don't Panic. Making Progress on the 'Going Dark' Debate" (Harvard University's Berkman Center for Internet & Society, February 2016), https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.

190. See, for example, Peter Swire, Huang Professor of Law and Ethics, Scheller College of Business, Georgia Institute of Technology, testimony to the Committee on the Judiciary, U.S. Senate, July 8, 2015, 2, https://www.judiciary.senate.gov/imo/media/doc/07-08-15%20Swire%20Testimony.pdf.

191. Vance, "Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy."

192. See, for example, Daniel J. Weitzner, "Warning Signs: A Checklist for Recognizing Flaws of Proposed 'Exceptional Access' Systems," Lawfare, May 11, 2016, https://www.lawfareblog.com/warning-signs-checklist-recognizing-flaws-proposed-exceptional-access-systems ("History shows that even keys from governments and major companies can be stolen." (citing examples)); see generally Harold Abelson et al., "Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications," MIT-CSAIL-TR-2015-026 (Massachusetts Institute of Technology's Computer Science and Artificial Intelligence Laboratory, July 6, 2015), 10, https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf.

193. Defense Secretary Ash Carter, "Remarks by Secretary Carter" (Commonwealth Club, San Francisco, March 1, 2016), http://www.defense.gov/News/Transcripts/Transcript-View/Article/683775/remarks-by-secretary-carter-at-the-commonwealth-club-san-francisco-california.

194. Mike McConnell, Michael Chertoff, and William Lynn, "Why the fear over ubiquitous data encryption is overblown," *The Washington Post*, July 28, 2015, https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4_story.html.

195. Klein, "Decryption Mandates and Global Internet Freedom: Toward a Pragmatic Approach"; Frank Bajak and Jack Gillum, "Snapping up cheap spy tools, nations 'monitoring everyone,'" The Associated Press, August 2, 2016, http://bigstory.ap.org/article/f799cfd080b04b93a34df61fc007b096/snapping-cheap-spy-tools-nations-monitoring-everyone; and Andy Greenberg, "Hacking Team Breach Shows a Global Spying Firm Run Amok," *Wired* (July 6, 2015), https://www.wired.com/2015/07/hacking-team-breach-shows-global-spying-firm-run-amok/.

196. U.S. Department of State, Bureau of Democracy, Human Rights and Labor, *Request for Statements of Interest: DRL Internet Freedom Annual Program Statement* (June 13, 2016), http://www.state.gov/j/drl/p/258418.htm.

197. See, for example, Shane Huntley and Jonathan Pevarnek, "The Most Important Gmail Update You'll Hopefully Never See," Medium.com, March 24, 2016, https://medium.com/jigsaw/the-most-important-gmail-update-you-ll-hopefully-never-see-673b8ffe539e#.avh643kb1; Tor Project, "Tor: Sponsors," https://www.torproject.org/about/sponsors.html.en; and Electronic Frontier Foundation, "HTTPS Everywhere," https://www.eff.org/https-everywhere.

198. Ron Wyden, "This Isn't about One iPhone. It's About Millions of Them.," Backchannel.com, February 19, 2016, https://backchannel.com/this-isn-t-about-one-iphone-it-s-about-millions-of-them-3958bc619ea4#.dltm7ruqi. ("[I]f the FBI can force Apple to build a key, you can be sure authoritarian regimes like China and Russia will turn around and force Apple to hand it over to them.")

199. Patrick H. O'Neill, "Russian bill requires encryption backdoors in all messenger apps," The Daily Dot, June 20, 2016, http://www.dailydot.com/layer8/encryption-backdoor-russia-fsb/; Matthew Bodner, "What Russia's New Draconian Data Laws Mean for Users," *The Moscow Times*, July 12, 2016, https://themoscowtimes.com/articles/what-russias-new-draconian-data-laws-mean-for-users-54552; and Paul Mozur and Jane Perlez, "China Quietly Targets U.S. Tech Companies in Security Reviews," *The New York Times*, May 16, 2016, http://www.nytimes.com/2016/05/17/technology/china-quietly-targets-us-tech-companies-in-security-reviews.html. ("Chinese authorities are quietly scrutinizing technology products sold in China by Apple and other big foreign companies, focusing on whether they pose potential security threats to the country.")

200. See, for example, Sally Quillian Yates, Deputy Attorney General, testimony to the Committee on the Judiciary, U.S. Senate, July 8, 2015.

201. Riana Pfefferkorn, "Here's What the Burr-Feinstein Anti-Crypto Bill Gets Wrong," JustSecurity.org, April 15, 2016, https://www.justsecurity.org/30606/burr-feinstein-crypto-bill-terrible/.

202. Susan Hennessey, "Encryption Legislation: Critics Blinded by Outrage are Blinded to the Lessons," Lawfar, April 21, 2016 (emphasis added), https://www.lawfareblog.com/encryption-legislation-critics-blinded-outrage-are-blinded-lessons.

203. McConnell, Chertoff, and Lynn, "Why the fear over ubiquitous data encryption is overblown."

204. Cyrus Farivar, "FBI paid at least $1.3M for zero-day to get into San Bernardino iPhone," ArsTechnica.com, April 21, 2016, http://arstechnica.com/tech-policy/2016/04/fbi-paid-at-least-1-3m-for-zero-day-to-get-into-san-bernardino-iphone/.

205. "Read the NSC draft options paper on strategic approaches to encryption," *The Washington Post*, http://apps.washingtonpost.com/g/documents/national/read-the-nsc-draft-options-paper-on-strategic-approaches-to-encryption/1742/.

206. See, for example, *Cecilia Kang and Eric Lichtblau*, "F.B.I. Error Locked San Bernardino Attacker's iPhone," *The New York Times*, March 1, 2016 (noting that but for FBI error, Apple would have helped FBI recover shooter's data from cloud backup).

207. See, for example, Editorial Board, "The government wants social media sites to take down terrorist propaganda. Maybe they shouldn't.," *The Washington Post*, September 16, 2016, https://www.washingtonpost.com/pb/opinions/the-government-wants-social-media-sites-to-take-down-terrorist-propaganda-maybe-they-shouldnt/2016/09/16/148d75cc-7b77-11e6-ac8e-cf8e0dd91dc7_story.html.

208. National Academies, "Committee Membership Information: Law Enforcement and Intelligence Access to Plaintext Information in an Era of Widespread Strong Encryption: Options and Tradeoffs," September 7, 2016, https://www8.nationalacademies.org/cp/CommitteeView.aspx?key=49806.

209. H.R. 4651, 114th Congress (2016), https://homeland.house.gov/wp-content/uploads/2016/03/2016.03.03_HR-4651-Commission.pdf; and *"Hillary Clinton's Initiative on Technology & Innovation," HillaryClinton.com*, https://www.hillaryclinton.com/briefing/factsheets/2016/06/28/hillary-clintons-initiative-on-technology-innovation-2/.

210. Brendan Sasso, "The Hill's Newest Encryption Fight -- Over Committee Turf," GovExec.com, March 23, 2016, http://www.govexec.com/oversight/2016/03/hills-newest-encryption-light-over-committee-turf/126895/ ("'I think the chairmen and ranking members of the two committees of jurisdiction did not feel comfortable punting on it, in their opinion, by going with the commission.'").

211. House Report 103-827, 103d Congress (1994), 16–17.

212. Computerwoche, "De Maizière plant neue Behörde für Überwachung, " June 24, 2016, http://www.computerwoche.de/a/de-maiziere-plant-neue-behoerde-fuer-ueberwachung,3312792.

213. See generally Steven Bellovin et al., "Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet," *Northwestern Journal of Technology and Intellectual Property*, 12 no. 1 (2014), http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1209&context=njtip.

214. Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies*, 15.

215. Hilary Tuttle, "How the NSA's First CRO is Integrating Risk Management Into National Security," *Risk Management (December 1, 2015)*, http://www.rmmagazine.com/2015/12/01/mission-critical-how-the-nsas-first-cro-is-integrating-risk-management-into-national-security/.

216. "NSA Director Names New Chief Risk Officer," National Security Agency, press release, September 24, 2014, https://www.nsa.gov/news-features/press-room/press-releases/2014/new-chief-risk-officer.shtml; and Tuttle, "How the NSA's First CRO is Integrating Risk Management Into National Security."

217. Privacy and Civil Liberties Oversight Board, *Recommendations Assessment Report*, 26.

218. Michael Daniel, White House Cybersecurity Coordinator, "Heartbleed: Understanding When We Disclose Cyber Vulnerabilities" (April 28, 2014), https://www.whitehouse.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities.

219. Obama, "Remarks by the President on Review of Signals Intelligence"; and Entous and Yadron, "Some Senior U.S. Officials Not Comfortable With Obama's Curbs on NSA Spying on Leaders."

220. Bruce Schneier, "The NSA's New Risk Analysis," Schneier on Security blog on Schneier.com, October 9, 2013, https://www.schneier.com/blog/archives/2013/10/the_nsas_new_ri.html.

221. *Editorial Board,"Spying on allied leaders carries big risks: Our view," USA Today, October 24, 2013*, http://www.usatoday.com/story/opinion/2013/10/24/nsa-eavesdropping-foreign-leaders-angela-merkel-editorials-debates/3183277/.

222. For example, Barton Gellman and Ashkan Soltani, "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say," *The Washington Post*, October 30, 2013, https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

223. *Cf.* Mieke Eoyang, "Beyond Privacy and Security: The Role of the Telecommunications Industry in Electronic Surveillance," Aegis Paper Series No. 1603 (Hoover Institution, April 2016), 13, http://www.hoover.org/sites/default/files/research/docs/eoyang_privacysecurity_final_v3_digital.pdf.

224. Schneier, "Cisco Shipping Equipment to Fake Addresses."

225. Ibid.

226. Dave Aitel and Matt Tait, "Everything You Know About the Vulnerability Equities Process Is Wrong," Lawfare, August 18, 2016, https://lawfareblog.com/everything-you-know-about-vulnerability-equities-process-wrong#.

227. Daniel, "Heartbleed."

228. Andy Greenberg, "The Shadow Brokers Mess is What Happens When the NSA Hoards Zero-Days," *Wired* (August 17, 2016), https://www.wired.com/2016/08/shadow-brokers-mess-happens-nsa-hoards-zero-days/.

229. Bruce Schneier, "The NSA Is Hoarding Vulnerabilities," Schneier on Security blog on Schneier.com, August 26, 2016, https://www.schneier.com/blog/archives/2016/08/the_nsa_is_hoar.html; and Omar Santos, "The Shadow Brokers EPICBANANA and EXTRABACON Exploits," Security blog on Cisco.com, August 17, 2016, https://blogs.cisco.com/security/shadow-brokers. ("There are no workarounds for this vulnerability.")

230. Susan Hennessey and Nicholas Weaver, "A Judicial Framework for Evaluating Network Investigative Techniques," Lawfare, July 28, 2016, https://www.lawfareblog.com/judicial-framework-evaluating-network-investigative-techniques; and *Joseph Cox*, "The FBI's 'Unprecedented' Hacking Campaign Targeted Over a Thousand Computers," Motherboard.Vice.com, January 5, 2016, https://motherboard.vice.com/read/the-fbis-unprecedented-hacking-campaign-targeted-over-a-thousand-computers.

231. Aitel and t Tait, "Everything You Know About the Vulnerability Equities Process."

232. Klein, "Decryption Mandates and Global Internet Freedom: Toward a Pragmatic Approach," 6.

233. Daniel, "Heartbleed: Understanding When We Disclose Cyber Vulnerabilities"; see generally Jason Healey, "The U.S. Government and Zero-Day Vulnerabilities: From Pre-Heartbleed to Shadow Brokers," *Columbia SIPA Journal of International Affairs* (November 2016), https://jia.sipa.columbia.edu/sites/default/files/attachments/Healey%20VEP.pdf.

234. Daniel, "Heartbleed: Understanding When We Disclose Cyber Vulnerabilities."

235. Ibid.; and Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies*, 37.

236. Don Reisinger, "NSA: We Disclose 91 Percent of Security Bugs We Find," *PC Magazine* (November 9, 2015), http://www.pcmag.com/article2/0,2817,2494740,00.asp.

237. Commercial and Government Information Technology and Industrial Control Product or System Vulnerabilities Equities Policy and Process (February 16, 2010), https://www.eff.org/document/vulnerabilities-equities-process-january-2016.

238. Ibid., 8, § 6.7(c).

239. Daniel, "Heartbleed: Understanding When We Disclose Cyber Vulnerabilities."

240. Susan Hennessey, "Vulnerabilities Equities Reform That Makes Everyone (and No One) Happy," Lawfare, July 8, 2016, https://www.lawfareblog.com/vulnerabilities-equities-reform-makes-everyone-and-no-one-happy.

241. Ibid.

242. Ari Schwartz and Rob Knake, "Government's Role in Vulnerability Disclosure: Creating a Permanent and Accountable Vulnerability Equities Process" (Belfer Center for Science and International Affairs, June 2016), http://belfercenter.ksg.harvard.edu/files/vulnerability-disclosure-web-final3.pdf.

243. Ibid., 13–14.

244. *Cf.* ibid., 15–16.

245. Commercial and Government Information Technology and Industrial Control Product or System Vulnerabilities Equities Policy and Process, 8–9.

246. See text accompanying notes 31, 42.

247. See Part II.

248. See text accompanying notes 34–35.

249. Scott Wilson and Ann Gearan, "Obama didn't know about surveillance of U.S.-allied world leaders until summer, officials say," *The Washington Post*, October 28, 2013, https://www.washingtonpost.com/politics/obama-didnt-know-about-surveillance-of-us-allied-world-leaders-until-summer-officials-say/2013/10/28/0cbacefa-4009-11e3-a751-f032898f2dbc_story.html (describing backlash in France and Spain).

250. Entous and Yadron, "Some Senior U.S. Officials Not Comfortable With Obama's Curbs on NSA Spying on Leaders"; and Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies*, 20.

251. "Joint Statement on U.S.-Germany Cyber Bilateral Meeting"; and accompanying text.

252. Peter Swire, "US Surveillance Law, Safe Harbor, and Reforms Since 2013" (Future of Privacy Forum, December 17, 2015), Chapter 1, https://fpf.org/wp-content/uploads/2015/12/White-Paper-Swire-US-EU-Surveillance.pdf; and Jacques Bourgeois et al., "Essentially Equivalent: A comparison of the legal orders for privacy and data protection in the European Union and United States" (Sidley Austin LLP, January 2016), http://www.sidley.com/-/media/publications/essentially-equivalent---final.pdf.

253. Bourgeois et al., "Essentially Equivalent: A comparison of the legal orders for privacy and data protection in the European Union and United States," 5. The review covered Belgium, France, Germany, Italy, Ireland, the Netherlands, Poland, and the U.K. Ibid., 35.

254. Ibid., 37.

255. Ibid., 51.

256. PPD-28, § 4.

257. Bourgeois et al., "Essentially Equivalent: A comparison of the legal orders for privacy and data protection in the European Union and United States," 6.

258. Kelly Fiveash, "Investigatory Powers Bill passes through Commons after Labour backs Tory spy law," ArsTechnica.co.uk, July 6, 2016, http://arstechnica.co.uk/tech-policy/2016/06/labour-backs-principle-of-investigatory-powers-bill/.

259. Alison Smale, "Germany Proposes Tougher Measures to Combat Terrorism," *The New York Times*, August 11, 2016, http://www.nytimes.com/2016/08/12/world/europe/germany-antiterrorism-measures.html.

260. Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies*, 20.

261. Fontaine, "Bringing Liberty Online: Reenergizing the Internet Freedom Agenda in the Post-Snowden Era," 7. ("[T]he United States should call on other governments toembrace similar principles, or to explain why they are unwilling to do so.")

262. *Cf.* PPD-28 § 4.

263. *Cf.* IC on the Record, *Intelligence Community's Implementation of Section 4 of Presidential Policy Directive / PPD-28, Signals Intelligence Activities* (2016), https://icontherecord.tumblr.com/ppd-28/2016.

264. *Cf.* PPD-28 § 4.

265. *Cf.* PPD-28 § 2.

266. *Cf.* PPD-28 § 4(d); and "Designation of the Senior Coordinator for International Information Technology Diplomacy," U.S. Department of State, press release, March 5, 2014, http://www.state.gov/r/pa/prs/ps/2014/03/223001.htm.

267. *Cf.* 50 U.S.C. § 36, Subchapter I, "Electronic Surveillance."

268. Zachary Keck, "Robert Gates: Most Countries Conduct Economic Espionage," *The Diplomat* (May 23, 2014), http://thediplomat.com/2014/05/robert-gates-most-countries-conduct-economic-espionage/.

269. Adam Rawnsley, "Espionage? Moi?," *Foreign Policy* (July 2, 2013), http://foreignpolicy.com/2013/07/02/espionage-moi/.

270. For example, German Missions in the United States, "Interior Minister de Maizière in DC for Talks on Combatting Terrorism" (May 19, 2016), http://www.germany.info/Vertretung/usa/en/__pr/P__Wash/2016/05/19-deMaiziere-DC.html.

271. Eric Schmitt, "U.S. Officials Met With Belgians on Security Concerns Before Attacks," *The New York Times*, April 4, 2016, http://www.nytimes.com/2016/04/05/world/europe/us-security-brussels-attacks.html?_r=0.

272. Ibid.

273. Fioretti and Volz, "Privacy group launches legal challenge against EU-U.S. data pact."

274. Catherine Muyl, "EU-US Data Transfers: An update on actions taken by European DPAs," Foley Hoag Security, Privacy and the Law blog on SecurityPrivacyandtheLaw.com, June 18, 2016, http://www.securityprivacyandthelaw.com/2016/06/eu-us-data-transfers%E2%80%8E-an-update-on-actions-taken-by-european-dpas/.

275. Letter from Litt to Antonipillai and Dean; Swire, "US Surveillance Law, Safe Harbor, and Reforms Since 2013"; and Bourgeois et al., "Essentially Equivalent: A comparison of the legal orders for privacy and data protection in the European Union and United States."

276. "EU-U.S. Privacy Shield: Frequently Asked Questions," European Commission, press release, February 29, 2016, http://europa.eu/rapid/press-release_MEMO-16-434_en.htm.

277. Ibid.

278. Public Law 93-579, *The Privacy Act of 1974 (As Amended)*, Section 2(a)(4).

279. Article 29 Working Party Statement on the decision of the European Commission on the EU-U.S. Privacy Shield, http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf.

280. 18 U.S.C. § 121, "Stored Wire and Electronic Communications and Transactional Records Access."

281. Jonah Force Hill, "Problematic Alternatives: MLAT Reform for the Digital Age," *Harvard Law School National Security Journal* (January 28, 2015), http://harvardnsj.org/2015/01/problematic-alternatives-mlat-reform-for-the-digital-age/. ("The MLAT system today is deeply dysfunctional. Responses to MLAT requests for information are often abysmally slow; many of the requests are denied or only partially satisfied due to confusion over the rules governing data.")

282. Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies*, 227.

283. Ibid.

284. Brad Smith, President and Chief Legal Officer, Microsoft Corporation, written testimony to the Judiciary Committee, U.S. House of Representatives, February 25, 2016, 3, https://judiciary.house.gov/wp-content/uploads/2016/02/brad-smith-testimony.pdf.

285. Letter from Assistant Attorney General Peter J. Kadzik to the Honorable Joseph R. Biden, President of the Senate (July 15, 2016), https://www.documentcloud.org/documents/2994379-2016-7-15-US-UK-Biden-With-Enclosures.html.

286. David Kris, "U.S. Government Presents Draft Legislation for Cross-Border Data Requests," Lawfare, July 16, 2016, https://www.lawfareblog.com/us-government-presents-draft-legislation-cross-border-data-requests.

287. U.S. Department of Justice section-by-section analysis of legislation, 3, https://www.documentcloud.org/documents/2994379-2016-7-15-US-UK-Biden-With-Enclosures.html.

288. Jennifer Daskal and Andrew Woods, "A New US-UK Data Sharing Treaty?," JustSecurity.org, June 23, 2015, https://www.justsecurity.org/24145/u-s-u-k-data-sharing-treaty/.

289. Jennifer Daskal and Andrew Keane Woods, "Congress Should Embrace the DOJ's Cross-Border Data Fix," Lawfare, August 1, 2016, https://www.lawfareblog.com/congress-should-embrace-dojs-cross-border-data-fix-0.

290. Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies*, 227–229; LEADS Act, S. 512, 114th Congress; U.S. Department of Justice Criminal Division, *FY 2016 Budget Request*, *20–29*, https://www.justice.gov/sites/default/files/jmd/pages/attachments/2015/02/02/10_criminal_division_crm.pdf; and Bryan Cunningham, "Measuring MLAT," *The Hill*, *June 19, 2015*, http://thehill.com/blogs/congress-blog/foreign-policy/245454-measuring-mlat.

291. *Microsoft v. United States*, No. 14-2985 (2d Cir. July 14, 2016).

292. Jennifer Daskal, "The Dangerous Implications of the Microsoft Ireland Case," JustSecurity.org, October 14, 2016, https://www.justsecurity.org/33577/dangerous-implications-microsoft-ireland-case/.

293. Andrew Keane Woods, "Reactions to the Microsoft Warrant Case," Lawfare, July 15, 2016, https://www.lawfareblog.com/reactions-microsoft-warrant-case.

294. See text accompanying notes 9–110; and Jennifer Daskal, "A New Lawsuit from Microsoft: No More Gag Orders!," JustSecurity.org, April 14, 2016, https://www.justsecurity.org/30583/challenge-microsoft-gag-orders/.

295. Greenberg, "The Shadow Brokers Mess is What Happens When the NSA Hoards Zero-Days,"; Schneier, "The NSA Is Hoarding Vulnerabilities."

About the Center for a New American Security

The mission of the Center for a New American Security (CNAS) is to develop strong, pragmatic and principled national security and defense policies. Building on the expertise and experience of its staff and advisors, CNAS engages policymakers, experts and the public with innovative, fact-based research, ideas and analysis to shape and elevate the national security debate. A key part of our mission is to inform and prepare the national security leaders of today and tomorrow.

CNAS is located in Washington, and was established in February 2007 by co-founders Kurt M. Campbell and Michèle A. Flournoy.

CNAS is a 501(c)3 tax-exempt nonprofit organization. Its research is independent and non-partisan. CNAS does not take institutional positions on policy issues. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the authors.

1152 15th Street, NW Suite 950 Washington, DC 20005

t. 202.457.9400 | f. 202.457.9401 | info@cnas.org | cnas.org

Center for a
New American
Security

Bold. Innovative. Bipartisan.