



October 12, 2018

MR. MICHAEL BEKESHA  
JUDICIAL WATCH  
SUITE 800  
425 THIRD STREET SW  
WASHINGTON, DC 20024

FOIPA Request No.: 1386628-000  
Subject: Anthony Weiner  
(Records Retrieved from Laptop)

Dear Mr. Bekesha:

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 kick sheet was inserted to indicate where pages were withheld entirely and identify which exemptions were applied. The checked exemptions boxes used to withhold information are further explained in the enclosed Explanation of Exemptions.

**Section 552**

☐ (b)(1)

☐ (b)(2)

☒ (b)(3)

Rule 6(e), Federal Rules of

Criminal Procedure

18 U.S.C., Section 3509(d)

☐ (b)(4)

☐ (b)(5)

☒ (b)(6)

☒ (b)(7)(A)

☐ (b)(7)(B)

☒ (b)(7)(C)

☒ (b)(7)(D)

☒ (b)(7)(E)

☐ (b)(7)(F)

☐ (b)(8)

☐ (b)(9)

**Section 552a**

☐ (d)(5)

☐ (j)(2)

☐ (k)(1)

☐ (k)(2)

☐ (k)(3)

☐ (k)(4)

☐ (k)(5)

☐ (k)(6)

☐ (k)(7)

133 pages were reviewed and 39 pages are being released.

Below you will also find additional informational paragraphs about your request. Where applicable, check boxes are used to provide you with more information about the processing of your request. Please read each item carefully.

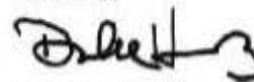
- ☐ Document(s) were located which originated with, or contained information concerning, other Government Agency [OGA].
- ☐ This information has been referred to the OGA(s) for review and direct response to you.
- ☐ We are consulting with another agency. The FBI will correspond with you regarding this information when the consultation is completed.
- ☐ In accordance with standard FBI practice and pursuant to FOIA exemption (b)(7)(E) and Privacy Act exemption (j)(2) [5 U.S.C. § 552/552a (b)(7)(E)/(j)(2)], this response neither confirms nor denies the existence of your subject's name on any watch lists.

For your information, Congress excluded three discrete categories of law enforcement and national security records from the requirements of the Freedom of Information Act (FOIA). See 5 U.S.C. § 552(c) (2006 & Supp. IV (2010)). This response is limited to those records that are subject to the requirements of the FOIA. This is a standard notification given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist. Enclosed for your information is a copy of the Explanation of Exemptions.

Please direct any further inquiries about this case to the Assistant United States Attorney representing the Government in this matter. Please use the FOIPA Request Number and/or Civil Action Number in all correspondence or inquiries concerning your request.

- ☐ The enclosed material is from the main investigative file(s), meaning the subject(s) of your request was the focus of the investigation. Our search located additional references, in files relating to other individuals, or matters, which may or may not be about your subject(s). Our experience has shown such additional references, if identified to the same subject of the main investigative file, usually contain information similar to the information processed in the main file(s). As such, we have given priority to processing only the main investigative file(s) given our significant backlog. If you would like to receive any references to the subject(s) of your request, please submit a separate request for the reference material in writing. The references will be reviewed at a later date, as time and resources permit.
- ☒ See additional information which follows.

Sincerely,



David M. Hardy  
Section Chief  
Record/Information  
Dissemination Section  
Information Management Division

Enclosure(s)

The enclosed documents represent the final release of information responsive to items 1 and 2 of your Freedom of Information Act (FOIA) request.

Additionally, please be advised that item 3 of your original request seeking "any and all records of communications, including but not limited to emails, text messages and instant chats, sent to or from FBI officials relating to Hillary Clinton's knowledge or possible knowledge of illicit activities involving former Congressman Anthony Weiner" does not comport with the requirements of 28 CFR § 16.3(b). It does not provide enough detail to enable personnel to locate records "with a reasonable amount of effort." This portion of your request is overly broad in scope and seeks information in vague and undefined terms. Therefore, no search was conducted.

For your information, sealed court records are not eligible for release under the Freedom of Information Act. Material responsive to your request has been withheld and marked "OTHER-Sealed" pursuant to appropriate order(s) issued by federal district courts.

To minimize costs to both you and the FBI, duplicate copies of the same document were not processed. This material is being provided to you at no charge; accordingly, it is unnecessary to adjudicate your request for a fee waiver.



## **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**

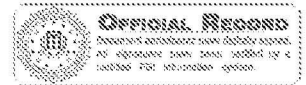
- (d)(5) information compiled in reasonable anticipation of a civil action proceeding;
- (j)(2) material reporting investigative efforts pertaining to the enforcement of criminal law including efforts to prevent, control, or reduce crime or apprehend criminals;
- (k)(1) information which is currently 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.

FEDERAL BUREAU OF INVESTIGATION  
FOI/PA  
DELETED PAGE INFORMATION SHEET  
FOI/PA# 1386628-0

Total Deleted Page(s) = 30

Page 29 ~ Duplicate;  
Page 30 ~ Duplicate;  
Page 31 ~ Duplicate;  
Page 32 ~ OTHER - SEALED;  
Page 33 ~ OTHER - SEALED;  
Page 34 ~ OTHER - SEALED;  
Page 35 ~ OTHER - SEALED;  
Page 36 ~ OTHER - SEALED;  
Page 37 ~ OTHER - SEALED;  
Page 38 ~ OTHER - SEALED;  
Page 39 ~ OTHER - SEALED;  
Page 40 ~ OTHER - SEALED;  
Page 41 ~ OTHER - SEALED;  
Page 42 ~ OTHER - SEALED;  
Page 43 ~ OTHER - SEALED;  
Page 44 ~ OTHER - SEALED;  
Page 45 ~ OTHER - SEALED;  
Page 46 ~ OTHER - SEALED;  
Page 47 ~ OTHER - SEALED;  
Page 48 ~ OTHER - SEALED;  
Page 49 ~ OTHER - SEALED;  
Page 50 ~ OTHER - SEALED;  
Page 51 ~ OTHER - SEALED;  
Page 52 ~ OTHER - SEALED;  
Page 53 ~ OTHER - SEALED;  
Page 54 ~ OTHER - SEALED;  
Page 55 ~ OTHER - SEALED;  
Page 56 ~ OTHER - SEALED;  
Page 57 ~ OTHER - SEALED;  
Page 58 ~ OTHER - SEALED;

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



UNCLASSIFIED

**FEDERAL BUREAU OF INVESTIGATION****Collected Item Log**

**Event Title:** (U) ITEMS BELONGING TO ANTHONY  
WEINER

**Date:** 09/27/2016

**Approved By:** SSA [REDACTED]

b6  
b7C

**Drafted By:** [REDACTED]

**Case ID #:** 305G-NY-2082673

(U) ANTHONY WEINER;  
PRODUCERS OF CHILD PORNOGRAPHY  
[REDACTED]

b7E

**Full Investigation Initiated:** 09/27/2016

**Enclosure(s):** Enclosed are the following items:

1. (U) 597

**Collected From:** [REDACTED]

Granite Intelligence

b6  
b7C

**Receipt Given?:** No

**Holding Office:** NEW YORK

**Details:**

On September 27, 2016, Special Agent [REDACTED] acquired three devices: an iPhone IMEI [REDACTED] an iPad IMEI [REDACTED] and a Dell Laptop bearing service tag [REDACTED]

These items were acquired from GRANITE INTELLIGENCE employee [REDACTED]  
[REDACTED] was provided with a receipt for the items seized, which resulted from a Search Warrant executed by SDNY Judge Ronald Ellis.

b6  
b7C

Item Type	Description
-----------	-------------

UNCLASSIFIED

**UNCLASSIFIED**

Title: (U) ITEMS BELONGING TO ANTHONY WEINER

Re: 305G-NY-2082673, 09/27/2016

1B Digital (U) Apple iPhone 6 [REDACTED]  
Collected On: 09/26/2016 05:00 PM EDT  
Receipt Number: QNY1  
Seizing Individual: [REDACTED]  
Collected By: [REDACTED]  
Location Area: Granite Intelligence  
Specific Location: Granite Intelligence  
Device Type: Cell Phone  
Make: Apple  
Model: iPhone  
Serial Number: [REDACTED]  
Number of Devices Collected: 1

b6  
b7C

1B Digital (U) Apple iPad 2  
Collected On: 09/26/2016 05:00 PM EDT  
Receipt Number: QNY2  
Seizing Individual: [REDACTED]  
Collected By: [REDACTED]  
Location Area: Granite Intelligence  
Specific Location: Granite Intelligence  
Device Type: Laptop/Tablet Computer  
Make: Apple  
Model: iPad2  
Serial Number: [REDACTED]  
Number of Devices Collected: 1

b6  
b7C

1B Digital (U) Dell Inspiron Laptop  
Collected On: 09/26/2016 05:00 PM EDT  
Receipt Number: QNY3  
Seizing Individual: [REDACTED]  
Collected By: [REDACTED]  
Location Area: Granite Intelligence  
Specific Location: Granite Intelligence  
Device Type: Laptop/Tablet Computer  
Make: Dell  
Model: Inspiron  
Serial Number: [REDACTED]  
Number of Devices Collected: 1

b6  
b7C

**UNCLASSIFIED**



**UNCLASSIFIED**

Title: (U) ITEMS BELONGING TO ANTHONY WEINER

Re: 305G-NY-2082673, 09/27/2016

◆◆

**UNCLASSIFIED**

UNITED STATES DEPARTMENT OF JUSTICE  
FEDERAL BUREAU OF INVESTIGATION  
Receipt for Property Received/Returned/Released/Seized

File # 3056-NY-2082673

On (date) 9/26/16

- item(s) listed below were:
- ☐ Received From
  - ☐ Returned To
  - ☐ Released To
  - ☒ Seized

(Name) GRANITE INTELLIGENCE - [redacted]

(Street Address) 23 W 73rd Street

(City) NY, NY 10027

Description of Item(s): ① white ipad w/ cracked screen

b6  
b7C

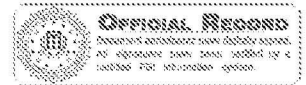
② iphon - silver

③ Dell laptop Service tag [redacted]

Received By: [redacted]

Received From: [redacted]

b6  
b7C



UNCLASSIFIED

**FEDERAL BUREAU OF INVESTIGATION****Electronic Communication****Title:** (U) Case Update- 9/29/2016**Date:** 09/29/2016**CC:** [redacted] (SSA) [redacted]  
b3  
b6  
b7C**From:** NEW YORK  
NY-C20**Contact:** [redacted] 212-384-1000**Approved By:** SSA [redacted]b6  
b7C**Drafted By:** [redacted]**Case ID #:** 305G-NY-2082673 (U) ANTHONY WEINER;  
PRODUCERS OF CHILD PORNOGRAPHY  
[redacted]

b7E

**Synopsis:** (U) This EC serves to memorialize certain legal process and evidentiary matters, as well as to provide a general update for later reference.

**Full Investigation Initiated:** 09/27/2016**Enclosure(s):** Enclosed are the following items:

1. (U) Weiner Warrant
2. (U) Wiener Warrant Receipt
3. [redacted]
4. [redacted]

OTHER -Sealed

**Details:**

On September 22, 2016, [redacted] agents served [redacted]  
[redacted] (PROTECT IDENTITY) with Grand Jury Subpoenas for [redacted]  
[redacted] to be made available in New York on [redacted]  
[redacted]

b3  
b6  
b7C  
b7D

Discussions immediately ensued between the US Attorneys Offices in the Southern District of New York (SDNY) and [redacted]

b3  
b6  
b7C  
b7D

UNCLASSIFIED

## UNCLASSIFIED

Title: (U) Case Update- 9/29/2016

Re: 305G-NY-2082673, 09/29/2016

[REDACTED], as well as the Department of Justice in Washington, DC. As a result, it was determined that SDNY would assume the lead in the prosecution of the case.

b3  
b6  
b7C  
b7D

During these discussions between the US Attorneys Offices, [REDACTED] FBI [REDACTED] willingness to make [REDACTED] available for interviews. [REDACTED] are currently en route to FBI NYO, and have been logged into this case file.

b3  
b6  
b7C  
b7D

Writer shall coordinate with FBI [REDACTED] SA [REDACTED] to arrange interviews at a convenient time and place for all parties. It is noted that NYO FBI and [REDACTED] FBI agree that both offices should have an opportunity to review evidence before conducting any interviews. Accordingly, FBI NYO shall provide [REDACTED]

b3  
b6  
b7A  
b7C  
b7D  
b7E

FBI [REDACTED] SA [REDACTED] provided writer with the name of the [REDACTED] VS [REDACTED] assigned to [REDACTED] Writer shall provide this information to NYO VS [REDACTED] who may coordinate with [REDACTED] as necessary.

b3  
b6  
b7C  
b7D

As for FBI NYO investigation, between September 22 and instant date, [REDACTED] was for devices owned/operated by ANTHONY WEINER; these devices have been seized and searches of same are ongoing. [REDACTED]

OTHER -Sealed

OTHER -Sealed

UNCLASSIFIED



**UNCLASSIFIED**

Title: (U) Case Update- 9/29/2016

Re: 305G-NY-2082673, 09/29/2016

◆◆

**UNCLASSIFIED**

ORIGINAL

## UNITED STATES DISTRICT COURT

for the  
Southern District of New YorkIn the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

See Attachment A

16 MAG 6123

## SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search  
of the following person or property located in the Southern District of New York

(identify the person or describe the property to be searched and give its location):

See Attachment A

The person or property to be searched, described above, is believed to conceal (identify the person or describe the  
property to be seized):

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or  
property.

YOU ARE COMMANDED to execute this warrant on or before

10-3-16 *pk*  
October 10, 2016

(not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10 p.m.☒ at any time in the day or night as I find reasonable cause has been  
established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property  
taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the  
place where the property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an  
inventory as required by law and promptly return this warrant and inventory to the Clerk of the Court.☒ Upon its return, this warrant and inventory should be filed under seal by the Clerk of the Court.*pk*  
USMJ Initials☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay  
of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be  
searched or seized (check the appropriate box) ☐ for \_\_\_\_\_ days (not to exceed 30).☐ until, the facts justifying, the later specific date of \_\_\_\_\_

Date and time issued:

9-26-16

2:57 pm

*Ronald L. Ellis*

Judge's signature

City and state: New York, NY

The Honorable Ronald L. Ellis

Printed name and title

[illegible]

## **Attachment A**

### **I. Devices to be Searched**

The devices to be searched (the "Subject Devices") are described as follows:

Subject Device-1 is an iPhone that was transferred from the Target Subject to Granite Intelligence LLC (the "Security Firm") on September 23, 2016, and that currently is housed at the Security Firm's office.

Subject Device-2 is an iPad that was transferred from the Target Subject to the Security Firm on September 23, 2016, and that currently is housed at the Security Firm's office.

Subject Device-3 is a laptop computer, believed to be a Dell, that was transferred from the Target Subject to the Security Firm on September 23, 2016, and that currently is housed at the Security Firm's office.

### **II. Review of ESI on the Subject Devices**

Law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the ESI and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained on the Subject Devices for the following evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1470, 2251, 2252, 2252A, and 2422 (the "Subject Offenses"):

1. Evidence concerning the identity or location of, and communications with, victims or intended victims of the Subject Offenses, including, but not limited to, photographs, contact lists, address books, instant messages, chats, text messages, emails, and photographs or videos sent to and received by minors;
2. Evidence concerning the commission of the Subject Offenses, including images of child pornography or suggestive images of the Target Subject.
3. Evidence of who used, owned, or controlled the Subject Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chats," instant messaging logs, photographs, and correspondence.
4. Evidence of the times the Subject Devices were used.
5. Evidence of the existence of other electronic devices that the Target Subject may have used to commit the Subject Offenses.



### **III. Seizure for Later Review of Electronically Stored Information**

#### **A. Seizure of Computers and Media**

This warrant authorizes the seizure of computers and electronic storage media as set forth below. In lieu of seizing any particular electronic storage media, this warrant also authorizes the copying of electronically stored information for later review. Electronic storage media which may be seized or copied include without limitation:

Computer devices, electronic media and electronic storage devices, including, but not limited to, computers, disk drives, modems, thumb drives, personal digital assistants, smart phones, digital cameras, and scanners and the data within the aforesaid objects relating to said materials, which may contain information within the scope of this warrant.

Any physical keys, encryption devices, and similar physical items that are necessary to gain access to the computer equipment, storage devices or data mentioned above, or any passwords, password files, test keys, encryption codes or other information necessary to access the above-mentioned computer equipment, storage devices or data.

#### **B. Review of Electronic Storage Media and Electronically Stored Information**

Following creation of forensic image copies as may be necessary to preserve the integrity of seized electronically stored information, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and outside technical experts under government control) are authorized to review the seized information for information and data within the scope of this warrant.

In conducting this review, law enforcement personnel may use various techniques to determine which files or other ESI contain evidence or fruits of the Subject Offenses. Such techniques may include, but shall not be limited to, surveying various file directories or folders and the individual files they contain; conducting a file-by-file review by "opening" or reading the first few "pages" of such files in order to determine their precise contents; "scanning" storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic "key-word" searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation. Depending on the circumstances, a complete review of the seized ESI may require examination of all of the seized data to evaluate its contents and determine whether the data is responsive to the warrant. Forensically trained law enforcement personnel may also, as appropriate to the circumstances, search for and attempt to recover "deleted," "hidden," or encrypted data to determine whether the data falls within the list of items to be seized as set forth in this affidavit. ESI that is responsive to the warrant will be identified and/or copied for further use in the investigation and any resultant prosecution.

UNITED STATES DISTRICT COURT

for the  
Southern District of New York

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)  
See Attachment A

16 MAG 6123

Case No. 16 Mag.

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):  
See Attachment A

located in the Southern District of New York, there is now concealed (identify the person or describe the property to be seized):

PLEASE SEE ATTACHED AFFIDAVIT AND RIDER.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. 1470	Transmitting obscene material to a minor
18 U.S.C. 2251	Sexual exploitation of children
18 U.S.C. 2252	Activities related to child pornography

The application is based on these facts:

PLEASE SEE ATTACHED AFFIDAVIT AND RIDER.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


\_\_\_\_\_  
s signature  
\_\_\_\_\_  
Special Agent  
Printed name and title

b6  
b7C

Sworn to before me and signed in my presence.

Date: 09/26/2016

City and state: New York, NY

  
Judge's signature  
The Honorable Ronald L. Ellis  
Printed name and title

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

16 MAG 6123

In the Matter of the Application of the United States Of America for a Search Warrant for (1) an iPhone, (2) an iPad, and (3) a Laptop Computer, Housed at Granite Intelligence LLC and Provided by Anthony Weiner on September 23, 2016

~~TO BE FILED UNDER SEAL~~

**Agent Affidavit in Support of  
Application for Search Warrant**

SOUTHERN DISTRICT OF NEW YORK) ss.:



being duly sworn, deposes and says:

b6  
b7c

**I. Introduction**

**A. Affiant**

1. I have been employed as a Special Agent with the Federal Bureau of Investigation ("FBI") since July 2006. I am currently assigned to the Crimes Against Children squad. I am familiar with the child pornography laws and how child pornography violations are commonly committed. I have been assigned to investigate violations of criminal law relating to the sexual exploitation of children. I have gained expertise in how to conduct such investigations through, among other things, training I have received in seminars and classes, and my daily work in relation to these types of investigations. As part of my responsibilities, I have participated in numerous investigations into the receipt, possession, distribution, and production of child pornography by electronic means and have reviewed thousands of photographs depicting children (less than eighteen years of age) being sexually exploited by adults. Through my experience in these investigations, I have become familiar with the manner in which acts of sexual exploitation of children are committed and the methods of determining whether a child is a minor. I am also a member of the Southern and Eastern Districts of New York Project Safe Childhood Task Forces.

2. I make this Affidavit in support of an application pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the electronic devices specified below (the "Subject Devices") for the items and information described in Attachment A. This affidavit is based upon my personal knowledge; my review of documents and other evidence; my conversations with other law enforcement personnel; and my training, experience and advice received concerning the use of computers in criminal activity and the forensic analysis of electronically stored information ("ESI"). 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 my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

**B. The Subject Devices**

3. The first subject device ("Subject Device-1") is particularly described as an iPhone that was transferred from Anthony Weiner (the "Target Subject") to Granite Intelligence LLC, a Manhattan private security firm, (the "Security Firm") on September 23, 2016, and that currently is housed at the Security Firm's office.

4. The second subject device ("Subject Device-2") is particularly described as an iPad that was transferred from the Target Subject to the Security Firm on September 23, 2016, and that currently is housed at the Security Firm's office.

5. The third subject device ("Subject Device-3," or, collectively with Subject Device-1 and Subject Device-2, the "Subject Devices") is particularly described as a laptop computer, believed to be a Dell, that was transferred from the Target Subject to the Security Firm on September 23, 2016, and that currently is housed at the Security Firm's office.



6. Based on my training, experience, and research, I know that the Subject Devices have capabilities that allow them to serve as wireless communications devices, digital cameras, portable media players, GPS navigation devices, and PDAs.

7. The Subject Devices presently are located in the Southern District of New York.

### **C. The Subject Offenses**

8. For the reasons detailed below, I believe that there is probable cause to believe that the Subject Devices contain evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1470 (transmitting obscene material to minor), 2251 (sexual exploitation of children), 2252 (activities related to child pornography), 2252A (activities related to child pornography), and 2422 (coercion and enticement) (the "Subject Offenses").

### **D. Terminology**

9. As used herein, the following terms have the following meaning:

a. "Child Pornography" means any visual depiction, the production of which involved the use of a minor engaged in sexually explicit conduct. *See* 18 U.S.C. §§ 2252, 2256(2), and 2256(8).

b. "Computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. *See* 18 U.S.C. § 1030(e)(1).

c. "Directory" or "folder" means a simulated electronic file folder or container used to organize files and directories in a hierarchical or tree-like structure.

d. "Electronically Stored Information" or "ESI" includes, consistent with Federal Rule of Criminal Procedure 41 and the Advisory Committee Comments to the 2009 amendments, writings, drawings, graphs, charts, photographs, sound recordings, images, and other

data or data compilations stored in any medium from which information can be obtained, including all types of computer-based information as may be developed over time. "Computer data" as used herein is synonymous with ESI.

e. "File" means a collection of related data or information stored as a unit under a specified name on storage medium. Not all ESI is stored in files.

f. "Internet" means a global network of computers and other devices that communicate with each other. It supports services such as email, the World Wide Web, file transfer, and Internet Relay Chat. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when devices communicating with each other are in the same state.

g. "Internet Service Providers" ("ISPs") are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line ("DSL") or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "email address," an email mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an ISP over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

h. “Minor” means any person under the age of eighteen years. *See* 18 U.S.C. § 2256(1).

i. “Records,” “documents,” and “materials” include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (“DVDs”), Personal Digital Assistants (“PDAs”), Multi Media Cards (“MMC’s”), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

j. “Sexually explicit conduct” means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. *See* 18 U.S.C. § 2256(2).

## **II. Probable Cause**

### **A. Probable Cause Regarding Target Subject’s Commission of the Subject Offenses**

#### Overview

10. As set forth in greater detail below, on or about September 21, a media report (the “Media Report”) was published, indicating that the Target Subject had engaged in an online relationship with a minor (the “Victim”) from in or about January 2016 through in or about July 2016, which included explicit sexual communications. *See infra* ¶¶ 11, 15. Following the

publication of that report, the FBI spoke with the Victim, who confirmed, in sum and substance, that the Victim had participated in the reported digital communications with the Target Subject, as well as additional online communications that had not been included in the Media Report. *See infra* ¶ 15. An attorney for the Target Subject has since confirmed that the Subject Devices belong to the Target Subject and have been surrendered to a security firm, from which they can be recovered pursuant to a search warrant. *See infra* ¶ 19 & n.2.

### The Investigation

11. On or about September 21, 2016, a United Kingdom-based news outlet published the Media Report, which reported that the Target Subject has engaged in an online relationship with a minor (the “Victim”) from in or about January 2016 through in or about July 2016. The Target Subject and the Victim communicated over the internet using text and video messaging applications, including Kik, Skype, Facebook, Twitter, and Confide. Based on my training and experience, I know that these messaging applications are accessed through electronic devices, including cellular telephones, tablets, and computers. The Media Report made clear that in the course of the Target Subject and the Victim’s online relationship, the Target Subject induced the Victim to engage in sexually explicit conduct over video chat. Some of the communications are set forth below. *See infra* ¶ 15.

12. Based on my conversations with other law FBI agents involved in this investigation, I have learned, among other things, the following:

- a. The Victim is under eighteen years old.
- b. On or about September 22, 2016, the Victim and the Victim’s father confirmed to FBI agents in the state in which the Victim resides that the Victim is the person identified in the Media Report (as having engaged in sexual communications with the Target

Subject), and confirmed that they possess the electronic devices that the Victim used to communicate with the Target Subject.

c. According to the Victim and the Victim's father, the electronic devices contain the communications between the Target Subject and the Victim that were published in the Media Report, as well as additional communications between the Target Subject and the Victim.

13. Based on my review of open source information, including media reports, I have learned, among other things, that the Target Subject has acknowledged to the media that he had communicated online with the Victim. For example:

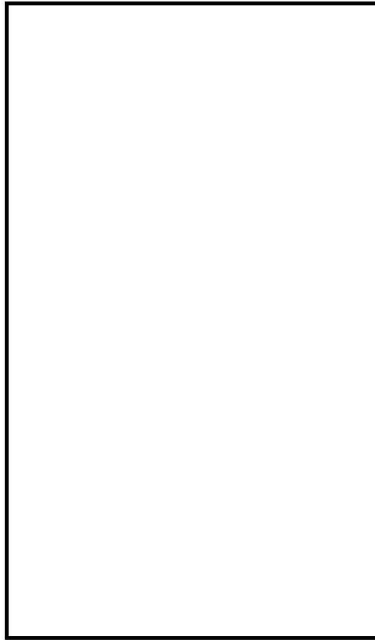
a. On or about September 21, 2016, the Target Subject provided the media with a statement that he had "demonstrated terrible judgment about the people [he] had communicated with online and the things [he had] sent."

b. On or about September 21, 2016, the Target Subject provided the media with a redacted letter that the Victim had written and the Target Subject had in his possession.

14. Based on my review of publicly available information, including messages posted on Twitter and user photographs, the Target Subject appears to have used and maintained a Twitter account with the username "@anthonyweiner" (the "Target Subject Twitter Account").

15. Based on my review of the communications between the Target Subject and the Victim that were published in the Media Report, I have learned, among other things, the following:

a. The Target Subject Twitter Account and the Victim appear to have exchanged private messages through Twitter. Based on the content of those messages the Target Subject appears to have been aware that the Victim was a high school student and therefore a minor. For example:



b3  
b6  
b7C

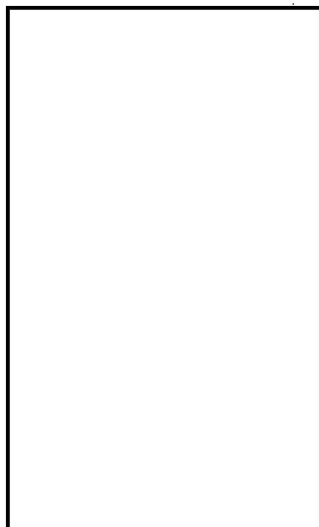
b. The Target Subject Twitter Account and the Victim discussed having additional conversations over Skype, which, based on my training and experience, I know to be an application that allows for video communication, among other things. For example:



b3  
b6  
b7C

c. The Victim exchanged private messages through an internet messaging application called Kik with a user account the Target Subject appears to have used and maintained (the "Target Subject Kik Account"). For example:

i. The Target Subject Kik Account sent the Victim a message that included a “selfie”<sup>1</sup> photograph that appears to be of the Target Subject.



b3  
b6  
b7C

ii. The Target Subject agreed that the Victim could refer to him with the nickname “Carlos Danger,” which, based on my training, experience, and review of open source materials, I know to be a nickname the Target Subject has publically acknowledged to have used in the past.

---

<sup>1</sup> A “selfie” is a photograph that a person takes of him or herself, typically with a cellular telephone or other portable electronic device.



b3  
b6  
b7C

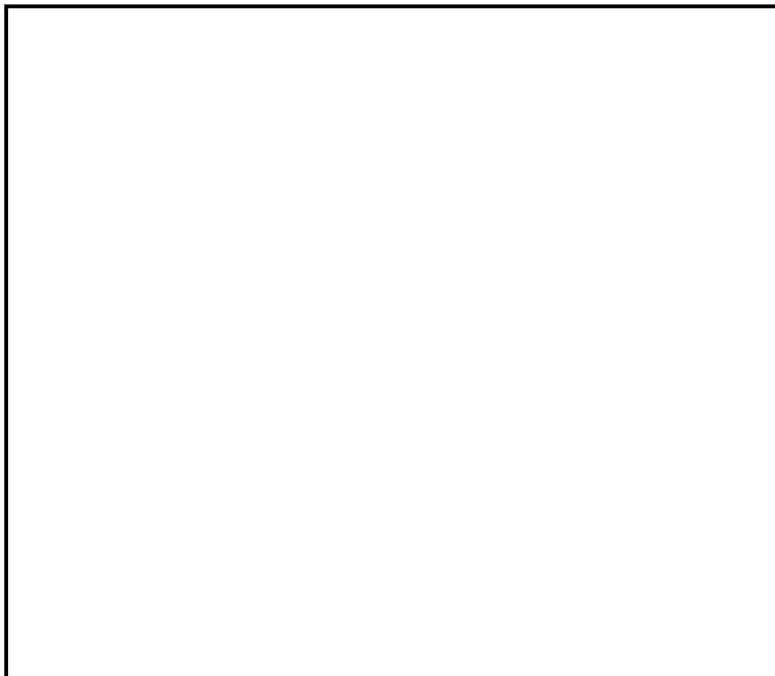
iii. The Victim referred to the Target Subject by name.



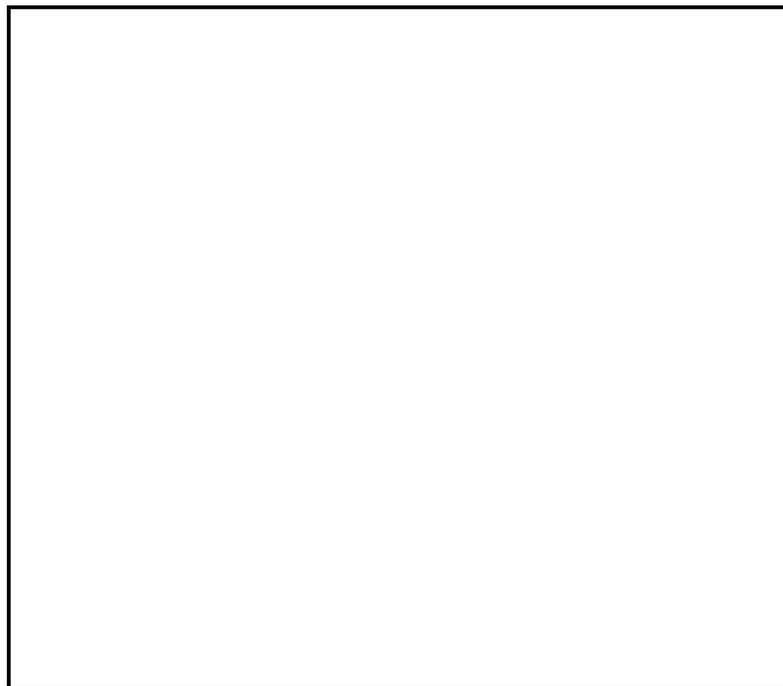
b3  
b6  
b7C



d. The Target Subject Kik Account exchanged sexually explicit messages with the Victim and exchanged “selfie” photographs. For example:



b3  
b6  
b7C



b3  
b6  
b7C

e. The Victim exchanged private messages through an online messaging application called Confide with an account the Victim has said the Target Subject used. Although

Confide permanently deletes messages after they are read, the Victim took photographs of sexually explicit messages received from the Target Subject. For example:



b3  
b6  
b7C

16. Based on my training and experience, I know that individuals who engage in sexually explicit text conversations with minors often use other means of communication, including video chats, to induce the minors to engage in sexually explicit conduct. Those individuals often use services such as Skype, *see supra* ¶ 15(b), to receive and view video of minors engaging in sexually explicit conduct.

**B. Probable Cause Justifying Search of the Subject Devices**

17. Based on the foregoing, and my training and experience, there is probable cause to believe that the Target Subject has used one or more electronic devices, including cellular telephones, tablets, and laptop computers, to commit the Subject Offenses, and that these devices will contain evidence, or are the instrumentalities, of the Subject Offenses, including evidence of the Target Subject's participation in the Subject Offenses.

18. As set forth above, at least one of the photographs that appears to have been sent from the Target Subject to the Victim appears to have been taken with a device held in the hand of the Target Subject at the time it was taken. *See supra* ¶ 15(c)(i).

19. Based on my conversation with an attorney for the Target Subject, I have learned, among other things, the following:

a. The Target Subject possessed the Subject Devices until on or about September 23, 2016, when he transferred their custody to an agent of the Security Firm for safekeeping.<sup>2</sup>

b. The Subject Devices were transported to and currently are located at the Security Firm's office, which is in the Southern District of New York.

c. The Subject Devices have been securely maintained since their transfer to the Security Firm's custody.

20. Based on my training and experience, individuals who engage in the solicitation and possession of child pornography often store records relating to their illegal activity and to persons involved with them in that activity on electronic devices such as the Subject Devices. Such records can include, for example, logs of online "chats" with victims; email correspondence; contact information of victims, including telephone numbers, email addresses, and identifiers for instant messaging and social medial accounts; and still images and videos of child pornography. Such individuals may go to great lengths to conceal or protect their collections of illicit materials from discovery, theft, and damage.

---

<sup>2</sup> The Subject Devices were transferred to the Security Firm at the direction of counsel for the Target Subject in order to avoid the need to search the Target Subject's home. Other individuals involved in this investigation have informed me that counsel for the Target Subject has agreed to cooperate with the execution of this search warrant.

21. Computer files or remnants of such files can be recovered months or even years after they have been created or saved on an electronic device such as the Subject Devices. Even when such files have been deleted, they can often be recovered, depending on how the hard drive has subsequently been used, months or years later with forensics tools. Thus, the ability to retrieve from information from the Subject Devices depends less on when the information was first created or saved than on a particular user's device configuration, storage capacity, and computer habits.

22. In addition to probable cause to believe that the Subject Devices contain evidence of the Subject Offenses, there is also probable cause to believe that the Subject Devices also constitute contraband subject to seizure, in that the devices contain contraband child pornography, and are instrumentalities of the Subject Offenses.

23. Based on the foregoing, I respectfully submit there is probable cause to believe that the Target Subject has engaged in the Subject Offenses, and that evidence of this criminal activity is likely to be found on the Subject Devices.

### **III. Procedures for Searching ESI**

#### **A. Review of ESI**

24. Law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the ESI and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will review the ESI contained on the Subject Devices for information responsive to the warrant.

25. In conducting this review, law enforcement may use various techniques to determine which files or other ESI contain evidence or fruits of the Subject Offenses. Such techniques may include, for example:

- surveying directories or folders and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- conducting a file-by-file review by “opening” or reading the first few “pages” of such files in order to determine their precise contents (analogous to performing a cursory examination of each document in a file cabinet to determine its relevance);
- “scanning” storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and
- performing electronic keyword searches through all electronic storage areas to determine the existence and location of search terms related to the subject matter of the investigation. (Keyword searches alone are typically inadequate to detect all information subject to seizure. For one thing, keyword searches work only for text data, yet many types of files, such as images and videos, do not store data as searchable text. Moreover, even as to text data, there may be information properly subject to seizure but that is not captured by a keyword search because the information does not contain the keywords being searched.)

26. Law enforcement personnel will make reasonable efforts to restrict their search to data falling within the categories of evidence specified in the warrant. Depending on the circumstances, however, law enforcement may need to conduct a complete review of all the ESI from the Subject Devices to locate all data responsive to the warrant.

#### **B. Return of the Subject Devices**

27. If the Government determines that the Subject Devices are no longer necessary to retrieve and preserve the data on the device, and that the Subject Devices are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(c), the Government will return the Subject Devices, upon request. Computer data that is encrypted or unreadable will not be returned unless law enforcement personnel have determined that the data is not (i) an instrumentality of the offense, (ii) a fruit of the criminal activity, (iii) contraband, (iv) otherwise unlawfully possessed, or (v) evidence of the Subject Offenses.

#### IV. Conclusion and Ancillary Provisions

28. Based on the foregoing, I respectfully request the court to issue a warrant to seize the items and information specified in Attachment A to this affidavit and to the Search and Seizure Warrant.

29. In light of the confidential nature of the continuing investigation, the full scope of which is not known to the Target Subject or the public, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise.



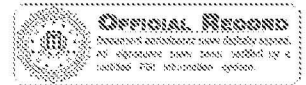
Special Agent  
Federal Bureau of Investigation

b6  
b7C

Sworn to before me on  
the 26th day of September, 2016

A handwritten signature in black ink, reading "Ronald L. Ellis".

HON. RONALD L. ELLIS  
UNITED STATES MAGISTRATE JUDGE



UNCLASSIFIED

**FEDERAL BUREAU OF INVESTIGATION****Import Form**

Form Type: EMAIL

Date: 10/05/2016

Title: (U) FYI

Approved By: SSA [REDACTED]

b6

b7C

Drafted By: [REDACTED]

Case ID #: 305G-NY-2082673

(U) ANTHONY WEINER;

PRODUCERS OF CHILD PORNOGRAPHY  
[REDACTED]

b7E

Synopsis: (U) FYI

◆◆

UNCLASSIFIED

**To:** [REDACTED] (NY) (FBI)  
**Subject:** FYI --- UNCLASSIFIED

b6  
b7C

**SentinelCaseId:** 305G-NY-2082673  
**SentToSentinel:** 10/3/2016 6:55:59 PM

Classification: UNCLASSIFIED

=====  
Sent for Approval for RECORD//Sentinel Case 305G-NY-2082673

Hey [REDACTED] b6  
b7C

Just putting this on the record because of the optics of this case.

During the course of my review of a computer seized from Anthony Weiner, a seizure and search of which was authorized by an SDNY Search Warrant, I encountered approximately/at least 340,000 emails stored on the computer. The large number of emails appears to be a result of a mail client program installed on that computer (such as Outlook) that pulled emails from servers belonging to both Anthony Weiner and Huma Abedin.

A significant number of these 340,000 emails appeared to be between Huma Abedin and Hillary Clinton (the latter who appears to have used a number of different email addresses). This is based simply a review of the header information. I did not review content of these emails, as the warrant only authorized me to view items that would give me probable cause to believe that CP evidence may reside therein.

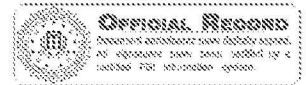
SDNY is comfortable with me continuing my review as I have, which is to NOT read any emails to/from Anthony Weiner to which his wife, or a possible attorney is a party. Even if there is a third party on those emails, I will not review their content out of an abundance of caution. Obviously, I will not review any emails to which Anthony Weiner is not a party (such as emails between Ms. Abedin and Mrs. Clinton).

I just wanted to formally bring this to your attention due to the pending election, the ongoing Congressional investigation into the FBI's own investigation into Ms. Clinton's email activities, etc.

[REDACTED] b6  
b7C

=====  
Classification: UNCLASSIFIED



UNCLASSIFIED//~~FOUO~~**FEDERAL BUREAU OF INVESTIGATION****Electronic Communication**

b7E

**Title:** (U) CEAU [redacted] Case Request for Assistance**Date:** 10/06/2016**From:** OPERATIONAL TECHNOLOGY

DP-CEAU

**Contact:** [redacted] 212-384-1000**Approved By:** SSA [redacted]b6  
b7C**Drafted By:** [redacted]**Case ID #:** 305G-NY-2082673(U) ANTHONY WEINER;  
PRODUCERS OF CHILD PORNOGRAPHY[redacted]  
(U//~~FOUO~~) [redacted]b7A  
b7E**Synopsis:** (U) CEAU [redacted] assistance is requested in support of the captioned case.**Full Investigation Initiated:** 09/27/2016**Package Copy:** (U) NYO CART FE [redacted] has placed the image on [redacted]b6  
b7C  
b7E**Details:**

\* Indicates required information.

**1. (U) Service Requested****1.1 \*Identification of requested support**

(U) NYO requests that CEAU examine [redacted]

**1.2 \*Deadline and/or priority status (warrant expiration, court dates, etc.)**[redacted]  
belonging to ANTHONY WEINER. NYO requests that this effort be made as soon as possible.

b7E

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

Title: (U) CEAU,  Case Request for Assistance  
Re: 305G-NY-2082673, 10/06/2016

b7E

**2. (U) Legal Authority**

2.1 \*Proof of legal authority (Include copy in 1A package or reference document serial)

- e.g. Search warrant, Consent to Search, other legal process

Search warrant for laptop was issued, see 305G-NY-2083673, Serial 3.

**3. (U) Device Identification**

3.1 \*Identification of device(s) to be analyzed

- Include make, serial number (S/N), part/model number, description, and associated evidentiary information including 1B, RCFL, and/or Lab numbers

b6  
b7C  
b7E

**4. (U) Brief Synopsis/Background of Case**UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

Title: (U) CEAU, [REDACTED] Case Request for Assistance

b7E

Re: 305G-NY-2082673, 10/06/2016

<p>4.1 *Brief synopsis/background of the case, including victim and subject names, and dates of interest</p>	<p>(U) ANTHONY WEINER may have engaged in sexually explicit chats with [REDACTED]. These chats may reside within WEINER's iPhone 6, which is passcode protected.</p>
--	--

b3  
b6  
b7C

<p><b>5.(U) Previous Analysis/Status of Computer Hard drive</b></p>	
<p>5.1 *Characterization of any previously conducted analysis</p> <p>5.2 *Status of Computer: locked, unlocked, or unknown. Also include password or potential passwords gleaned through other investigative methods</p> <p>5.3 *If device is not considered evidence, state this clearly</p>	<p>(U) NYO CART and DEXT personnel are already reviewing WEINER's laptop [REDACTED]. [REDACTED] No passwords belonging to WEINER have been identified. Efforts to obtain those passwords are ongoing.</p>

OTHER -Sealed

<p><b>6. (U) POC/Special Handling of Evidence</b></p>
---

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

Title: (U) CEAU, [REDACTED] Case Request for Assistance  
Re: 305G-NY-2082673, 10/06/2016

b7E

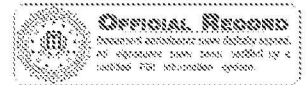
6.1 \*Requestor's point-of-contact information,  
supporting CART examiner, and special handling of  
evidence

(U) Should CEAU have any questions,  
SA [REDACTED] may be  
contacted via cell, [REDACTED]

b6  
b7C

◆◆

UNCLASSIFIED//~~FOUO~~



UNCLASSIFIED

**FEDERAL BUREAU OF INVESTIGATION****Electronic Communication****Title:** (U) Documentation of [REDACTED]**Date:** 10/13/2016

OTHER -Sealed

**From:** NEW YORK

NY-C20

**Contact:** [REDACTED] 212-384-1000**Approved By:** SSA [REDACTED]b6  
b7C**Drafted By:** [REDACTED]**Case ID #:** 305G-NY-2082673(U) ANTHONY WEINER;  
PRODUCERS OF CHILD PORNOGRAPHY  
[REDACTED]

b7E

**Synopsis:** (U) This EC serves to memorialize [REDACTED]  
[REDACTED] in connection with captioned case.

OTHER -Sealed

**Full Investigation Initiated:** 09/27/2016**Enclosure(s):** Enclosed are the following items:

1. (U) [REDACTED]

b3  
b6  
b7C  
b7D**Details:**

OTHER -Sealed

The following [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]b3  
b6  
b7C  
b7D  
OTHER -Sealed

UNCLASSIFIED

**UNCLASSIFIED**

Title: (U) Documentation of

**OTHER -Sealed**

Re: 305G-NY-2082673, 10/13/2016

◆◆

**UNCLASSIFIED**

UNCLASSIFIED

Physical 1A/1C Cover Sheet for Serial Export

**Created From:** 305G-NY-2082673

Serial 9

**Package:** 1A3

**Stored Location:** None

**Summary:** (U) [REDACTED]

**Acquired By:** [REDACTED]

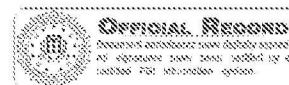
**Acquired On:** 2016-10-12

**Attachment:** (U) [REDACTED]

b6

b7C

OTHER -Sealed



UNCLASSIFIED

**FEDERAL BUREAU OF INVESTIGATION****Collected Item Log**

Event Title: (U) Creation of CART Derivative  
Evidence [REDACTED]

Date: 10/30/2016

Approved By: SSA [REDACTED]

b6  
b7C  
b7E

Drafted By: [REDACTED]

Case ID #: 305G-NY-2082673

(U) ANTHONY WEINER;  
PRODUCERS OF CHILD PORNOGRAPHY  
[REDACTED]

b7E

Full Investigation Initiated: 09/27/2016

Collected From: CART

Receipt Given?: No

Holding Office: NEW YORK

## Details:

Creation of CART DE [REDACTED]

Item Type  
1B Digital

## Description

(U) [REDACTED]  
[REDACTED]b6  
b7C  
b7E

Collected On: 10/30/2016 05:30 AM EDT

Seizing Individual: [REDACTED]

Collected By: [REDACTED]

Location Area: CART

Specific Location: 26 Federal Plaza

Device Type: [REDACTED]  
[REDACTED]

b7E

Designation: Derivative

Number of Devices Collected: 1

UNCLASSIFIED



**UNCLASSIFIED**

Title: (U) Creation of CART Derivative Evidence

**b7E**

Re: 305G-NY-2082673, 10/30/2016

◆◆

**UNCLASSIFIED**

FEDERAL BUREAU OF INVESTIGATION  
FOI/PA  
DELETED PAGE INFORMATION SHEET  
FOI/PA# 1386628-0

Total Deleted Page(s) = 64

Page 1 ~ OTHER - SEALED;  
Page 2 ~ OTHER - SEALED;  
Page 3 ~ OTHER - SEALED;  
Page 4 ~ OTHER - SEALED;  
Page 5 ~ OTHER - SEALED;  
Page 6 ~ OTHER - SEALED;  
Page 7 ~ OTHER - SEALED;  
Page 8 ~ OTHER - SEALED;  
Page 9 ~ OTHER - SEALED;  
Page 10 ~ OTHER - SEALED;  
Page 11 ~ OTHER - SEALED;  
Page 12 ~ OTHER - SEALED;  
Page 13 ~ OTHER - SEALED;  
Page 14 ~ OTHER - SEALED;  
Page 15 ~ OTHER - SEALED;  
Page 16 ~ OTHER - SEALED;  
Page 17 ~ OTHER - SEALED;  
Page 18 ~ OTHER - SEALED;  
Page 19 ~ OTHER - SEALED;  
Page 20 ~ OTHER - SEALED;  
Page 21 ~ OTHER - SEALED;  
Page 22 ~ OTHER - SEALED;  
Page 23 ~ OTHER - SEALED;  
Page 24 ~ OTHER - SEALED;  
Page 25 ~ OTHER - SEALED;  
Page 26 ~ OTHER - SEALED;  
Page 27 ~ OTHER - SEALED;  
Page 28 ~ OTHER - SEALED;  
Page 29 ~ OTHER - SEALED;  
Page 30 ~ OTHER - SEALED;  
Page 31 ~ OTHER - SEALED;  
Page 32 ~ OTHER - SEALED;  
Page 33 ~ OTHER - SEALED;  
Page 34 ~ OTHER - SEALED;  
Page 35 ~ OTHER - SEALED;  
Page 36 ~ OTHER - SEALED;  
Page 37 ~ OTHER - SEALED;  
Page 38 ~ OTHER - SEALED;  
Page 39 ~ OTHER - SEALED;  
Page 40 ~ OTHER - SEALED;  
Page 41 ~ OTHER - SEALED;  
Page 42 ~ OTHER - SEALED;  
Page 43 ~ OTHER - SEALED;  
Page 44 ~ OTHER - SEALED;  
Page 45 ~ OTHER - SEALED;  
Page 46 ~ OTHER - SEALED;  
Page 47 ~ OTHER - SEALED;  
Page 48 ~ OTHER - SEALED;

Page 49 ~ OTHER - SEALED;  
Page 50 ~ OTHER - SEALED;  
Page 51 ~ OTHER - SEALED;  
Page 52 ~ OTHER - SEALED;  
Page 53 ~ OTHER - SEALED;  
Page 54 ~ OTHER - SEALED;  
Page 55 ~ OTHER - SEALED;  
Page 56 ~ OTHER - SEALED;  
Page 57 ~ OTHER - SEALED;  
Page 58 ~ Duplicate;  
Page 59 ~ Duplicate;  
Page 60 ~ OTHER - SEALED;  
Page 61 ~ OTHER - SEALED;  
Page 62 ~ OTHER - SEALED;  
Page 63 ~ OTHER - SEALED;  
Page 64 ~ OTHER - SEALED;

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