U.S. Department of Justice

Federal Bureau of Investigation
Washington, D.C. 20535

March 29, 2022

MR. JOHN R. GREENEWALD JR.
SUITE 1203
27305 WEST LIVE OAK ROAD
CASTAIC, CA 91384-4520

FOIPA Request No.: 1381538-000
DOJ Appeal No.: 2017-003992
Subject: All Emails Containing the Keyword Snowden

Dear Mr. Greenewald:

The enclosed documents were reviewed under the Freedom of Information/Privacy Acts (FOIPA), Title 5, United States Code, Section 552/552a. Below you will find check boxes under the appropriate statute headings which indicate the types of exemptions asserted to protect information which is exempt from disclosure. The appropriate exemptions are noted on the enclosed pages next to redacted information. In addition, a deleted page information sheet was inserted to indicate where pages were withheld entirely and identify which exemptions were applied. The checked exemption boxes used to withhold information are further explained in the enclosed Explanation of Exemptions.

Section 552		Section 552a
☑ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☑ (b)(3)	☑ (b)(7)(C)	☐ (k)(1)
50 U.S.C., Section 3024 (i)(1)	☑ (b)(7)(D)	☐ (k)(2)
	☑ (b)(7)(E)	☐ (k)(3)
	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☑ (b)(5)	☐ (b)(9)	☐ (k)(6)
☑ (b)(6)		☐ (k)(7)

31 page(s) were reviewed and 20 page(s) are being released.

Please see the paragraphs below for relevant information specific to your request as well as the enclosed FBI FOIPA Addendum for standard responses applicable to all requests.

☐ Document(s) were located which originated with, or contained information concerning, other Government Agency (ies) [OGA].

☐ This information has been referred to the OGA(s) for review and direct response to you.
☐ We are consulting with another agency. The FBI will correspond with you regarding this information when the consultation is completed.

Please refer to the enclosed FBI FOIPA Addendum for additional standard responses applicable to your request. **"Part 1"** of the Addendum includes standard responses that apply to all requests. **"Part 2"** includes additional standard responses that apply to all requests for records about yourself or any third party individuals. **"Part 3"** includes general information about FBI records that you may find useful. Also enclosed is our Explanation of Exemptions.

For questions regarding our determinations, visit the www.fbi.gov/foia website under “Contact Us.” The FOIPA Request Number listed above has been assigned to your request. Please use this number in all correspondence concerning your request.

If you are not satisfied with the Federal Bureau of Investigation’s determination in response to this request, you may administratively appeal by writing to the Director, Office of Information Policy (OIP), United States Department of Justice, 441 G Street, NW, 6th Floor, Washington, D.C. 20530, or you may submit an appeal through OIP's FOIA STAR portal by creating an account following the instructions on OIP’s website: https://www.justice.gov/oip/submit-and-track-request-or-appeal. Your appeal must be postmarked or electronically transmitted within ninety (90) days of the date of my response to your request. If you submit your appeal by mail, both the letter and the envelope should be clearly marked "Freedom of Information Act Appeal." Please cite the FOIPA Request Number assigned to your request so it may be easily identified.

You may seek dispute resolution services by contacting the Office of Government Information Services (OGIS). The contact information for OGIS is as follows: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, Maryland 20740-6001, e-mail at ogis@nara.gov; telephone at 202-741-5770; toll free at 1-877-684-6448; or facsimile at 202-741-5769. Alternatively, you may contact the FBI’s FOIA Public Liaison by emailing foipaquestions@fbi.gov. If you submit your dispute resolution correspondence by email, the subject heading should clearly state “Dispute Resolution Services.” Please also cite the FOIPA Request Number assigned to your request so it may be easily identified.

☑ See additional information which follows.

As a result of your administrative appeal to the Office of Information Policy (OIP), Department of Justice (DOJ), material was located responsive to your request. Enclosed is a processed copy of the documents.

Duplicate copies of the same document were not processed.

Sincerely,

Michael G. Seidel
Section Chief
Record/Information
Dissemination Section
Information Management Division

Enclosure(s)

FBI FOIPA Addendum

As referenced in our letter responding to your Freedom of Information/Privacy Acts (FOIPA) request, the FBI FOIPA Addendum provides information applicable to your request. Part 1 of the Addendum includes standard responses that apply to all requests. Part 2 includes standard responses that apply to requests for records about individuals to the extent your request seeks the listed information. Part 3 includes general information about FBI records, searches, and programs.

Part 1: The standard responses below apply to all requests:

(i) **5 U.S.C. § 552(c).** Congress excluded three categories of law enforcement and national security records from the requirements of the FOIPA [5 U.S.C. § 552(c)]. FBI responses are limited to those records subject to the requirements of the FOIPA. Additional information about the FBI and the FOIPA can be found on the www.fbi.gov/foia website.

(ii) **Intelligence Records**. To the extent your request seeks records of intelligence sources, methods, or activities, the FBI can neither confirm nor deny the existence of records pursuant to FOIA exemptions (b)(1), (b)(3), and as applicable to requests for records about individuals, PA exemption (j)(2) [5 U.S.C. §§ 552/552a (b)(1), (b)(3), and (j)(2)]. The mere acknowledgment of the existence or nonexistence of such records is itself a classified fact protected by FOIA exemption (b)(1) and/or would reveal intelligence sources, methods, or activities protected by exemption (b)(3) [50 USC § 3024(i)(1)]. This is a standard response and should not be read to indicate that any such records do or do not exist.

Part 2: The standard responses below apply to all requests for records on individuals:

(i) **Requests for Records about any Individual—Watch Lists.** The FBI can neither confirm nor deny the existence of any individual's name on a watch list pursuant to FOIA exemption (b)(7)(E) and PA exemption (j)(2) [5 U.S.C. §§ 552/552a (b)(7)(E), (j)(2)]. This is a standard response and should not be read to indicate that watch list records do or do not exist.

(ii) **Requests for Records about any Individual—Witness Security Program Records.** The FBI can neither confirm nor deny the existence of records which could identify any participant in the Witness Security Program pursuant to FOIA exemption (b)(3) and PA exemption (j)(2) [5 U.S.C. §§ 552/552a (b)(3), 18 U.S.C. 3521, and (j)(2)]. This is a standard response and should not be read to indicate that such records do or do not exist.

(iii) **Requests for Records for Incarcerated Individuals.** The FBI can neither confirm nor deny the existence of records which could reasonably be expected to endanger the life or physical safety of any incarcerated individual pursuant to FOIA exemptions (b)(7)(E), (b)(7)(F), and PA exemption (j)(2) [5 U.S.C. §§ 552/552a (b)(7)(E), (b)(7)(F), and (j)(2)]. This is a standard response and should not be read to indicate that such records do or do not exist.

Part 3: General Information:

(i) **Record Searches.** The Record/Information Dissemination Section (RIDS) searches for reasonably described records by searching systems or locations where responsive records would reasonably be found. A standard search normally consists of a search for main files in the Central Records System (CRS), an extensive system of records consisting of applicant, investigative, intelligence, personnel, administrative, and general files compiled by the FBI per its law enforcement, intelligence, and administrative functions. The CRS spans the entire FBI organization, comprising records of FBI Headquarters, FBI Field Offices, and FBI Legal Attaché Offices (Legats) worldwide; Electronic Surveillance (ELSUR) records are included in the CRS. Unless specifically requested, a standard search does not include references, administrative records of previous FOIPA requests, or civil litigation files. For additional information about our record searches, visit www.fbi.gov/services/information-management/foipa/requesting-fbi-records.

(ii) **FBI Records.** Founded in 1908, the FBI carries out a dual law enforcement and national security mission. As part of this dual mission, the FBI creates and maintains records on various subjects; however, the FBI does not maintain records on every person, subject, or entity.

(iii) **Requests for Criminal History Records or Rap Sheets.** The Criminal Justice Information Services (CJIS) Division provides Identity History Summary Checks – often referred to as a criminal history record or rap sheet. These criminal history records are not the same as material in an investigative "FBI file." An Identity History Summary Check is a listing of information taken from fingerprint cards and documents submitted to the FBI in connection with arrests, federal employment, naturalization, or military service. For a fee, individuals can request a copy of their Identity History Summary Check. Forms and directions can be accessed at www.fbi.gov/about-us/cjis/identity-history-summary-checks. Additionally, requests can be submitted electronically at www.edo.cjis.gov. For additional information, please contact CJIS directly at (304) 625-5590.

(iv) **National Name Check Program (NNCP).** The mission of NNCP is to analyze and report information in response to name check requests received from federal agencies, for the purpose of protecting the United States from foreign and domestic threats to national security. Please be advised that this is a service provided to other federal agencies. Private Citizens cannot request a name check.

EXPLANATION OF EXEMPTIONS

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552

(b)(1) (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified to such Executive order;

(b)(2) related solely to the internal personnel rules and practices of an agency;

(b)(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;

(b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;

(b)(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;

(b)(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;

(b)(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual;

(b)(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or

(b)(9) geological and geophysical information and data, including maps, concerning wells.

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552a

(d)(5) information compiled in reasonable anticipation of a civil action proceeding;

(j)(2) material reporting investigative efforts pertaining to the enforcement of criminal law including efforts to prevent, control, or reduce crime or apprehend criminals;

(k)(1) information which is currently and properly classified pursuant to an Executive order in the interest of the national defense or foreign policy, for example, information involving intelligence sources or methods;

(k)(2) investigatory material compiled for law enforcement purposes, other than criminal, which did not result in loss of a right, benefit or privilege under Federal programs, or which would identify a source who furnished information pursuant to a promise that his/her identity would be held in confidence;

(k)(3) material maintained in connection with providing protective services to the President of the United States or any other individual pursuant to the authority of Title 18, United States Code, Section 3056;

(k)(4) required by statute to be maintained and used solely as statistical records;

(k)(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment or for access to classified information, the disclosure of which would reveal the identity of the person who furnished information pursuant to a promise that his/her identity would be held in confidence;

(k)(6) testing or examination material used to determine individual qualifications for appointment or promotion in Federal Government service the release of which would compromise the testing or examination process;

(k)(7) material used to determine potential for promotion in the armed services, the disclosure of which would reveal the identity of the person who furnished the material pursuant to a promise that his/her identity would be held in confidence.

FBI/DOJ

Mccall, A. T. (OTD) (FBI)

From: Mccall, A. T. (OTD) (FBI)

Sent: Saturday, April 08, 2017 8:31 PM

To: Piehota, Christopher M. (NS) (FBI); McCabe, Andrew G. (DO) (FBI); Kortan, Michael P. (DO) (FBI); Ghattas, Carl (CTD) (FBI); Priestap, E. W. (CD) (FBI); Strzok, Peter P. (CD) (FBI); Bowdich, David L. (DO) (FBI); Page, Lisa C. (OGC) (FBI); Rybicki, James E. (DO) (FBI); Comey, James B. (DO) (FBI)

Subject: RE: Snowden Tweet?

We're following up with our partners. In the meantime, for those who haven'the seen it, below is a link to a fairly decent summary.

https://www.cyberscoop.com/shadow-brokers-linux-nsa-donald-trump-syria/

More to follow.

Todd

--

-------- Original message --------
From: "Piehota, Christopher M. (NS) (FBI)" [redacted]
Date: 04/08/2017 7:37 PM (GMT-05:00)
To: "McCabe, Andrew G. (DO) (FBI)" [redacted] "Kortan, Michael P. (DO) (FBI)" [redacted] "Ghattas, Carl (CTD) (FBI)" [redacted] "Priestap, E. W. (CD) (FBI)" [redacted] "Strzok, Peter P. (CD) (FBI)" [redacted] "Bowdich, David L. (DO) (FBI)" [redacted] "Page, Lisa C. (OGC) (FBI)" [redacted] "Rybicki, James E. (DO) (FBI)" [redacted] "Comey, James B. (DO) (FBI)" [redacted] "Mccall, A. T. (OTD) (FBI)" [redacted] b7E
Subject: RE: Snowden Tweet?

Sir - Thank you for the info below. We will review and coordinate with other partners and stakeholders to evaluate potential impacts and equities. I am currently OCONUS and I apologize for the extended response time. AD-OTD McCall will cover STB business for this matter.

AD McCall - Please have OTD coordinate with CD and OPA, as well as with applicable US Government parties, to frame and characterize the information below. We require as much unified, integrated information as can be assembled. Provide feedback at your soonest opportunity (suitable for UNET channels). Go direct with this email group to expedite group awareness in case I am outside of immediate comms. Thank you.

-

-------- Original message --------
From: "McCabe, Andrew G. (DO) (FBI)" [redacted]
Date: 4/8/17 4:49 PM (GMT-05:00) b7E
To: "Kortan, Michael P. (DO) (FBI)" [redacted] "Ghattas, Carl (CTD) (FBI)"

[redacted] "Priestap, E. W. (CD) (FBI)" [redacted] "Strzok, Peter P. (CD) (FBI)" [redacted] "Bowdich, David L. (DO) (FBI)" [redacted] "Page, Lisa C. (OGC) (FBI)" [redacted] "Rybicki, James E. (DO) (FBI)" [redacted] "Comey, James B. (DO) (FBI)" [redacted] "Piehota, Christopher M. (NS) (FBI)" [redacted]
Subject: RE: Snowden Tweet?

Chris

FYI. Please make sure you folks are tracking and reviewing for our equities.

Andrew G. McCabe
Deputy Director
Federal Bureau of Investigation
Work [redacted]

b7E

-------- Original message --------
From: "Kortan, Michael P. (DO) (FBI)" [redacted]
Date: 4/8/17 5:25 PM (GMT-05:00)
To: "McCabe, Andrew G. (DO) (FBI)" [redacted] "Ghattas, Carl (CTD) (FBI)" [redacted] "Priestap, E. W. (CD) (FBI)" [redacted] "Strzok, Peter P. (CD) (FBI)" [redacted] "Bowdich, David L. (DO) (FBI)" [redacted] "Page, Lisa C. (OGC) (FBI)" [redacted] "Rybicki, James E. (DO) (FBI)" [redacted] "Comey, James B. (DO) (FBI)" [redacted]
Subject: FW: Snowden Tweet?

b7E

All: FYI, we just were advised of through our channels. M.

From: [redacted] (DO) (FBI)
Sent: Saturday, April 8, 2017 4:24 PM
To: Kortan, Michael P. (DO) (FBI); Quinn, Richard P. (DO) (FBI); [redacted] (DO) (FBI); [redacted] (DO) (FBI); [redacted] (DO) (FBI); [redacted] (NY) (FBI)
Subject: Fwd: Snowden Tweet?

b6
b7C

Hello,

Snowden started a series of tweets saying:
"NSA just lost control of its Top Secret arsenal of digital weapons; hackers leaked it."

He then gave Web addresses where the materials apparently have been posted.

[redacted]

b6
b7C

-------- Original message --------
[redacted]
Date: 04/08/2017 4:14 PM (GMT-05:00)
To: [redacted]
Cc: [redacted]
[redacted] (DO) (FBI)" [redacted]

b6
b6
b7E

Subject: Re: Snowden Tweet?

Thanks, it's a series of Tweets, [redacted] etc., new materials. Hard to share on this mobile so easiest if you just look at his handle for full series in last few hours. Just a head's up! b3 b7E

[redacted]
[redacted] desk b6
mobile b7C

Mueller, Robert S.

From: Mueller, Robert S.
Sent: Sunday, June 23, 2013 2:22 PM
To: [redacted] b6 b7C
Cc: Joyce, Sean M.
Subject: Re: Update - Snowden

[redacted] b5 b7E

On Jun 23, 2013, at 11:16 AM, [redacted] wrote: b6 b7C b7E

Appears to be booked through to Cuba (departing Moscow tomorrow) and speculation is that Venezuela or Ecuador is final destination. Details below.

From: Welch, Michael S.
To [redacted] b6 b7C
Sent: Sun Jun 23 11:01:04 2013
Subject: Fw: Update - Snowden

FYSA

From: Paige, Tracy Ann
To: McFeely, Richard A.; Welch, Michael S.; McCauley, Brian F.; Williams, Kendrick D.; Taddeo, Leo; [redacted] b6 b7C Priestap, E. W.; Smith, Debra E.
Sent: Sun Jun 23 10:57:49 2013
Subject: Update - Snowden

Update:

[redacted] b6 b7C b7D

- Russian press reporting Snowden will spend the night in the Venezuelan Embassy and that Venezuelan diplomats met him at the airport.

- Russian press also reporting Snowden will leave Russia on Aeroflot flight 150 to Havana on Monday, 24 June 2013, departing at 2:05pm (6:05am EDT), and speculates he will travel from there to Venezuela.

- Conflicting reports also have Snowden traveling to Ecuador on 24 June 2013. Legat Bogota report US Embassy Ecuador believes Snowden will be welcome in Ecuador.

- [redacted] b7E

Action:

- SVTC schedule for noon with CD and affected Legats.
- Timeline of events is being prepared by CD as requested by the Director
- [redacted] b7E

Background:

- Legats Copenhagen, Caracas, Bogota advised of media reported onward travel of Snowden to Venezuela, Ecuador or Iceland

Tracy A. Paige
Section Chief
International Operations Division
Federal Bureau of Investigation
desk [redacted] b7E
cell [redacted]

Mueller, Robert S.

From: Mueller, Robert S.
Sent: Wednesday, July 17, 2013 2:22 PM
To: Cole, James (ODAG) (JMD)
Cc: [redacted] b6 b7C
Subject: Snowden

[redacted] b5 b7D

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1381538-000

Total Deleted Page(s) = 11
Page 51 ~ Duplicate;
Page 54 ~ b5; b6; b7C;
Page 55 ~ b5; b6; b7C;
Page 57 ~ b1; b3; b6; b7C; b7D; b7E;
Page 58 ~ b1; b3; b6; b7C; b7D; b7E;
Page 59 ~ b1; b3; b6; b7C; b7D; b7E;
Page 60 ~ b1; b3; b6; b7C; b7D; b7E;
Page 61 ~ b1; b3; b6; b7C; b7D; b7E;
Page 62 ~ b1; b3; b6; b7C; b7D; b7E;
Page 72 ~ b5; b6; b7C; b7E;
Page 73 ~ b5; b6; b7C; b7E;

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

b6
b7C

COMEY, JAMES B. (DO) (FBI)

From: COMEY, JAMES B. (DO) (FBI)
Sent: Saturday, May 31, 2014 9:47 AM
To: ROSENBERG, CHUCK P. (DO) (FBI)
Subject: RE: SNOWDEN meeting --- ~~SECRET~~

Thanks.

From: ROSENBERG, CHUCK P. (DO) (FBI)
Sent: Thursday, May 29, 2014 6:09 PM
To: COMEY, JAMES B. (DO) (FBI)
Subject: FW: SNOWDEN meeting --- ~~SECRET~~

Classification: ~~SECRET~~

~~Classified By: CRosenberg~~
~~Derived From: FBI NSIC, dated 20120629~~
Declassify On: 20391231
==========

FYI

From: COLEMAN, RANDALL C. (CD) (FBI)
Sent: Thursday, May 29, 2014 5:14 PM
To: GIULIANO, MARK F (DO) (FBI); MCCABE, ANDREW G. (NSB) (FBI); ROSENBERG, CHUCK P. (DO) (FBI)
Subject: SNOWDEN meeting --- ~~SECRET~~

Classification: ~~SECRET~~

~~Classified By:~~ [redacted]
~~Derived From: FBI NSIC, dated 20120629~~
Declassify On: 20391231
==========

b6
b7C

Results of SNOWDEN meeting today at WFO.

[redacted]

b7E

==========
Classification: ~~SECRET~~

==========

Classification: ~~SECRET~~

COMEY, JAMES B. (DO) (FBI)

From: COMEY, JAMES B. (DO) (FBI)
Sent: Saturday, October 11, 2014 4:31 PM
To: [redacted](DA) (FBI); [redacted](CD) (FBI); [redacted] (BS) (FBI); [redacted](CD) (FBI); [redacted] (CD) (FBI); [redacted](CD) (FBI); [redacted] (FBI); [redacted](SECD)(FBI); [redacted]
Cc: [redacted]CE) (FBI); [redacted](TD) (FBI) [redacted] (CD) (FBI)
Subject: Thank you

b6
b7C

Folks:

I was in Charlotte this week and recognized [redacted] for his efforts in developing the Insider Threat program. He told me that he was just one among many and urged me to remember all of you.

b6
b7C

That's the purpose of this email, to thank you for your work on an otherwise thankless effort that is critical to protecting the FBI. We don't need to look farther than Snowden to see the incalculable damage that an insider can do to an organization and a country.

Thanks again for your good work.

Jim Comey

COMEY, JAMES B. (DO) (FBI)

From: COMEY, JAMES B. (DO) (FBI)
Sent: Thursday, July 30, 2015 11:54 AM
To: [redacted] (FBI) b6 b7C
Subject: RE: (U//~~LES~~) Comments on encryption discussion --- UNCLASSIFIED//~~LES~~

Thanks [redacted] This is both stimulating and helpful. My quick thoughts are below.

I have not come across the idea of enhancing punishment for use of encryption during an offense. Thanks for that. Very interesting.

I respectfully disagree with your view that public discussion will drive the proliferation of encryption. If Edward Snowden had never been born, I might agree with you, but, when I became Director in September 2013, his disclosures were driving encryption on device and data-in-motion like crazy, especially among bad guys. We could actually watch terrorists, nation-state actors, and criminal make the change post-Snowden. We see drug gangs using iMessage to communicate, knowing we can't get it. The post-Snowden world has seen encryption move from an available option to the default. In short, I think we are following the trend, not leading it, which is why I decided to start speaking about it.

I also have a very different view of both the frequency with which we are encountering encryption and of our ability to "break encryption." I may be wrong, of course, but [redacted] b3 b7E [redacted] I hope you will touch base with colleagues at OTD and see if you get a different sense of the facts today than I have gotten. Because I care a whole lot about our credibility.

As I have said publicly many times, I don't know what the answer is, but I am skeptical of those who point to Clipper Chip and tell me it is simply too hard. Do you think the best minds in our country have really tried? What incentive has industry had to be innovative in this area? I wonder what the world would look like if Congress passed a law that simply required all providers of communications services or devices of any kind that are based in/operate in the USA to be able to comply with court orders for production of content. Companies would need to figure out on their own how to accomplish that and

would probably come up with many different approaches, none of which they would need to disclose to the government. They simply need to comply when they receive an order.

For example, I have never heard anyone say that Google is fatally flawed from a security perspective, yet they are able to comply with all court orders for content because they strongly encrypt in transit but are able to see content as it crosses their servers (that's their business model, of course). Why don't folks say that the Google model is unworkable? Am I missing something there? I recognize that the Google approach doesn't make sense to Apple, because they market themselves as the anti-Google, but is it really "too hard" to imagine Apple figuring out a way to securely visualize content when they receive a court order? (And, like you, I believe there is no such thing as a "secure" product or service; there are only relative degrees of security.)

I agree that the solution (and, as I said, there may be thousands of individual "solutions") must include some international norm component, to avoid chasing business away from the USA (although I continue to be skeptical as to what proportion of customer decisions are driven by an assessment of a provider's ability to comply with court orders). Our allies also need some sort of international norms. And, surprisingly, a number of companies are warming to the idea of international norms, both to avoid having to balkanize their data in response to new individual national laws and as a firewall against folks like the Chinese, who are unlikely to meet the norms if they involve due process and an independent judiciary.

In closing, I very much appreciate you writing to me, and I strongly agree that our talent is at the heart of our efforts. Thanks for finding us great people.

Jim Comey

From: [redacted] (FBI) b6 b7C
Sent: Tuesday, July 28, 2015 3:23 PM
To: COMEY, JAMES B. (DO) (FBI)
Subject: (U//~~LES~~) Comments on encryption discussion --- UNCLASSIFIED/~~/LES~~

Classification: UNCLASSIFIED//~~LES~~
==========

(U) Director Comey:

(U) As a [redacted] FBI agent with [redacted] b6 b7C

I have strong beliefs about encryption and technology, and many of my FBI coworkers in the technology arena share my sentiments. I have refrained from "jumping the chain of command" over the last year and provided my comments to Unit Chiefs, Section Chiefs, and various Assistant/Deputy Directors, but

some widely respected senior personnel recently encouraged me to share my thoughts and suggestions directly with you.

1. (U) Encryption is math, and developed globally, not just the United States. Foreign nationals discovered many of the encryption techniques we use (e.g. [redacted] of the leading security conference you attended last year in San Francisco), and regulation of encrypted foreign devices and applications within the U.S. will be difficult, if not impossible. b6 b7C

2. (U) Congress considered strong encryption as a weapon in the 1990s and became subject to export controls. You have started a discussion, and could now redirect the discussion towards increased sentencing guidelines for the use of encryption in conjunction with a crime, which is much more likely to gain traction with Congress. This would build on previous congressional actions, be a good first step for law enforcement, and redirect the discussion towards the Department of Justice's primary purpose of administering justice, instead of regulating technology.

3. (U) Previous governmental efforts to regulate encryption and export weakened encryption forced software developers to support weakened protocols, resulting in worldwide vulnerabilities discovered over the past year. We should allow the industry to develop suitable encryption solutions on their own, without legislation - even as some companies are now researching (some with FBI personnel), to allow the tests of time and public scrutiny for those innovations.

4. (U) The Clipper Chip should serve as a warning to us: Respected security authorities audited the Clipper Chip escrow system and discovered significant vulnerabilities. Companies such as Google and Apple are aware that the major companies involved with the Clipper chip were unable to continue as independent entities and were acquired by two (ironically) Dutch companies (Gemalto acquired SafeNet; Philips acquired VLSI, then spun it off as NXP Semiconductors).

5. (U) The U.S. government (OPM) was deficient in protecting our own employees' information, and reportedly granted contractor access to systems from the Internet, even though employee access was restricted to office access only. How can the government safely guard more information when we cannot follow basic security guidelines, or guard what we have already? This is more than a concern for private industry or the public; I have these questions myself.

6. (U//~~LES~~) The FBI has many "sensitive but unclassified" techniques that we do not discuss with the public or media; we simply do not want to make our jobs more difficult. Examples of these techniques include ou[redacted] and many more. Many of us categorize encryption as one of these techniques. b7E

    a. (U//~~LES~~) We have rarely encountered encryption in our investigations. Continued public discussion of encryption will only serve to increase the number of our encrypted cases, as well as increase our workload, backlog, and the difficulty of our cases.

    b. (U//~~LES~~) [redacted] b7E

c. (U//~~LES~~) [redacted] b6 b7C b7E

d. (U//~~LES~~) [redacted] b7E just as Edward Snowden damaged NSA credibility (and government credibility in general).

e. (U) Through the RCFL program, the FBI actively and successfully supports local agencies with digital forensics, including encryption and technology matters. We can successfully address a large number of the encryption issues currently face with legal process.

7. (U) I believe our personnel are our most valuable resource, and we should focus on recruiting and personnel development instead of legislation. As one of the senior digital forensics field agents eligible to retire in FY16, the impending shortage of qualified digital forensics agent and professional support personnel in the field alarms me. I intend to invest much of my remaining FBI career on improving this situation – if not Bureau-wide, than at least [redacted] I submitted an EC earlier this year detailing my goals [redacted] in this area:
[redacted]

(U) I am appreciative of your leadership for the FBI in these changing and difficult times. Thank you.

(U) [redacted] b6 b7C b7E
(U)
(U)
(U)
(U) [redacted] (main)
(U) [redacted] (fax)
(U) [redacted] (mobile)

==========

Classification: UNCLASSIFIED//~~LES~~

COMEY, JAMES B. (DO) (FBI)

From: COMEY, JAMES B. (DO) (FBI)
Sent: Thursday, July 30, 2015 12:01 PM
To: HESS, AMY S (DO)(FBI); RYBICKI, JAMES E (DO)(FBI)
Subject: FW: (U//~~LES~~) Comments on encryption discussion --- UNCLASSIFIED//~~LES~~

I received this email from one of our agents in the field. [redacted] b5

[redacted] Perhaps we can discuss at some point.

I have edited the text only to remove his name and particulars that would give away his identity because I want to encourage this kind of hand-raising. We learn a lot from this kind of stuff. Feel free to share with the GD team, as appropriate.

From: COMEY, JAMES B. (DO) (FBI)
Sent: Thursday, July 30, 2015 11:55 AM
To:
Subject: RE: (U//~~LES~~) Comments on encryption discussion --- UNCLASSIFIED//~~LES~~

This is both stimulating and helpful. My quick thoughts are below.

I have not come across the idea of enhancing punishment for use of encryption during an offense. Thanks for that. Very interesting.

I respectfully disagree with your view that public discussion will drive the proliferation of encryption. If Edward Snowden had never been born, I might agree with you, but, when I became Director in September 2013, his disclosures were driving encryption on device and data-in-motion like crazy, especially among bad guys. We could actually watch terrorists, nation-state actors, and criminal make the change post-Snowden. We see drug gangs using iMessage to communicate, knowing we can't get it. The post-Snowden world has seen encryption move from an available option to the default. In short, I think we are following the trend, not leading it, which is why I decided to start speaking about it.

I also have a very different view of both the frequency with which we are encountering encryption and of our ability to "break encryption." I may be wrong, of course, but [redacted] b3 b7E

[redacted] I hope you will touch base with colleagues at OTD and see if you get a different sense of the facts today than I have gotten. Because I care a whole lot about our credibility.

b3
b7E

As I have said publicly many times, I don't know what the answer is, but I am skeptical of those who point to Clipper Chip and tell me it is simply too hard. Do you think the best minds in our country have really tried? What incentive has industry had to be innovative in this area? I wonder what the world would look like if Congress passed a law that simply required all providers of communications services or devices of any kind that are based in/operate in the USA to be able to comply with court orders for production of content. Companies would need to figure out on their own how to accomplish that and would probably come up with many different approaches, none of which they would need to disclose to the government. They simply need to comply when they receive an order.

For example, I have never heard anyone say that Google is fatally flawed from a security perspective, yet they are able to comply with all court orders for content because they strongly encrypt in transit but are able to see content as it crosses their servers (that's their business model, of course). Why don't folks say that the Google model is unworkable? Am I missing something there? I recognize that the Google approach doesn't make sense to Apple, because they market themselves as the anti-Google, but is it really "too hard" to imagine Apple figuring out a way to securely visualize content when they receive a court order? (And, like you, I believe there is no such thing as a "secure" product or service; there are only relative degrees of security.)

I agree that the solution (and, as I said, there may be thousands of individual "solutions") must include some international norm component, to avoid chasing business away from the USA (although I continue to be skeptical as to what proportion of customer decisions are driven by an assessment of a provider's ability to comply with court orders). Our allies also need some sort of international norms. And, surprisingly, a number of companies are warming to the idea of international norms, both to avoid having to balkanize their data in response to new individual national laws and as a firewall against folks like the Chinese, who are unlikely to meet the norms if they involve due process and an independent judiciary.

In closing, I very much appreciate you writing to me, and I strongly agree that our talent is at the heart of our efforts. Thanks for finding us great people.

Jim Comey

From
Sent: Tuesday, July 28, 2015 3:23 PM
To: COMEY, JAMES B. (DO) (FBI)
Subject: (U//~~LES~~) Comments on encryption discussion --- UNCLASSIFIED//~~LES~~

Classification: UNCLASSIFIED//~~LES~~
==========

(U) Director Comey:

(U) As a [VETERAN AGENT WITH LOTS OF EXPERIENCE IN THIS AREA]I have strong beliefs about encryption and technology, and many of my FBI coworkers in the technology arena share my sentiments. I have refrained from "jumping the chain of command" over the last year and provided my comments to Unit Chiefs, Section Chiefs, and various Assistant/Deputy Directors, but some widely respected senior personnel recently encouraged me to share my thoughts and suggestions directly with you.

1. (U) Encryption is math, and developed globally, not just the United States. Foreign nationals discovered many of the encryption techniques we use (e.g. [redacted] of the leading security conference you attended last year in San Francisco), and regulation of encrypted foreign devices and applications within the U.S. will be difficult, if not impossible. b6 b7C

2. (U) Congress considered strong encryption as a weapon in the 1990s and became subject to export controls. You have started a discussion, and could now redirect the discussion towards increased sentencing guidelines for the use of encryption in conjunction with a crime, which is much more likely to gain traction with Congress. This would build on previous congressional actions, be a good first step for law enforcement, and redirect the discussion towards the Department of Justice's primary purpose of administering justice, instead of regulating technology.

3. (U) Previous governmental efforts to regulate encryption and export weakened encryption forced software developers to support weakened protocols, resulting in worldwide vulnerabilities discovered over the past year. We should allow the industry to develop suitable encryption solutions on their own, without legislation - even as some companies are now researching (some with FBI personnel), to allow the tests of time and public scrutiny for those innovations.

4. (U) The Clipper Chip should serve as a warning to us: Respected security authorities audited the Clipper Chip escrow system and discovered significant vulnerabilities. Companies such as Google and Apple are aware that the major companies involved with the Clipper chip were unable to continue as independent entities and were acquired by two (ironically) Dutch companies (Gemalto acquired SafeNet; Philips acquired VLSI, then spun it off as NXP Semiconductors).

5. (U) The U.S. government (OPM) was deficient in protecting our own employees' information, and reportedly granted contractor access to systems from the Internet, even though employee access was restricted to office access only. How can the government safely guard more information when we cannot follow basic security guidelines, or guard what we have already? This is more than a concern for private industry or the public; I have these questions myself.

6. (U//~~LES~~) The FBI has many "sensitive but unclassified" techniques that we do not discuss with the public or media; we simply do not want to make our jobs more difficult. Examples of these techniques include our [redacted] b7E

[redacted] and many more. Many of us categorize encryption as one of these techniques. b7E

a. (U//~~LES~~) We have rarely encountered encryption in our investigations. Continued public discussion of encryption will only serve to increase the number of our encrypted cases, as well as increase our workload, backlog, and the difficulty of our cases.

b. (U//~~LES~~) [redacted] b7E

c. (U//~~LES~~) [redacted] b6 b7C b7E

d. (U//~~LES~~) [redacted] just as Edward Snowden damaged NSA credibility (and government credibility in general). b7E

e. (U) Through the RCFL program, the FBI actively and successfully supports local agencies with digital forensics, including encryption and technology matters. We can successfully address a large number of the encryption issues currently face with legal process.

7. (U) I believe our personnel are our most valuable resource, and we should focus on recruiting and personnel development instead of legislation. As one of the senior digital forensics field agents eligible to retire in FY16, the impending shortage of qualified digital forensics agent and professional support personnel in the field alarms me. I intend to invest much of my remaining FBI career on improving this situation.

8. (U) I am appreciative of your leadership for the FBI in these changing and difficult times. Thank you.

==========

Classification: UNCLASSIFIED/~~LES~~

b6
b7C

COMEY, JAMES B. (DO) (FBI)

From: COMEY, JAMES B. (DO) (FBI)
Sent: Wednesday, August 17, 2016 11:23 AM
To: RYBICKI, JAMES E. (DO) (FBI)
Subject: Announcement --- UNCLASSIFIED

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

To all:

After long and extraordinary service in a hugely challenging role, Science & Technology Branch EAD Amy Hess, at her request, is going home to Louisville to serve as SAC. Amy has led us through more challenges than I can list, but among them are the Snowden disclosure fallout, Going Dark, issues with our historical hair comparison testimony, the explosion in gun background checks, and on and on. I speak with her every morning I am in Washington and will miss her judgment, drive, expertise, and humor. The good news is that she will bring all those things to her new role (the second time for her) as an SAC.

Amy also leaves big shoes to fill. I have asked Chris Piehota, Director of the Terrorist Screening center, to take over as EAD for STB. I have come to know Chris well over the last three years, as he has taken the TSC to a place of excellence and global impact. Chris brings the vital leadership traits to the new role, but he also speaks the language of science and technology, something he first learned in his pre-Bureau life, where he spent years working in both Air Force and NASA laboratories.

Please join me in congratulating Amy and Chris on their new roles.

Jim Comey

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

b6
b7C

HQ.DIRECTOR

From: HQ.DIRECTOR
Sent: Wednesday, August 17, 2016 4:18 PM
To: [redacted]
Subject: Leadership Announcements --- UNCLASSIFIED

b7E

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

[redacted]

To all:

After long and extraordinary service in a hugely challenging role, Science and Technology Branch EAD Amy Hess, at her request, is going home to Louisville to serve as SAC. Amy has led us through more challenges than I can list, but among them are the Snowden disclosure fallout, Going Dark, issues with our historical hair comparison testimony, the explosion in gun background checks, and on and on. I speak with her every morning I am in Washington and will miss her judgment, drive, expertise, and humor. The good news is that she will bring all those things to her new role (the second time for her) as an SAC.

Amy also leaves big shoes to fill. I have asked Chris Piehota, Director of the Terrorist Screening Center, to take over as EAD for STB. I have come to know Chris well over the last three years, as he has taken the TSC to a place of excellence and global impact. Chris brings the vital leadership traits to the new role, but he also speaks the language of science and technology, something he first learned in his pre-Bureau life, where he spent years working in both Air Force and NASA laboratories.

Please join me in congratulating Amy and Chris on their new roles.

Jim Comey

[redacted]

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