IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

THE REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS, and **THE ASSOCIATED PRESS** Plaintiffs, v. **FEDERAL BUREAU OF INVESTIGATION**, and **UNITED STATES DEPARTMENT OF JUSTICE** Defendants.	Civil Action No. 15-cv-01392 (RJL)
THE REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS Plaintiff, v. **FEDERAL BUREAU OF INVESTIGATION**, and **UNITED STATES DEPARTMENT OF JUSTICE** Defendants.	Civil Action No. 18-cv-00345 (RJL)

DECLARATION OF KATIE TOWNSEND

I, Katie Townsend, declare as follows:

1. I am the Legal Director at the Reporters Committee for Freedom of the Press (the "Reporters Committee" or "RCFP"), an unincorporated nonprofit association located in Washington, D.C., a position I have held since May 2018. I am an attorney and counsel of record for Plaintiffs in this matter. Prior to becoming RCFP's Legal Director, I was RCFP's Litigation Director; I held that position from September 2014 to May 2018. I am a member in good standing of the bar for the District of Columbia and am admitted to practice before this Court. I make this declaration in support of Plaintiffs' Opposition to the Motion for Summary Judgment filed by Defendants Federal Bureau of Investigation ("FBI") and U.S. Department of Justice ("DOJ") and in support of Plaintiffs' Cross-Motion for Summary Judgment. I have personal knowledge of the matters stated in this declaration.

2. The Reporters Committee did not receive a letter from the FBI denying expedited processing of FOIPA Request No. 1319138-000, at issue in Case No. 15-1392 (the "2015 Matter").

3. During initial proceedings in the 2015 Matter, Defendants provided Plaintiffs with a letter dated March 28, 2016 with attached records responsive to Plaintiffs' 2014 FOIA Requests. The attached records did not include any pages previously withheld in full. Based on my review of those records, the only additional release of information consists of one word in RCFP-63, and four and a half words and an icon for an attachment to an email in RCFP-65.

4. Defendants did not release any records relating to any specific instance where the FBI impersonated a member of the news media other than the Seattle/Timberline Incident in response to Plaintiffs' 2014 FOIA Requests, at issue in the 2015 Matter, or Plaintiff Reporters Committee's 2017 FOIA Request, at issue in Case No. 18-345 (the "2018 Matter").

5. Other than two records, consisting of 11 pages of material, Defendants did not release any records in the initial proceedings of the 2015 Matter relating to the Seattle/Timberline Incident that date from or post-date October 2014.

6. Attached hereto as **Exhibit A** is a true and correct copy of the following publicly available letter to the editor of *The New York Times*: James Comey, *Letter to the Editor*, The New York Times (Nov. 6, 2014), obtained from https://www.nytimes.com/2014/11/07/opinion/to-catch-a-crook-the-fbis-use-of-deception.html, *archived at* https://perma.cc/GZ4C-N6B5.

7. Attached hereto as **Exhibit B** is a true and correct copy of the following publicly available document that was obtained, at my direction, from ECF: Application and Affidavit for Search Warrant, ECF No. 1, Case No. 3:07-mj-05114-JPD (W.D. Wash. Jun. 12, 2007).

8. Attached hereto as **Exhibit C** is a true and correct copy of the following publicly available document that was obtained, at my direction, from ECF: Search Warrant, ECF No. 2, Case No. 3:07-mj-05114-JPD (W.D. Wash. June 21, 2007).

9. Attached hereto as **Exhibit D** is a true and correct copy of the publicly available docket report for the following case that was obtained, at my direction, from ECF: Case No. 3:07-mj-05114-JPD (W.D. Wash.).

10. Attached hereto as **Exhibit E** is a true and correct copy of the following publicly available news article: Mike Carter, *FBI created fake Seattle Times Web page to nab bomb-threat suspect*, Seattle Times (Oct. 27, 2014), obtained from: http://www.seattletimes.com/seattle-news/fbi-created-fake-seattle-times-web-page-to-nab-bomb-threat-suspect/, *archived at* https://perma.cc/78WE-DMLS.

11. Attached hereto as **Exhibit F** is a true and correct copy of the following publicly available news article: *FBI says it faked AP story to catch bomb suspect*, The Associated Press

(Oct. 28, 2014), https://www.ap.org/ap-in-the-news/2014/fbi-says-it-faked-ap-story-to-catch-bomb-suspect, *archived at* https://perma.cc/7UZN-H5WM.

12. Attached hereto as **Exhibit G** is a true and correct copy of a letter, dated October 30, 2014, from AP's General Counsel Karen Kaiser to then-Attorney General Eric Holder, which is publicly available at https://corpcommap.files.wordpress.com/2014/10/letter_103014.pdf, and archived at https://perma.cc/W46W-2DLW.

13. Attached hereto as **Exhibit H** is a true and correct copy of the following publicly available news article: Editorial, *Deceptions of the F.B.I.*, The New York Times (Oct. 31, 2014), http://mobile.nytimes.com/2014/11/01/opinion/deceptions-of-the-fbi.html, *archived at* https://perma.cc/N8GL-MEYD.

14. Attached hereto as **Exhibit I** is a true and correct copy of a publicly available press release issued by the Office of U.S. Senator Chuck Grassley setting forth the text of a June 12, 2015 letter it states was sent by Senator Grassley to FBI Director James Comey, that was obtained from https://www.grassley.senate.gov/news/news-releases/grassley-seeks-details-fbi-spyware-programs, and is archived at https://perma.cc/5VML-TEAC.

15. Attached hereto as **Exhibit J** is a true and correct copy of the following publicly available report of the Office of the Inspector General for the Department of Justice ("OIG"): *A Review of the FBI's Impersonation of a Journalist in a Criminal Investigation* (Sept. 15, 2016), obtained from https://oig.justice.gov/reports/2016/o1607.pdf, *archived at* https://perma.cc/PF6J-S5NE.

16. Defendants did not provide Plaintiffs with any records responsive to their 2014 FOIA Requests before the 2015 Matter was filed.

17. Defendants did not provide Plaintiff Reporters Committee with any records

responsive to its 2017 FOIA Request before the 2018 Matter was filed.

18. Based on my review of the records produced by the FBI in response to the 2018 Matter and the 2015 Matter on remand from the D.C. Circuit, none of the records produced by the FBI since the D.C. Circuit's December 2017 decision are duplicative of records produced prior to the last round of summary judgment briefing in the 2015 Matter, which was before this Court in 2016. Plaintiffs do not intend to re-litigate any of the withholdings in records that were subject to the first round of summary judgment briefing.

19. Attached hereto as **Exhibit K** are true and correct copies of the following records produced to Plaintiffs in response to their FOIA Requests:

- RCFP-303 – RCFP-306
- RCFP-801 – RCFP-802

20. Attached hereto as **Exhibit L** are true and correct copies of the following records produced to Plaintiffs in response to their FOIA Requests:

- RCFP-344 – RCFP-346
- RCFP-669 – RCFP-671
- RCFP-683

21. Attached hereto as **Exhibit M** are true and correct copies of the following records produced to Plaintiffs in response to their FOIA Requests:

- RCFP-818 – RCFP-819
- RCFP-849 – RCFP-850

22. Attached hereto as **Exhibit N** are true and correct copies of the following records produced to Plaintiffs in response to their FOIA Requests:

- RCFP-289 – RCFP-290

23. Attached hereto as **Exhibit O** are true and correct copies of the following records produced to Plaintiffs in response to their FOIA Requests:

- RCFP-270 – RCFP-271
- RCFP-291 – RCFP-296
- RCFP-434
- RCFP-436
- RCFP-438
- RCFP-448
- RCFP-623 – RCFP-624
- RCFP-629 – RCFP-632

I declare under penalty of perjury that the foregoing is true and correct.

Executed on July 25, 2019.

/s/ Katie Townsend
Katie Townsend

EXHIBIT A

The New York Times

LETTER

To Catch a Crook: The F.B.I.'s Use of Deception

NOVEMBER 6, 2014

To the Editor:

In "Deceptions of the F.B.I." (editorial, Nov. 1), you use a 2007 Seattle bomb threat investigation and a 2014 defense lawyer's characterization of an unrelated Las Vegas illegal gambling investigation to express concern about the prospect of the Federal Bureau of Investigation's "deceptive tactics ... opening the door to constitutional abuses on a much wider scale."

We do use deception at times to catch crooks, but we are acting responsibly and legally.

In 2007, to solve a series of bomb threats and cyberattacks directed at a Seattle-area high school, an F.B.I. agent communicated online with the anonymous suspect. Relying on an agency behavioral assessment that the anonymous suspect was a narcissist, the online undercover officer portrayed himself as an employee of The Associated Press, and asked if the suspect would be willing to review a draft article about the threats and attacks, to be sure that the anonymous suspect was portrayed fairly.

The suspect agreed and clicked on a link relating to the draft "story," which then deployed court-authorized tools to find him, and the case was solved. No actual story was published, and no one except the suspect interacted with the undercover "A.P." employee or saw the fake draft story. Only the suspect was fooled, and it led to his arrest and the end of a frightening period for a high school.

That technique was proper and appropriate under Justice Department and F.B.I. guidelines at the time. Today, the use of such an unusual technique would probably require higher level approvals than in 2007, but it would still be lawful and, in a rare case, appropriate.

The Las Vegas case is still in litigation, so there is little we can say, but it would

have been better to wait for the government's response and a court decision before concluding that the F.B.I. engaged in abusive conduct.

Every undercover operation involves "deception," which has long been a critical tool in fighting crime. The F.B.I.'s use of such techniques is subject to close oversight, both internally and by the courts that review our work.

JAMES B. COMEY
Director
Federal Bureau of Investigation
Washington, Nov. 5, 2014

EXHIBIT B

United States District Court

FILED LODGED ENTERED RECEIVED

JUN 12 2007 LK

CLERK U.S. DISTRICT COURT WESTERN DISTRICT OF WASHINGTON DEPUTY

WESTERN DISTRICT OF WASHINGTON

In the Matter of the Search of any computer accessing electronic message(s) directed to administrator(s) of MySpace account "Timberlinebombinfo" and opening message(s) delivered to that account by the government.

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

CASE NUMBER: MJ07-0388

FILED UNDER SEAL

MJ07-5114

I, U.S. FBI Special Agent Norman B. Sanders, Jr., being duly sworn depose and say:

I am a(n) Special Agent with the Federal Bureau of Investigations (FBI), and have reason to believe that ( ) on the person of or (XX) on the property known as (name, description and/or location)

Any computer accessing electronic message(s) directed to administrator(s) of MySpace account "Timberlinebombinfo" and opening message(s) delivered to that account by the government.

in the Western District of Washington, there is now concealed a certain person or property, namely: (describe the person or property to be seized)

Network level messages, IP addresses, MAC addresses, other variables, and certain registry-type information. **THIS WARRANT DOES NOT SEEK AUTHORIZATION TO OBTAIN THE CONTENT OF ANY ELECTRONIC COMMUNICATIONS.**

which is (state one or more basis for search and seizure set forth under Rule 41(b) of the Federal Rules of Criminal Procedure)

Evidence of a crime

concerning a violation of Title 18 United States Code, Section(s) 875(c); 1030(a)(5)(A)(i) and (B)(iv). The facts to support a finding of Probable Cause are as follows:

See attached Affidavit of Special Agent Norman B. Sanders, Jr.

Continued on the attached sheet and made a part hereof. (X) Yes ( ) No

Signature of Affiant
NORMAN B. SANDERS, JR.

Sworn to before me, and subscribed in my presence:

June 12, 2007 2 pm at Seattle, Washington
Date City and State

JAMES P. DONOHUE, United States Magistrate Judge
Name and Title of Judicial Officer

James P. Donohue
Signature of Judicial Officer

USAO No. 2007R00791

07-MJ-05114-APPL

AFFIDAVIT

MS07 088 JPD

STATE OF WASHINGTON)
) ss:
COUNTY OF KING)

Norman B. Sanders Jr., being duly sworn on oath, deposes and says:

1. I am a Special Agent for the Federal Bureau of Investigation ("FBI"), and have been such for the past five years. Prior to becoming a Special Agent, I was employed by the FBI as a Computer Forensic Examiner, for six and one-half years. I am currently assigned to the Seattle Office's Cyber Crime Squad, which investigates various computer, and Internet-related federal crimes.

2. My experience as an FBI Agent has included the investigation of cases involving Computer Intrusions, Extortion, Internet Fraud, Identity Theft, Crimes Against Children, Intellectual Property Rights, and other federal violations involving computers and the Internet. I have also received specialized training and gained experience in interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, cyber crimes computer evidence identification, computer evidence seizure and forensic processing, and various other criminal laws and procedures. I have personally participated in the execution of arrest warrants and search warrants involving the search and seizure of computers and electronic evidence, as well as paper documents and personal belongings.

3. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, in that I am empowered by law to conduct investigations and to make arrests for federal felony offenses.

4. Relative to this investigation, my duties include the investigation of offenses including violations of Title 18, United States Code, Sections 875(c) (Interstate Transmission of Communication Containing Threat to Injure), and 1030(a)(5)(A)(i) and

Warrant Affd.

(B)(iv) (Computer Intrusion Causing a Threat to Public Safety).

5. I submit this affidavit in support of the application of the United States for a search warrant. This search warrant pertains to the Government's planned use of a specialized technique in a pending criminal investigation. Essentially, if a warrant is approved, a communication will be sent to the computer being used to administer www.myspace.com [1] ("MySpace") user account "Timberlinebombinfo".

The communication to be sent is designed to cause the above referenced computer to transmit data, in response, that will identify the computer and/or the user(s) of the computer.[2] In this manner, the FBI may be able to identify the computer and/or user of the computer that are involved in committing criminal violations of United States Code specifically, Title 18, United States Code, Sections 875(c) (Interstate Transmission of Communication Containing Threat to Injure), and 1030(a)(5)(A)(i) and (B)(iv) (Computer Intrusion Causing a Threat to Public Safety).

More specifically, the United States is applying for a search warrant authorizing:

a). the use of a Computer & Internet Protocol Address[3] ("IP address")

---

[1] MySpace is a international free service that uses the Internet for online communication through an interactive social network of photos, videos, weblogs, user profiles, blogs, e-mail, instant messaging, web forums, and groups, as well as other media formats. MySpace users are capable of customizing their user webpage and profile. Users are also capable of searching or browsing other MySpace webpages and adding other users as "friends". If the person identified approves your "friend" request, he or she will be added to your list of friends. Users are capable of sending MySpace messages and posting comments on other user's MySpace webpages.

[2] In submitting this request, the Government respectfully does not concede that a reasonable expectation of privacy exists in the internet protocol address assigned by a network service provider or other provider to a specific user and used to address and route electronic communications to and from that user. Nor does the government concede that a reasonable expectation of privacy is abridged by the use of this communication technique, or that the use of this technique to collect a computer's IP address, MAC address or other variables that are broadcast by the computer whenever it is connected to the Internet, constitutes a search or seizure.

[3] Conceptually, IP addresses are similar to telephone numbers, in that they are used to identify computers that exchange information over the Internet. An IP address is a unique numeric address used to direct information over the Internet and is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). In general, information sent over the Internet must contain an originating IP address and a destination IP address, which identify the computers sending and receiving the information. Section 216 of the USA Patriot Act (P.L. 107-56) amended 18 U.S.C. §§3121 *et seq* to specifically authorize the recovery of "addressing" and "routing" information of

Verifier ("CIPAV") in conjunction with any computer that administers MySpace user account "Timberlinebombinfo" (http://www.myspace.com/timberlinebombinfo), without prior announcement within ten days from the date this Court authorizes the use of the CIPAV;

b). that the CIPAV may cause any computer - wherever located - that activates any CIPAV authorized by this Court (an "activating computer") to send network level messages[4] containing the activating computer's IP address and/or MAC address,[5] other environment variables, and certain registry-type information[6] to a computer controlled by the FBI;

c). that the FBI may receive and read within ten days from the date this Court authorizes the use of the CIPAV, at any time of day or night, the information that any CIPAV causes to be sent to the computer controlled by the FBI; and

d). that, pursuant to 18 U.S.C. §3103a(b)(3), to satisfy the notification

---

electronic As used here, a network-level message refers to an exchange of technical information between computers. communications by a pen register/trap & trace order.

[4] Such messages work in established network protocols, determining, for example, how a given communication will be sent and received. Every time a computer connected to a local area network (LAN) or to the Internet connects to another computer on the LAN or the Internet, it broadcasts network-level messages, including its IP address, and/or media access control (MAC) address, and/or other "environment variables." A MAC address is an unique numeric address of the network interface card in a computer. Environment variables that may be transmitted include: operating system type and version, browser type and version, the language the browser is using, etc. These network-level messages also often convey network addressing information, including origin and destination information. Network-level messages are used to make networks operate properly, transparently, and consistently.

[5] Computers that access, and communicate on LANs do so via a network interface card (NIC) installed in the computer. The NIC is a hardware device and every NIC contains its own unique MAC address. Every time a computer connected to a LAN communicates on the LAN, the computer broadcasts its MAC address.

[6] As used here, "registry-type information" refers to information stored on the internal hard drive of a computer that defines that computer's configuration as it relates to a user's profile. This information includes, for example, the name of the registered owner of the computer and the serial number of the operating system software installed. Registry information can be provided by a computer connected to the Internet, for example, when that computer connects to the Internet to request a software upgrade from its software vendor.

requirement of Federal Rule of Criminal Procedure 41(f)(3), the FBI may delay providing a copy of the search warrant and the receipt for any property taken until no more than thirty (30) days after such time as the name and location of the owner or user of the activating computer is positively identified or a latter date as the court may, for good cause shown, authorize. Provision of a copy of the search warrant and receipt may, in addition to any other methods allowed by law, be effectuated by electronic delivery of true and accurate electronic copies (e.g. Adobe PDF file) of the fully executed documents.

6. I am thoroughly familiar with the information contained in this Affidavit, which I have learned through investigation conducted with other law enforcement officers, review of documents, and discussions with computer experts. Because this an application for a search warrant and pen register, not every fact known about the investigation is set forth, but only those that are pertinent to the application. As a result of the investigation, I submit there is probable cause to believe the MySpace "Timberlinebombinfo" account, e-mail account "dougbriggs123@gmail.com"; e-mail account "dougbrigs@gmail.com"; e-mail account "dougbriggs234@gmail.com"; e-mail account "thisisfromitaly@gmail.com"; and e-mail account "timberline.sucks@gmail.com" have been used to transmit interstate communications containing threats to injure, and involve computer intrusion causing a threat to public safety in violation of Title 18, United States Code, Sections 875(c) and 1030(a)(5)(A)(i) and (B)(iv). I further submit that there is probable cause to believe that using a CIPAV in conjunction with the target MySpace account (Timberlinebombinfo) will assist in identifying the individual(s) using the activating computer to commit these violations of the United States Code.

7. In general, a CIPAV utilizes standard Internet computer commands commonly used commercially over local area networks (LANs) and the Internet to request that an activating computer respond to the CIPAV by sending network level

messages, and/or other variables, and/or registry information, over the Internet[7] to a computer controlled by the FBI. The exact nature of these commands, processes, capabilities, and their configuration is classified as a law enforcement sensitive investigative technique, the disclosure of which would likely jeopardize other on-going investigations and/or future use of the technique. As such, the property to be accessed by the CIPAV request is the portion of the activating computer that contains environmental variables and/or certain registry-type information; such as the computer's true assigned IP address, MAC address, open communication ports, list of running programs, operating system (type, version, and serial number), internet browser and version, language encoding, registered computer name, registered company name, current logged-in user name, and Uniform Resource Locator (URL) that the target computer was previously connected to.

8. An Internet Service Provider (ISP) normally controls a range of several hundred (or even thousands) of IP addresses, which it uses to identify its customers' computers. IP addresses are usually assigned "dynamically": each time the user connects to the Internet, the customer's computer is randomly assigned one of the available IP addresses controlled by the ISP. The customer's computer retains that IP address until the user disconnects, and the IP address cannot be assigned to another user during that period. Once the user disconnects, however, that IP address becomes available to other customers who connect thereafter. ISP business customers will commonly have a permanent, 24-hour Internet connection to which a "static" (i.e., fixed) IP address is assigned. Practices for assigning IP addresses to Internet users vary, with many providers assigning semi-persistent numbers that may be allocated to a single user for a period of days or weeks.

9. Every time a computer accesses the Internet and connects to a web site,

[7] The "Internet" is a global computer network, which electronically connects computers and allows communications and transfers of data and information across state and national boundaries. To gain access to the Internet, an individual utilizes an Internet Service Provider (ISP). These ISP's are available worldwide.

that computer broadcasts its IP address along with other environment variables. Environment variables, such as what language the user is communicating in, allows the web site to communicate back and display information in a format that the computer accessing the web site can understand. These environment variables, including but not limited to, the IP address and the language used by the computer, may assist in locating the computer, as well as provide information that may help identify the user of the computer.

10. The hard drives of some computers contain registry-type information. A registry contains, among other things, information about what operating system software and version is installed, the product serial number of that software, and the name of the registered user of the computer. Sometimes when a computer accesses the Internet and connects to a software vendor's web site for the purpose of obtaining a software upgrade, the web site retrieves the computer's registry information stored on its internal hard drive. The registry information assists the software vendor in determining if that computer is running, among other information, a legitimate copy of their software because the registry information contains the software's product registration number. Registry information, such as the serial number of the operating system software and the computer's registered owner, may assist in locating the computer and identifying its user(s).

THE INVESTIGATION

11. On May 30, 2007, a handwritten note was discovered on the premises of the Timberline High School in Lacey, Washington. Subsequently, school administrators ordered an evacuation of the students based on the handwritten bomb threat note.

a). On June 4, 2007, Timberline High School received a bomb threat e-mail from sender: "dougbriggs123@gmail.com". The Unknown Subject(s) (UNSUB) stated in the e-mail "I will be blowing up your school Monday, June 4,

2007. There are 4 bombs planted throughout timberline high school. One in the math hall, library hall, main office and one portable. The bombs will go off in 5 minute intervals at 9:15 AM." In addition, the UNSUB(s) stated, "The email server of your district will be offline starting at 8:45 am." The UNSUB(s) launched a Denial-of-Service (DOS)[8] attack on the Lacey School District computer network, which caused over 24,000,000 hits on the system within a 24 hour period. School administrators ordered an evacuation of the school on June 4, 2007.

b). On June 5, 2007, the UNSUB(s) sent an e-mail from "dougbrigs@gmail.com" stating the following:

> <<Read This ASAP>>
> Now that the school is scared from yesturdays fake bomb threat it's now time to get serious. One in a gym locker, the girls. It's in a locker hidden under a pile of clothes. The other four I will only say the general location. One in the Language Hall, One in the math hall, One underneath a portable taped with strong ducktape. This bomb will go off if any vibrations are felt. And the last one, Is in a locker. It is enclosed in a soundproof package, and litteraly undetectable. I have used a variety of chemicals to make the bombs. They are all different kinds.
>
> They will all go off at 10:15AM. Through remote detonation. Good Luck. And if that fails, a failsafe of 5 minutes later.

The UNSUB(s) goes on to state:

> Oh and for the police officers and technology idots at the district office trying to track this email and yesturdays email's location. I can give you a hint. The email was sent over a newly made gmail account, from overseas in a foreign country. The gmail account was created there, and this email and yesturdays was sent from there. So good luck talking with Italy about getting the identify of the person who owns the 100Mbit dedicated server

c). In another e-mail from sender "dougbriggs234@gmail.com" the UNSUB(s) states the following:

> Hello Again. Seeing as how you're too stupid to trace the email back lets get serious." [The UNSUB(s) mentions 6 bombs set to

---

[8] A DOS attack is an Internet based computer attack in which a compromised system attacks a single target, thereby causing a denial of service for users of the targeted computer system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users. The DOS attack is generally targeted at a particular network service, such as e-mail or web access.

detonate between 10:45-11:15 AM, and adds] Seriously, you are not going to catch me. So just give up. Maybe you should hire Bill Gates to tell you that it is coming from Italy. HAHAHA Oh wait I already told you that. So stop pretending to be "tracing it" because I have already told you it's coming from Italy. That is where trace will stop so just stop trying. Oh and this email will be behind a proxy behind the Italy server.

d). School administrators ordered an evacuation of the school on June 5, 2007.

e). On June 6, 2007, Principle Dave Lehnis of Timberline High School received an e-mail from sender: "dougbriggs911@gmail.com". The e-mail contained the following text: "ENJOY YOUR LIFE ENDING".

f). In another e-mail from "dougbriggs911@gmail.com," the UNSUB(s) states the following,

> Well hello Timberline, today is June 6, 2007 and I"M just emailing you today to say that school will blow up and that's final! There are 2 bombs this time (Iran short on money to buy things at home depot). They will go off at exactly 10:45:00 AM. One is on located on a portable. And the other is somewhere else. Keep trying to 'trace' this email. The only thing you will be able to track is that it came from Italy. There is no other information that leads it back to the United States in any way so get over it. You should hire Bill Gates to track it for you. HAHAHAHA. He will just tell you that it came from over seas, so if you have close relations with the POPE you might get some information. But other than that, have fun looking in Italy. :-)
> Also, stop advising teachers to no show this email to classmates. Everyone would be ammused by this email and I might stop if you do. Funny how I can trick you all into thinking that I included my name to show that it isn't me, because who the hell would put their name? Or is that just what I want you to think.
> And yet again, this email was sent from overseas to a newly made email account that has
> already been deleted of all information by the time you read this email. Get your ass on a plane to Italy if you want it to stop.

g). School administrators ordered an evacuation of the school on June 6, 2007.

h). On June 7, 2007, Timberline High School received an e-mail from sender "thisisfromitaly@gmail.com." The UNSUB(s) states:

"There are 3 bombs planted in the school and they're all different kinds. I have premade these weeks in advance and tested the timers to make sure they work to exact millisecond. Locking the doors is a good plan, but too late."

i). School administrators ordered an evacuation of the school on June 7, 2007.

j). On June 7, 2007, the UNSUB(s) posted three of the threatening e-mails in the comments section of the online news publication service, "theolympian". The administrator from theolympian.com" removed the threatening e-mail postings. Shortly thereafter, the UNSUB(s) re-posted the threatening e-mails. Eventually, the administrator of "theolympian.com" disabled the "Comments" section.

k). On June 7, 2007, Detective Jeremy Knight, Lacey Police Department (LPD), received information from the Thurston County Sheriff's Office, which had revealed a complaint from a person identified as AG. AG stated that she received an invitation through myspace.com from the MySpace profile of "Timberlinebombinfo" wanting her to post a URL link to http://bombermails.hyperphp.com on her myspace.com webpage. The UNSUB(s) advised her that failure to comply would result in her name being associated with future bomb threats. Similarly, Knight received a phone call from a parent alleging that her son received the same request from the UNSUB(s). According to Knight, 33 students received a request from the UNSUB(s) to post the link on their respective myspace.com webpages. Subsequent interviews performed by Knight yielded limited information.

l). On June 7, 2007, VW and BP received MySpace private invitations from an individual utilizing the MySpace moniker "Timberlinebombinfo". VW accepted the invitation from "Timberlinebombinfo" and received an America Online Instant Message (AIM) from an individual utilizing AIM screen name

"Alexspi3ring_09." Communication ceased with "Alexspi3ring_09" after VW requested additional information related to the bomb threats. VW believed screen name "Alexspi3ring_09" was associated to ALEX SPIERING, a student at Timberline High School. VW stated "Alexspi3ring_09" and "Timberlinebombinfo" used to have the identical graphic on their MySpace webpage. "Timberlinebombinfo" recently changed his/her graphic from a picture of guns to a picture of a bomb.

m). On June 7, 2007, Thurston County School District reported ALEX SPIERING resides at 6133 Winnwood Loop SE, Olympia, WA, 98513, telephone (360) 455-0569, date of birth [redacted], 19[redacted].

n). On June 8, 2007, Comcast Internet, Thorofare, New Jersey, reported that residential address 6133 Winnwood Loop SE, Olympia, WA, 98513 received Comcast Internet services for the following subscriber:

Sara Spiering
6133 Winnwood Loop SE, Lacey, WA 98513
Telephone (360) 455-0569
Dynamically Assigned Active Account
Account Number: 8498380070269681

o). On June 8, 2007, Thurston County School District received two additional bomb threat e-mails from "Timberline.Sucks@gmail.com," which resulted in the evacuation of the Timberline High School.

12. On June 4, 2007, Google provided subscriber, registration, and IP Address log history for e-mail address "dougbriggs123@gmail.com" with the following results:

Status: Enabled (user deleted account)
Services: Talk, Search History, Gmail

Name: Doug Briggs
Secondary Email:
Created on: 03-Jun-2007
Lang: en
IP: 80.76.80.103
LOGS: All times are displayed in UTC/GMT
dougbriggs123@gmail.com

Date/Time	IP
04-Jun-2007 05:47:29 am	81.27.207.243
04-Jun-2007 05:43:14 am	80.76.80.103
03-Jun-2007 06:19:44 am	80.76.80.103

a). On June 6, 2007, a SmartWhoIs lookup of IP Address 80.76.80.103 resolved to Sonic S.R.L, Via S.Rocco l, 24064, Grumello Del Monte, Italy, Phone: +390354491296, E-mail: Staff@sonic.it. Your affiant connected to http://sonic.it, which displayed an Italian business webpage for Sonic SRL Internet Service Provider.

b). On June 7, 2007, a request to MySpace for subscriber and IP Address logs for MySpace user "Timberlinebombinfo" provided the following results:

User ID:	199219316
First Name:	Doug
Last Name:	Briggs
Gender:	Male
Date of Birth:	12/10/1992
Age:	14
Country:	US
City:	Lacey

Postal Code: 985003
Region: Western Australia
Email Address: timberline.sucks@gmail.com
User Name: timberlinebombinfo
Sign up IP Address: 80.76.80.103
Sign up Date: June 7, 2007 7:49PM
Delete Date: N/A
Login Date June 7, 2007 7:49:32:247 PM IP Address 80.76.80.103

c). FBI Seattle Division contacted FBI Legate Attache Rome, Italy and an official request was provided to the Italian National Police requesting assistance in *contacting Sonic SRL and locating the compromised computer utilizing IP Address* 80.76.80.103.

d). On June 7, 2007, the System Administrator for the www.theolympian.com advised the posting of the bomb threat e-mails originated from IP Address 192.135.29.30. A SmartWhois lookup resolved 192.135.29.30 to "The National Institute of Nuclear Physics (INFN), LNL - Laboratori Nazionali di Legnaro, Italy".

13. Based on my training, experience, and the investigation described herein, I know the following among other things:

a). that network level messages, including the originating IP address and MAC address, other variables, and certain registry-type information of a computer can be used to assist in identifying the individual(s) using that computer; and

b). the individual(s) using the aforementioned activated computer utilized compromised computers to conceal their true originating IP address and thereby intentionally inhibiting the individual(s)' identification. Compromised computers are generally infected with computer viruses, trojans, or other malevolent programs, which can allow a user the ability to control computer(s) on the Internet or particular services

of compromised computer(s) without authorization. It is common for individuals engaged in illegal activity to access and control compromised computer(s) to perform malicious acts in order to conceal their originating IP addresses.

14. Based on training, experience, and the investigation described herein, I have concluded that using a CIPAV on the target MySpace "Timberlinebombinfo" account may assist the FBI to determine the identities of the individual(s) using the activating computer. A CIPAV's activation will cause the activating computer to send network level messages, including the activating computer's originating IP address and MAC address, other variables, and certain registry-type information. This information may assist the FBI in identifying the individual(s) using the activating computers.

15. The CIPAV will be deployed through an electronic messaging program from an account controlled by the FBI. The computers sending and receiving the CIPAV data will be machines controlled by the FBI. The electronic message deploying the CIPAV will only be directed to the administrator(s) of the "Timberlinebombinfo" account.

a). Electronic messaging accounts commonly require a unique user name and password.

b). Once the CIPAV is successfully deployed, it will conduct a one-time search of the activating computer and capture the information described in paragraph seven.

c). The captured information will be forwarded to a computer controlled by the FBI located within the Eastern District of Virginia.

d). After the one-time search, the CIPAV will function as a pen register device and record the routing and destination addressing information for electronic communications originating from the activating computer.

e). **The pen register will record IP address, dates, and times of the electronic communications, but not the contents of such communications or the contents contained on the computer, and forward the IP address data to a computer controlled by the FBI, for a period of (60) days.**

CONCLUSION

16. Based upon my review of the evidence, my training and experience, and information I have gathered from various computer experts, I have probable cause to believe that deploying a CIPAV in an electronic message directed to the administrator(s) of the MySpace "Timberlinebombinfo" account will assist in identifying a computer and individual(s) using the computer to transmit bomb threats and related communications in violation of Title 18, United States Code Sections 875(c) and 1030(a)(5)(A)(i) and (B)(iv).

17. Because notice as required by Federal Rule of Criminal Procedure 41(f)(3) would jeopardize the success of the investigation, and because the investigation has not identified an appropriate person to whom such notice can be given, I hereby request authorization to delay such notice until an appropriate person is identified. Further, assuming providing notice would still jeopardize the investigation after an appropriate person to receive notice is identified, I request permission to ask this Court to authorize an additional delay in notification. In any event, the United States government will notify this Court when it identifies an appropriate person to whom to give notice, so that this Court may determine whether notice shall be given at that time.

18. Because there are legitimate law enforcement interests that justify an unannounced use of the CIPAV and review of the messages generated by the activating

computer in this case,[9] I ask this Court to authorize the proposed use of a CIPAV without the prior announcement of its use. One of these legitimate law enforcement interests is that announcing the use of the CIPAV would assist a person controlling the activating computer(s) to evade revealing its true IP address, other variables, and certain registry-type information - thereby defeating the CIPAV's purpose.

19. Rule 41(e)(2) requires that (A) the warrant command the FBI "to execute the warrant within a specified time no longer than 10 days" and (B) "execute the warrant during the daytime unless the judge for good cause expressly authorizes execution at another time..." In order to comply with Rule 41, the Government will only deploy CIPAV between the hours of 6:00 a.m. and 10:00 p.m. (PST) during an initial 10-day period. However, the Government seeks permission to read any messages generated by the activating computer as a result of a CIPAV at any time of day or night during the initial 10-day period. This is because the individuals using the activating computer may activate the CIPAV after 10:00 p.m. or before 6:00 a.m., and law enforcement would seek to read the information it receives as soon as it is aware of the CIPAV response given the emergent nature of this investigation. If the CIPAV is not activated within the initial 10-day period, the Government will seek further authorization from the Court to read any information sent to the computer controlled by the FBI as a result of that CIPAV after the 10th day from the date the Court authorizes the use of the first CIPAV.

20. Because the FBI cannot predict whether any particular formulation of a CIPAV to be used will cause a person(s) controlling the activating computer to activate a CIPAV, I request that this Court authorize the FBI to continue using additional CIPAV's in conjunction with the target MySpace account (for up to 10 days after this warrant is authorized), until a CIPAV has been activated by the activating computer.

---

[9] See Wilson v. Arkansas, 514 U.S. 927, 936 (1995) (recognizing that "law enforcement interests may . . . establish the reasonableness of an unannounced entry.")

21. Accordingly, it is respectfully requested that this Court issue a search warrant authorizing the following:

a). the use of multiple CIPAVs until one CIPAV is activated by the activating computer in conjunction with the target MySpace "Timberlinebombinfo" account, without prior announcement, within 10 days from the date this Court authorizes the use of the first CIPAV;

b). the CIPAV may cause an activating computer - wherever located - to send network level messages containing the activating computer's IP address, and/or MAC address, and/or other variables, and/or certain registry-type information to a computer controlled by the FBI and located within the Eastern District of Virginia;

c). that the FBI may receive and read, at any time of day or night, within 10 days from the date the Court authorizes of use of the CIPAV, the information that any CIPAV causes to be sent to the computer controlled by the FBI;

d). that once the FBI has received an initial CIPAV response from the activating computer consisting of network level messages containing the activating computer's IP address, and/or MAC address, and/or other variables, and/or certain registry-type information, the FBI will thereafter only be collecting the types of addressing and routing information that can be collected pursuant to a pen register order; and

e). that, pursuant to 18 U.S.C. §3103a(b)(3), to satisfy the notification requirement of Federal Rule of Criminal Procedure 41(f)(3), the FBI may delay providing a copy of the search warrant and the receipt for any property taken until no more than thirty (30) days after such time as the name and location of the individual(s) using the activating computer is positively identified or a latter date as the court may, for good cause shown, authorize. Provision of a copy of the search warrant and receipt may, in addition to any other methods allowed by law, be effectuated by electronic delivery of true and accurate electronic copies (e.g. Adobe PDF file) of the fully executed documents.

22. It is further requested that this Application and the related documents be filed under seal. The information to be obtained is relevant to an on-going investigation. Premature disclosure of this Application and related documents may jeopardize the success of the above-described investigation.

WHEREFORE, Affiant respectfully requests that a warrant be issued authorizing the FBI to utilize a CIPAV and receive the attendant information according to the terms set forth in this Affidavit.

THIS APPLICATION DOES NOT SEEK AUTHORIZATION TO OBTAIN THE CONTENT OF ANY ELECTRONIC COMMUNICATIONS, AND THE WARRANT WILL SO SPECIFY.

Norman B. Sanders
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me this 12th day of June, 2007

Hon. James P. Donohue
United States Magistrate Judge

EXHIBIT C

United States District Court

WESTERN DISTRICT OF WASHINGTON

FILED ENTERED
LODGED RECEIVED

JUN 2 1 2007

AT SEATTLE
CLERK U.S. DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
DEPUTY

In the Matter of the Search of

(Name, address or brief description of person or property to be searched)

any computer accessing electronic message(s) directed to administrator(s) of MySpace account "Timberlinebombinfo" and opening message(s) delivered to that account by the government.

MJ07-5114 JPD

SEARCH WARRANT

CASE NUMBER: ~~MS07-088~~

FILED UNDER SEAL

To: NORMAN B. SANDERS, JR., and any Authorized Officer of the United States.

Affidavit(s) having been made before me by NORMAN B. SANDERS, JR., who has reason to believe that ( ) on the person of or (X) on the property or premises known as (name, description and/or location)

Any computer accessing electronic message(s) directed to administrator(s) of MySpace account "Timberlinebombinfo" and opening message(s) delivered to that account by the government.

in the Western District of Washington, there is now concealed a certain person or property, namely:
(describe the person or property)

Network level messages, IP addresses, MAC addresses, other variables, and certain registry-type information.
THIS WARRANT DOES NOT SEEK AUTHORIZATION TO OBTAIN THE CONTENT OF ANY ELECTRONIC COMMUNICATIONS.

I am satisfied that the affidavit(s) and any record testimony establish probable cause to believe that the person or property so described is now concealed on the person or premises above-described and establish ground for the issuance of this warrant.

YOU ARE HEREBY COMMANDED to search on or before June 22, 2007 (Date) JPD 10 days

(not to exceed 10 days) the person or place named above for the person or property specified, serving this warrant and making the search (in daytime -- 6:00 AM to 10:00 PM) (at any time in the day or night as I find reasonable cause has been established) and if the person or property be found there to seize same, leaving a copy of this warrant and receipt for the person or property taken, and prepare a written inventory of the person or property seized and promptly return this warrant to **a United States Magistrate Judge** as required by law.

June 12, 2007 2pm
Date and Time

at Seattle, Washington
City and State

JAMES P. DONOHUE, U.S. Magistrate Judge
Name and Title of Judicial Officer

Signature of Judicial Officer

07-MJ-05114-RCPT

USAO No. 2007R00791

RETURN

DATE WARRANT RECEIVED	DATE & TIME WARRANT EXECUTED	COPY OF WARRANT & RECEIPT FOR ITEMS LEFT WITH
6-12-2007	6-13-2007 5:49pm	N/A

INVENTORY MADE IN THE PRESENCE OF

N/A - EXECUTED ON INTERNET

INVENTORY OF PERSON OR PROPERTY TAKEN PURSUANT TO THE WARRANT

1 CDROM CONTAINING CIPAV RESULTS.

CERTIFICATION

I swear that this inventory is a true and detailed account of the person or property taken by me on the warrant.

Subscribed, sworn to, and returned to me this date.

James P. Bourdette
U.S. Judge or Magistrate

June 21, 2007
Date

EXHIBIT D

CLOSED

U.S. District Court
United States District Court for the Western District of Washington (Tacoma)
CRIMINAL DOCKET FOR CASE #: 3:07-mj-05114-JPD All Defendants

Case title: USA v. MySpace account "Timberlinebombinfo"

Date Filed: 06/12/2007
Date Terminated: 06/21/2007

Assigned to: Hon. James P. Donohue

Defendant (1)

MySpace account "Timberlinebombinfo"
TERMINATED: 06/21/2007

Pending Counts	**Disposition**
None	

Highest Offense Level (Opening)

None

Terminated Counts	**Disposition**
None	

Highest Offense Level (Terminated)

None

Complaints	**Disposition**
None	

Plaintiff

USA represented by **Kathryn A Warma**
US ATTORNEY'S OFFICE (SEA)
700 STEWART ST
STE 5220
SEATTLE, WA 98101-1271
206-553-7970
Email: ECF-CRM.USAWAW@usdoj.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Date Filed	#	Docket Text
06/12/2007	1	APPLICATION FOR Search WARRANT issued, by Judge James P. Donohue. (Attachments: # 1 search warrant) (PV,) (Entered: 06/12/2007)
06/21/2007	2	Search Warrant Returned Executed on 6/13/07 in case as to MySpace account "Timberlinebombinfo". ***Case terminated. ***Case unsealed. (JT,) (Entered: 06/21/2007)

PACER Service Center

Transaction Receipt

04/21/2016 09:08:13

PACER Login:	rc0719:2620841:0	**Client Code:**	
Description:	Docket Report	**Search Criteria:**	3:07-mj-05114-JPD
Billable Pages:	1	**Cost:**	0.10

EXHIBIT E

FBI created fake Seattle Times Web page to nab bomb-threat suspect

Originally published October 27, 2014 at 12:00 am *Updated October 29, 2014 at 9:47 pm*

By Mike Carter
Seattle Times staff reporter

The FBI in Seattle created a fake news story on a bogus Seattle Times web page to plant software in the computer of a suspect in a series of bomb threats to Lacey's Timberline High School in 2007, according to documents obtained by the Electronic Frontier Foundation (EFF) in San Francisco.

The deception was publicized Monday when Christopher Soghoian, the principal technologist for the American Civil Liberties Union in Washington, D.C., revealed it on Twitter.

In an interview, Soghoian called the incident "outrageous" and said the practice could result in "significant collateral damage to the public trust" if law enforcement begins co-opting the media for its purposes.

The EFF documents reveal that the FBI dummied up a story with an Associated Press byline about the Thurston County bomb threats with an email link "in the style of The Seattle Times," including details about subscriber and advertiser information.

The link was sent to the suspect's MySpace account. When the suspect clicked on the link, the hidden FBI software sent his location and Internet Protocol information to the agents. A juvenile suspect was identified and arrested June 14.

The revelation brought a sharp response from the newspaper.

"We are outraged that the FBI, with the apparent assistance of the U.S. Attorney's Office, misappropriated the name of The Seattle Times to secretly install spyware on the computer of a crime suspect," said Seattle Times Editor Kathy Best.

"Not only does that cross a line, it erases it," she said.

"Our reputation and our ability to do our job as a government watchdog are based on trust. Nothing is more fundamental to that trust than our independence — from law enforcement, from government, from corporations and from all other special interests," Best said. "The FBI's actions, taken without our knowledge, traded on our reputation and put it at peril."

An AP spokesman also criticized the tactic.

"We are extremely concerned and find it unacceptable that the FBI misappropriated the name of The Associated Press and published a false story attributed to AP," Paul Colford, director of AP media relations. "This ploy violated AP's name and undermined AP's credibility."

Frank Montoya Jr., the special agent in charge of the FBI in Seattle, defended the investigation and the technique, which court records show led to the arrest and conviction of a 15-year-old student.

"Every effort we made in this investigation had the goal of preventing a tragic event like what happened at Marysville and Seattle Pacific University," Montoya said. "We identified a specific subject of an investigation and used a technique that we deemed would be effective in preventing a possible act of violence in a school setting.

"Use of that type of technique happens in very rare circumstances and only when there is sufficient reason to believe it could be successful in resolving a threat," he said.

Ayn Dietrich-Williams, the spokeswoman for the FBI-Seattle, pointed out that the bureau did not use a "real Seattle Times article, but material generated by the FBI in styles common in reporting and online media."

Assistant U.S. Attorney Tessa Gorman, chief of the office's criminal division, was reviewing the EFF documents provided to her by The Times and had no immediate comment. Kathryn Warma, the prosecutor who oversaw the case, has since retired.

The EFF posted 172 pages of documents concerning the FBI's use of a software tool called a "Computer and Internet Protocol Address Verifier" (CIPAV) in two cases — one involving the Timberline High School bomb threats and the other involving an extortion attempt against a cruise line in Florida. More than half of the documents relate to the Seattle case.

According to the documents, CIPAV lets the FBI "geophysically" locate a computer and its Internet Protocol address.

Soghoian said the software is activated when someone clicks on the bogus link. The technique apparently exploits the same computer-security vulnerabilities

used by hackers.

Police in Lacey, Thurston County, contacted the Northwest Cyber-Crime Task Force after the school began receiving a series of bomb threats beginning in late May 2007 and continuing into early June. The school was forced to evacuate students at least twice, and police were unable to identify a suspect.

The documents indicate the FBI in Seattle obtained a search warrant to "deploy" the CIPAV software after the task force, which is run by the FBI, received a public tip about a suspect. Special Agent Norman Sanders, in seeking the warrant, said the bureau would send a "communication" to the suspect's computer that would make the computer identify itself for the agent.

The case was taken up by the U.S. Attorney's Office, which helped draft and approve the warrant. The warrant does not say that "communication" would be a bogus news story that appeared to be published online by The Seattle Times.

Mike Carter: mcarter@seattletimes.com or 206-464-3706

***Mike Carter**: 206-464-3706 or mcarter@seattletimes.com; on Twitter: @stimesmcarter.*

Contact

About the company

Advertise

Subscriber Services

Today's Front Page

Facebook

Twitter

EXHIBIT F

FBI says it faked AP story to catch bomb suspect

By GENE JOHNSON, The Associated Press

Oct. 28, 2014

SEATTLE (AP) — The FBI confirmed Tuesday it faked an Associated Press story to catch a bomb threat suspect in 2007, but now says it did not spoof a Seattle Times Web page as part of the investigation.

Police in Lacey, near Olympia, sought the FBI's help as repeated bomb threats prompted a week of evacuations at Timberline High School in June 2007.

After police interviews of potential suspects came up empty, the agency obtained a warrant from a federal magistrate judge to send a "communication" to a social media account associated with the bomb threats, with the idea of tricking the suspect into revealing his location, according to documents obtained by the San Francisco-based Electronic Frontier Foundation.

The "communication," which contained a software tool that could verify Internet addresses, turned out to be a link to a phony AP story about the bomb threats posted on a Web page created by the FBI. The 15-year-old suspect clicked on the link, revealing his computer's location and Internet address, and helping agents confirm his identity.

The documents suggested the bogus story was posted on a fake Seattle Times site, but Seattle FBI spokeswoman Ayn Dietrich said Tuesday that was wrong. Instead, she said an undercover agent sent the teen a hyperlink that simply said "article," and nowhere was The Seattle Times referenced.

The confusion stemmed from an email between FBI employees that referred to an "email link in the style of The Seattle Times," but that link was simply provided as an example of what a news story link might look like, Dietrich said.

The FBI did not initially respond to AP's request earlier Tuesday for further detail about the fake story, beyond saying the ruse was necessary as part of the investigation.

"Every effort we made in this investigation had the goal of preventing a tragic event like what happened at Marysville and Seattle Pacific University," said Frank Montoya Jr., the FBI's special agent in charge in Seattle, referring to two local school shootings this year. "We identified a specific subject of an investigation and used a technique that we deemed would be effective in preventing a possible act of violence in a school setting. Use of that type of technique happens in very rare circumstances and only when there is sufficient reason to believe it could be successful in resolving a threat."

AP spokesman Paul Colford said Tuesday the FBI's "ploy violated AP's name and undermined AP's credibility."

"We are extremely concerned and find it unacceptable that the FBI misappropriated the name of The Associated Press and published a false story attributed to AP," Colford said in a statement.

Kathy Best, editor of The Seattle Times, said in a statement that while the newspaper was "pleased to hear" the FBI did not use the paper's name, it would have preferred to have found that information out earlier from the agency "instead of a defense of the tactic" Monday after the FBI was presented with internal agency documents showing a mocked up, phony Seattle Times email and Web page.

"Even if The Seattle Times name wasn't used, the issues raised are the same. The FBI, in placing the name of The Associated Press on a phony story sent to a criminal suspect, crossed a line and undermined the credibility of journalists everywhere — including at The Times," Best said.

Dietrich said she had no information about how often the FBI has faked news stories during investigations beyond Montoya's description that it was "very rare."

"In order to safeguard the FBI's ability to effectively detect, disrupt, and dismantle threats to the public, we must be judicious in how we discuss investigative techniques," Dietrich said in an email.

The documents revealing the deception were publicized Monday on Twitter by Christopher Soghoian, the principal technologist for the American Civil Liberties Union.

___

Follow Johnson at https://twitter.com/GeneAPseattle

EXHIBIT G

AP
ASSOCIATED PRESS

Karen Kaiser
General Counsel

450 West 33rd Street
New York, NY 10001
T 212.621.7287

www.ap.org

October 30, 2014

Attorney General Eric Holder
U.S. Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530-0001

Dear Attorney General Holder,

I am writing to protest in the strongest possible terms the FBI's fabrication and publication of a fake Associated Press news story in connection with its June 2007 investigation of a school bombing threat in the state of Washington.

AP learned of the FBI's ploy only this week, more than seven years after the incident occurred. Documents released under FOIA reveal that the FBI, seeking to implant a form of tracking technology onto the computer of a bomb threat suspect, created a phony AP news story to entice the suspect to click on the fake article so that the FBI could identify the suspect's location. In carrying out this scheme, the FBI both misappropriated the trusted name of The Associated Press and created a situation where our credibility could have been undermined on a large scale.

While AP is sensitive to the demands on law enforcement, particularly when addressing threats of school violence, the government's actions in this case were entirely unacceptable. It is improper and inconsistent with a free press for government personnel to masquerade as The Associated Press or any other news organization. The FBI may have intended this false story as a trap for only one person. However, the individual could easily have reposted this story to social networks, distributing to thousands of people, under our name, what was essentially a piece of government disinformation.

The FBI's actions also raise serious constitutional concerns. By creating false news accounts, misrepresenting the source of a news story, and falsely attributing it to the AP, the FBI undermined the most fundamental component of a free press -- its independence. Any attempt by the government, whatever its motives, to falsely label its own messages as coming from the news media serves to undermine the vital distinction between the government and the press in society. Such actions also compromise our ability to gather the news safely and effectively in parts of the world where our credibility rests on the basis of AP operating freely and independently. The Department of Justice should neither condone nor permit such conduct.

The actions taken by the FBI in this case inflict a very serious harm, and raise issues that need to be addressed promptly by the Department. We ask that you review the circumstances that led to this incident, and disclose promptly the authority under which this action was taken and who authorized the action. We also ask you to make public whether this type of impersonation of the press has occurred in other situations, and if so, how often it has occurred and what policies exist within the Department of Justice to govern this type of activity.

AP does not believe it is ever appropriate for the government to misrepresent itself as an independent news organization, and we seek your immediate assurance that the Department will never again misrepresent itself as the AP. We also call upon you to put into place appropriate policies and guidelines to ensure that the Department never again resorts to the conduct that occurred here.

We request an opportunity to discuss our concerns with the Department in the near future and to learn how the Department plans to address these critical issues.

Thank you for your prompt attention to this matter.

Respectfully submitted,

Karen Kaiser

EXHIBIT H

The New York Times

EDITORIAL

Deceptions of the F.B.I.

By THE EDITORIAL BOARD
OCTOBER 31, 2014

If your Internet service goes down and you call a technician, can you be certain that the person who arrives at your door is actually there to restore service? What if he is a law enforcement agent in disguise who has disabled the service so he can enter your home to look around for evidence of a crime?

Americans should not have to worry about scenarios like this, but F.B.I. agents used this ruse during a gambling investigation in Las Vegas in July. Most disturbing of all, the Justice Department is now defending the agents' actions in court.

During the 2014 World Cup, the agents suspected that an illegal gambling ring was operating out of several hotel rooms at Caesar's Palace in Las Vegas, but they apparently did not have enough evidence to get a court-issued warrant. So they enlisted the hotel's assistance in shutting off the Internet to those rooms, prompting the rooms' occupants to call for help. Undercover agents disguised as repairmen appeared at the door, and the occupants let them in. While pretending to fix the service, the agents saw men watching soccer matches and looking at betting odds on their computers.

There is nothing illegal about visiting sports-betting websites, but the agents relied primarily on that evidence to get their search warrant. What they failed to tell the judge was that they had turned off the Internet service themselves.

Of course, law enforcement authorities regularly rely on sting operations and other deceptive tactics, and courts usually allow them if the authorities reasonably believe they will find evidence of a crime. Without that suspicion, the Constitution prohibits warrantless searches of peoples' residences, including hotel rooms. The authorities can jump that hurdle if a home's occupant consents to let them enter, as when an undercover officer is invited into a home to buy drugs.

The Las Vegas case fails on both counts, according to a lawyer for the defendants. Although one of the defendants in the case, Wei Seng Phua, a Malaysian citizen, had been arrested in Macau earlier this year for running an illegal sports-gambling business, the agents did not have probable cause to believe anything illegal was happening in two of the rooms they searched. And a federal prosecutor had initially warned the agents not to use trickery because of the "consent issue." In fact, a previous ruse by the agents had failed when a person in one of the rooms refused to let them in.

In a separate case out of Seattle, F.B.I. agents pretended to be journalists in a 2007 investigation of high school bomb threats, according to documents recently uncovered by the Electronic Frontier Foundation. Agents there concocted a fake online news article by The Associated Press about the threats. They sent a link to the Myspace page of a student they suspected of making the threats, and when he opened the link, it downloaded malware that enabled the agents to track him down and arrest him. The A.P. is rightly outraged and has protested the F.B.I.'s misappropriation of its name as undermining "the most fundamental component of a free press — its independence."

The F.B.I. has a history of pushing the limits that protect Americans' civil liberties. And it has continued to broaden agents' investigative powers in troubling ways. The deceptive tactics used in Las Vegas and Seattle, if not prohibited by the agency or blocked by courts, risk opening the door to constitutional abuses on a much wider scale.

Meet The New York Times's Editorial Board »

219 COMMENTS »

EXHIBIT I

Grassley Seeks Details on FBI Spyware Programs

Jun 12, 2015

WASHINGTON – Senator Chuck Grassley, Chairman of the Senate Judiciary Committee, is pressing the Federal Bureau of Investigation (FBI) for more information on its spyware program.

The request comes amid the Justice Department's push to amend Rule 41 of the Federal Rules of Criminal Procedure in order to allow judges to grant warrants for remote searches of computers located outside their district or when the location of the computer is unknown. Currently, federal prosecutors generally must seek a warrant in the judicial district in which the target of the search is located.

In a letter to FBI Director James Comey, Grassley wrote, "It is essential that law enforcement has the necessary technological tools and legal framework to keep the public safe," however, "Publicly available information on the FBI's use of spyware is often inconsistent."

Grassley noted that the FBI's reported capabilities in this area can raise privacy concerns and in order to perform its constitutional duty of oversight, it's important that the committee understand the FBI's use of spyware and the Justice Department's proposed changes to the legal framework through which the FBI receives judicial approval.

The questions posed by Grassley to the FBI center on the types of spyware programs used; their capabilities; the FBI's internal policies and procedures for using spyware; the legal processes used; the methods of deploying spyware; and the audit procedures used to ensure the spyware is used in compliance with both FBI policies and the law.

A copy of the text of the letter is below. A signed copy of the letter can be found here.

June 12, 2015

VIA ELECTRONIC TRANSMISSION
The Honorable James B. Comey, Jr.
Director
Federal Bureau of Investigation
935 Pennsylvania Avenue, N.W.
Washington, D.C. 20535

Dear Director Comey:

I am writing in regard to the Federal Bureau of Investigation's ("FBI") use of spyware. According to press reports, spyware programs can be remotely deployed to a targeted computer to surreptitiously activate the computer's camera and microphone; collect passwords; search the computer's hard drive, random-access memory, and other storage media; generate latitude and longitude coordinates for the computer's location; and intercept phone calls, texts, and social media messages. Obviously, the use of such capabilities by the government can raise serious

privacy concerns.

As you and I discussed at an oversight hearing in May of last year, the Department of Justice is currently seeking to amend Federal Rule of Criminal Procedure 41 ("Rule 41") to allow the Department to deploy spyware more easily. Rule 41 applies to search and seizure warrants, and under the current version of the rule, federal prosecutors generally must seek a warrant in the judicial district in which the target of the search is located. [1] This can be a difficult task in the context of cybercrime. The Justice Department's proposed changes would, under certain circumstances, allow judges to grant warrants for remote searches of computers located outside their district or when the location is unknown -- changes that would allow the FBI to more easily obtain approval to infiltrate computer networks to covertly install spyware. [2] The proposed changes would not affect the requirement that, in order for the FBI to obtain a warrant under the rule, it must demonstrate probable cause that the targeted device contains evidence of a crime.

It is essential that law enforcement has the necessary technological tools and legal framework to keep the public safe. However, a number of organizations have raised concerns about the scope of the proposed rule change, including constitutional concerns, risks of forum-shopping, and potential extraterritorial use. [3] Despite these concerns, the U.S. Courts' Judicial Conference Advisory Committee on Criminal Rules voted in favor of the change in March of this year, as did the next group in the review process, the Courts' Standing Committee, on May 28. [4] In keeping with the process for modifying the rules, the proposed change will next be considered by the Judicial Conference, and if approved there, by the Supreme Court, with a Congressional review period to follow.

Although the uses of stealthy surveillance and deception to catch criminals are lawful and well-recognized investigative tactics under certain circumstances, and although the FBI's use of spyware in general has long been reported, [5] the Committee needs more specific information about the FBI's current use of spyware in order to fulfill its oversight responsibilities, including: the types of spyware programs used; their capabilities; the FBI's internal policies and procedures for using spyware; the legal processes used; the methods of deploying spyware; and the audit procedures used to ensure the spyware is used in compliance with both FBI policies and the law.

Publicly available information on the FBI's use of spyware is often inconsistent. It is unclear from public reporting which spyware programs the FBI currently uses and what their capabilities are. While some press reports have stated that FBI spyware merely logs a target's "IP address, MAC address, computer programs running, operating system details, browser details, and other identifying computer information," [6] a 2013 court order denying an FBI warrant application stated that the "application request[ed] authorization to surreptitiously install data extraction software [that] has the capacity to search the computer's hard drive, random access memory, and other storage media; to activate the computer's built-in camera; to generate latitude and longitude coordinates for the computer's location; and to transmit the extracted data to FBI agents." [7] A Washington Post article also reported that the FBI's spyware can "covertly download files, photographs[,] and stored e-mails, or even gather real-time images by activating cameras connected to computers[.]" [8] Similarly, while some press reports have described a spyware program developed in-house by the FBI, [9] others have noted that the U.S. government is now the largest purchaser of malware from the private sector, [10] and there are reports that another component of the Justice Department has purchased such private-sector spyware. [11]

The procedures used by the FBI to obtain approval to deploy spyware and the methods of such deployment also raise important issues. The Washington Post has reported that FBI agents "obtain warrants to search a suspect's computer but generally do not inform the judge of an intent to hack the computer to install the malware." [12] The Washington Post also reported that the most common delivery method for installing the spyware is phishing attacks, in which the FBI masquerades as a trustworthy source in order to trick the target into clicking on a link infected with the spyware. [13] In one publicly-reported case, FBI agents posed as the Associated Press and created a fake AP news article in a successful phishing effort to deploy spyware. [14] However, in the relevant search warrant application, the agents "did not alert the judge of their plan to mimic the media." [15] After learning of the ruse, the AP stated "[w]e find it unacceptable that the FBI misappropriated the name of the Associated Press and published a false story attributed to the AP. This ploy violated AP's name and undermined AP's credibility." [16] It is also unclear from public reporting whether the FBI uses other methods of spyware deployment in addition to phishing,

such as zero-day exploits, which exploit vulnerabilities in legitimate software applications.

In short, the FBI's use of spyware and the DOJ's proposed changes to the legal framework through which the FBI receives judicial approval to do so raise several important questions. The Committee needs additional information from the FBI in order to address them. Accordingly, please provide written responses to these questions by June 26, 2015:

1. Which spyware, related programs, and other network investigative techniques has the FBI used in the field since 2009? Please include both government-created programs and ones purchased externally, if any, from companies such as Hacking Team and Gamma Group International.

a. What are each program's capabilities?

b. How much has the FBI spent on each program?

c. How many times has the FBI used each of these programs in the field, and in what capacity? How many times has the FBI used the programs to remotely activate the subject device's camera or microphone?

2. What are the internal FBI policies and procedures related to requesting, approving, deploying, and terminating the use of spyware and related programs? Please provide copies of all guidance documents.

3. Pursuant to what legal authorities does the FBI deploy spyware and related programs?

a. Does the FBI always obtain a search warrant or other judicial approval prior to using such programs? If not, why not?

b. Does the FBI use different legal authorities or processes based on the jurisdiction in which it determines the target to be located?

c. Does the FBI use different legal authorities or processes if it cannot determine the jurisdiction in which the target is located?

4. Has the FBI deployed spyware on behalf of state or local law enforcement? If so, what are the internal FBI policies and procedures related to doing so?

5. When the FBI seeks a warrant to search a computer, does it always notify the judge when it intends to hack the targeted computer and surreptitiously install spyware? Does it specify in the warrant application the capabilities of the spyware it seeks to deploy? Does it specify the method of deployment to be used?

6. What methods does the FBI use to deploy spyware? Please list each method of deployment used in the field since 2009 and the number of times it has been used.

7. Does the FBI use zero-day exploits in conjunction with its use of spyware?

a. If so, are these zero-day exploits developed by the government or purchased externally from private companies, such as Vupen Security?

b. If so, how much has the FBI spent on developing or purchasing zero-day exploits? Please list both the cost for in-house development and external purchases.

c. If so, does the FBI ever notify the company that owns the exploited software of the security breach? If it does, what policies guide the timing and content of this disclosure? If it does not, why not?

8. As noted above, the FBI has acknowledged using phishing to deploy spyware, and impersonating a real media outlet in doing so. Since 2009, how many times has the FBI impersonated personnel from legitimate companies, whether media or otherwise, in deploying spyware?

a. Which companies has it impersonated?

b. Does the FBI notify the companies it impersonates that it has done so? If so, what policies guide the timing and content of this disclosure? If not, why not?

9. For how long does the FBI retain any data obtained through spyware?

a. Who has access to the data while it is in the FBI's possession?

b. How, if at all, is the data destroyed?

10. What internal audit procedures does the FBI use to ensure that spyware and related programs are used in accordance with agency policies, procedures, and the law?

a. If they exist, have such internal audit procedures discovered any violations of FBI policies, procedures, or applicable law relating to the use of spyware or related programs? Has the FBI discovered any such violations through other means?

b. If so, please provide the details of each violation, as well as any remedial or punitive measures taken in response.

Please number your answers according to their corresponding questions. In addition, please arrange for FBI officials to provide a briefing to Judiciary Committee staff about these issues following the provision of your responses, but in any event no later than July 2, 2015. If you have any questions about this request, feel free to contact Patrick Davis of my Committee staff at (202) 224-5225. Thank you for your attention to these important matters.

Charles E. Grassley
Chairman
Senate Committee on the Judiciary

1 Fed. R. Crim. P. 41(b)(1), subject to exceptions in Fed. R. Crim. P. 41(b)(2)-(5).
2 Dustin Volz, FBI's Plan to Expand Hacking Power Advances Despite Privacy Fears, NATIONAL JOURNAL, Mar. 16, 2015, available at http://www.nationaljournal.com/tech/fbi-s-plan-to-expand-hacking-power-advances-despite-privacy-fears-20150316.
3 Dustin Volz, Google Calls FBI's Plan to Expand Hacking Power a 'Monumental' Constitutional Threat, NATIONAL JOURNAL, Feb. 18, 2015; Stan Schroeder, Proposed Rule Would Give U.S. Power to Cybersnoop Worldwide, Google Warns, MASHABLE, Feb. 19, 2015.
4 Cory Bennett, FBI Request to Expand Hacking Power Advances, THE HILL, Mar. 17, 2015; Cory Bennett, FBI Inches Closer to Expanded Search Powers, THE HILL, May 29, 2015; Tim Cushing, Judicial Committee Gives FBI The First OK It Needs To Hack Any Computer, Anywhere On The Planet, TECHDIRT, Mar. 17, 2015.
5 Craig Timberg and Ellen Nakashima, FBI's Search for "Mo," Suspect in Bomb Threats, Highlights Use of Malware for Surveillance, THE WASHINGTON POST, Dec. 6, 2013; see Kevin Poulsen, Documents: FBI Spyware Has Been Snaring Extortionists, Hackers for Years, WIRED, Apr. 16, 2009.
6 Kate Knibbs, The FBI Has Its Own Secret Brand Of Malware, GIZMODO, April 2, 2015; Kevin Poulsen, FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats, WIRED, July 18, 2007.
7 In re Warrant to Search a Target Computer at Premises Unknown, 958 F.Supp.2d 753, 755

(S.D. Tex. 2013); see Jennifer Valentino-DeVries, Judge Denies FBI Request to Hack Computer in Probe, THE WALL STREET JOURNAL, Apr. 24, 2013.

8 Craig Timberg and Ellen Nakashima, FBI's Search for "Mo," Suspect in Bomb Threats, Highlights Use of Malware for Surveillance, THE WASHINGTON POST, Dec. 6, 2013.

9 Supra n. 6.

10 Zack Whittaker, U.S. Government Becomes the 'Biggest Buyer' of Malware, ZDNET, May 13, 2013; see Joseph Menn, Special Report: U.S. Cyberwar Strategy Stokes Fear of Blowback, REUTERS, May 10, 2013.

11 Lorenzo Franceschi-Bicchierai, The DEA Has Secretly Been Buying Hacking Tools From An Italian Company, MOTHERBOARD, April 15, 2015; Timothy J. Seppala, The DEA's Using Powerful Spyware For Surveillance Too, ENDGAGET, April 16, 2015.

12 Ellen Nakashima and Paul Farhi, FBI Lured Suspect With Fake Web Page, But May Have Leveraged Media Credibility, THE WASHINGTON POST, Oct. 28, 2014.

13 Craig Timberg and Ellen Nakashima, FBI's Search for "Mo," Suspect in Bomb Threats, Highlights Use of Malware for Surveillance, THE WASHINGTON POST, Dec. 6, 2013.

14 Supra n. 12; see James B. Comey, To Catch a Crook: The FBI's Use of Deception, Letter to the Editor, THE NEW YORK TIMES, Nov. 6, 2014.

15 Supra n. 12.

16 Id.

-30-

EXHIBIT J

Office of the Inspector General
U.S. Department of Justice

A Review of the FBI's Impersonation of a Journalist in a Criminal Investigation

Revised September 2016

EXECUTIVE SUMMARY

Over the course of 1 week in June 2007, a 15-year old high school student e-mailed a series of bomb threats to administrators and staff at Timberline High School, near Seattle, Washington. The threats caused daily school evacuations. The individual used "proxy servers" to e-mail the bomb threats in order to hide his location. When local law enforcement officials were unable to identify or locate the individual, they requested assistance from a cybercrime task force supervised by the Federal Bureau of Investigation's (FBI) Seattle Field Division.

FBI agents on the task force, working with FBI technology and behavioral experts at Headquarters (FBIHQ), developed a plan to surreptitiously insert a computer program into the individual's computer that would identify his location. An FBI undercover agent posed as an editor for the Associated Press (AP) and attempted to contact the individual through e-mail. During subsequent online communications, the undercover agent sent the individual links to a fake news article and photographs that had the computer program concealed within them. The individual activated the computer program when he clicked on the link to the photographs, thereby revealing his location to the FBI. FBI and local law enforcement agents subsequently arrested the individual and he confessed to e-mailing the bomb threats.

The FBI did not publicize the assistance its agents provided local law enforcement. However, on July 18, 2007, 2 days after the individual pleaded guilty, an online technology news website published an article that detailed the method by which the FBI identified the individual. Seven years later, in October 2014, *The Seattle Times* published an article that disclosed the fact that an FBI employee posed as a member of the news media when it contacted and then identified the subject as the author of the bomb threats. Later that same month the AP sent a letter to then-Attorney General Eric Holder protesting the FBI's impersonation of a member of the news media in connection with the FBI's investigation of the bomb threats. In addition, several newspapers wrote articles questioning the tactics the FBI used to identify and arrest the subject who sent the threats.

One week later, on November 6, 2014, FBI Director James Comey wrote a letter to the editor of *The New York Times* defending the FBI's actions. In particular, Comey stated that the "technique [the FBI used to identify and apprehend the individual who sent the threats] was proper and appropriate under Justice Department and F.B.I. guidelines at the time" and that "[t]oday, the use of such an unusual technique would probably require higher level approvals than in 2007, but it would still be lawful and, in a rare case, appropriate."

That same day, the Reporters Committee for Freedom of the Press, on behalf of 25 other news organizations, wrote a letter to Comey and Holder voicing its objection to the practice of FBI agents impersonating journalists, saying the practice endangers the media's credibility and undermines its independence, and that it appeared to violate FBI guidelines for when such tactics were permissible.

We initiated this review to examine whether under Department of Justice and FBI policies in effect at the time of the 2007 investigation, agents obtained the appropriate approval for the undercover activities the FBI conducted to locate the individual e-mailing the bomb threats. We also examined whether the undercover activities in 2007 would require a higher level of approval if conducted today under current Department and FBI polices.

As described in our full report, we concluded that FBI policies in 2007 did not expressly address the tactic of agents impersonating journalists. We further found that the FBI's undercover policies then in effect provided some relevant guidance, but were less than clear. As a result, we believe that the judgments agents made about aspects of the planned undercover activity in 2007 to pose as an editor for the AP did not violate the undercover policies in place at the time. We also determined that once the undercover plan was launched, certain investigative decisions were made concerning communications the undercover agent sent to the individual suspected of making the bomb threats that could have increased the level of approval required under FBI policy, a possibility the investigative team did not appear to fully consider.

As we were finalizing this report, the FBI adopted a new interim policy in June 2016 that provides guidance to FBI employees regarding their impersonation of members of the news media during undercover activity or an undercover operation (defined as a series of related undercover activities over a period of time). We found that prior to the adoption of this new interim policy, FBI policy would not have prohibited FBI employees from engaging in the undercover activities agents conducted during the 2007 Timberline investigation. The new interim policy, however, clearly prohibits FBI employees from engaging in undercover activity in which they represent, pose, or claim to be members of the news media, unless the activity is authorized as part of an undercover operation. In order for such an operation to be authorized, an application must first be approved by the head of the FBI field office submitting the application to FBIHQ, reviewed by the Undercover Review Committee at FBIHQ, and approved by the Deputy Director, after consultation with the Deputy Attorney General.

We believe the FBI's new interim policy is a significant improvement to policies that existed in 2007 during the Timberline investigation, as well as to those policies that would have governed similar undercover activities prior to June 2016. The new interim policy also is an important extension of policies the Department of Justice has previously implemented to regulate certain law enforcement activities that affect members of the news media, such as obtaining information from or about members of the news media in criminal and civil investigations. The FBI should move expeditiously to update its undercover policy guide to incorporate this new interim policy, and widely inform and educate FBI employees about the policy's existence and application.

Based upon our review, we made three recommendations to help ensure that FBI policies governing certain undercover activities and operations are well known, clear, and understood. The FBI concurred with the recommendations.

TABLE OF CONTENTS

I. Introduction

On Sunday, June 3, 2007 an unknown subject, later identified by the Federal Bureau of Investigation (FBI) as 15-year old high school student Charles Jenkins, sent an e-mail containing a bomb threat to numerous teachers and administrators of Timberline High School, near Seattle, Washington.[1] The high school was evacuated the next day. Jenkins e-mailed bomb threats to the school every day of the next week, causing daily evacuations.

Jenkins used "proxy servers" located in Europe to send his e-mails in a manner that would hide his true location. As a result, local law enforcement officials were not able to identify or locate Jenkins and they requested assistance from the Northwest Cybercrime Task Force, which was supervised by the FBI's Seattle Division. The FBI immediately opened an investigation.

FBI agents developed a plan to surreptitiously insert a computer program into Jenkins's computer that would identify his true location. An FBI undercover agent posed as an editor for the Associated Press (AP) and contacted Jenkins through e-mail. During subsequent online communications, the undercover agent sent Jenkins links to a fake news article and photographs that had the computer program embedded within them. Jenkins activated the computer program when he clicked on the link to the photographs, thereby revealing Jenkins's true location to the FBI.

FBI and local law enforcement agents subsequently arrested Jenkins and he confessed to e-mailing the bomb threats. On July 16, 2007 Jenkins pleaded guilty as a juvenile to several state felony offenses and was sentenced to 90 days of juvenile detention, 2 years of supervised release, 2 years of mental health counseling, and 2 years of probation with restrictions on internet and computer usage. Jenkins was also expelled from school.

The FBI did not publicize the assistance its agents provided local law enforcement. However, on July 18, 2007, 2 days after Jenkins pleaded guilty, the online technology news website Wired.Com released an article entitled "FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats" that detailed the method by which the FBI identified Jenkins. Seven years later, on October 27, 2014, *The Seattle Times* released an article based upon e-mails obtained by the Electronic Frontier Foundation through a Freedom of Information Act request to the FBI. Those e-mails disclosed the fact that the FBI posed as a member of the news media when it contacted and then identified Jenkins as the author of the bomb threats.

On October 30, 2014, the AP sent a letter to then-Attorney General Eric Holder protesting the FBI's impersonation of a member of the news media in connection with its investigation of the bomb threats. In addition, several

[1] Charles Jenkins is a pseudonym.

newspapers wrote articles questioning the tactics the FBI used to identify and arrest Jenkins.

One week later, on November 6, 2014, FBI Director James Comey wrote a letter to the editor of *The New York Times* defending the FBI's actions. In particular, Comey stated that the "technique [the FBI used to identify and apprehend Jenkins] was proper and appropriate under Justice Department and F.B.I. guidelines at the time" and that "[t]oday, the use of such an unusual technique would probably require higher level approvals than in 2007, but it would still be lawful and, in a rare case, appropriate."

The same day, the Reporters Committee for Freedom of the Press (RCFP), on behalf of 25 other news organizations, wrote a letter to Comey and then-Attorney General Eric Holder voicing its objection to the practice of FBI agents impersonating journalists, saying the practice endangers the media's credibility and undermines its independence, and that it appeared to violate FBI guidelines for when such tactics are permissible.[2]

We initiated this review to examine whether under Department of Justice (DOJ or Department) and FBI policies in effect at the time of the 2007 investigation, agents obtained the appropriate approval for the undercover activities the FBI conducted to locate Jenkins. We also examined whether the undercover activities in 2007 would require a higher level of approval if conducted today under current Department and FBI polices.

We concluded that FBI policies in 2007 did not expressly address the tactic of agents impersonating journalists. We further found that the FBI's undercover policies then in effect provided some guidance, but were less than clear. As a result, we believe that the judgments agents made about aspects of the planned undercover activity in 2007 did not violate the undercover policies in place at the time. We also determined that once the undercover plan was launched, certain investigative decisions were made that could have increased the level of approval required, a possibility the investigative team did not appear to fully consider.

On June 8, 2016, as we were finalizing this report, the FBI adopted a new interim policy that provides guidance to FBI employees regarding their impersonation of members of the news media during undercover activity or an undercover operation (defined as a series of related undercover activities over a period of time). Under this new policy, FBI agents may only represent, pose, or claim to be members of the news media when authorized by the FBI Deputy

[2] The RCFP also urged the FBI to publicly disclose when and under what circumstances they have digitally impersonated the news media in the past. The RCFP and the AP also filed a request for such records under the Freedom of Information Act (FOIA). When no records were provided, on August 27, 2015, the two media organizations filed a civil action against the FBI and Department of Justice under FOIA seeking an order requiring the agencies to comply with the FOIA request. The FBI subsequently released responsive documents to RCFP and AP in February and March 2016. In the still ongoing litigation, RCFP and the AP are seeking release of the documents the FBI withheld from disclosure pursuant to certain FOIA exemptions.

Director, after consultation with the Deputy Attorney General, as part of an undercover operation reviewed by the Undercover Review Committee (UCRC). The policy expressly prohibits FBI employees from engaging in such activity if it is not part of an undercover operation. Therefore, the undercover activities in 2007 would be prohibited today unless they were part of an undercover operation reviewed by the UCRC and authorized by the FBI Deputy Director, after consultation with the Deputy Attorney General.[3]

Based upon our review, we made three recommendations to help ensure that FBI policies governing certain undercover activities and operations are well known, clear, and understood. The FBI concurred with the recommendations.

II. Methodology of the OIG's Review and Organization of Report

In undertaking this review, the OIG examined approximately 2000 documents, including the FBI's investigative case file, applicable Department and FBI policies and guidelines, and a 2014 briefing paper prepared by FBI staff for Director Comey detailing the events surrounding the 2007 investigation and the applicable investigative standards currently in effect, including the new interim policy adopted by the FBI on June 8, 2016. We also interviewed FBI employees and a federal prosecutor who participated in the 2007 investigation and an FBI attorney who helped draft the 2014 briefing paper. In addition, we reviewed correspondence from the news media raising concerns regarding the undercover operation and the comments of Director Comey.

In Section III of this report, we identify the applicable Department and FBI policies and guidelines. In Section IV, we describe the facts and circumstances of the FBI's investigation of the 2007 Timberline bomb threats and the media's response to the FBI ruse to identify Jenkins. In Section V, we analyze whether the case agents followed the applicable guidelines in 2007 and whether different or additional approvals would be required under current Department and FBI policies.

III. Applicable Department and FBI Policies and Guidelines

A. Policies and Guidelines in Effect at Time of 2007 Investigation

1. Undercover Activity and Undercover Operations

In June 2007, the applicable FBI policies for online undercover criminal investigations were contained in the Manual of Investigative Operations & Guidelines, Part 2 (MIOG 2), Section 10-18; and the FBI's Field Guide for

[3] The FBI is in the process of incorporating the new interim policy into the Undercover Policy Guide, one of several policy implementation guides incorporated by reference into the FBI's Domestic Investigations and Operations Guide (DIOG). The DIOG sets forth FBI policies and procedures for all investigative activities and intelligence collection activities conducted by the FBI within the United States.

Undercover and Sensitive Operations (FGUSO). The MIOG 2 and the FGUSO incorporated the Attorney General's Guidelines on FBI Undercover Operations (AGG-UCO), and specifically with respect to online undercover investigations, also incorporated principles detailed in the Department's "Online Investigative Principles for Federal Law Enforcement Agents" (the Online Principles).[4] As we discuss later, both the MIOG 2 and the FGUSO were superseded by the FBI guidelines that are in effect today.

Section 10-18.5(a) of MIOG 2 permitted FBI employees to communicate online using false names or cover-identities and stated that undercover activity was governed by the FGUSO. While an FBI employee's use of another person's "online identity" in undercover online communications without that person's knowledge or consent required FBI Headquarters (FBIHQ) approval, FBI policy did not require special approval to use the identity of an organization or business in undercover online communications or in other undercover activities. MIOG § 10-8.5(4).[5] The FGUSO defined "undercover activities" as "any investigative activity involving the use of an assumed name or cover-identity by an employee of the FBI or another Federal, state, or local law enforcement organization working with the FBI." Undercover activity in which an undercover employee planned to meet with a subject required the approval of a Supervisory Special Agent (SSA).

The FGUSO differentiated between "undercover activity" and an "undercover operation." It defined an "undercover operation" as "an investigation involving a series of related undercover activities over a period of time by an undercover employee." According to the FGUSO, this "generally consists of more than three separate substantive contacts by an undercover employee with the individual(s) under investigation." Undercover operations had to be approved by the Special Agent-in-Charge (SAC) of the field office conducting the operation, in consultation with the Chief Division Counsel for the field office.

In regard to online undercover operations, the FGUSO specifically defined such operations as being "any investigation involving a series of related online covert contacts over a period of time by an Online Covert Employee (OCE)." According to the Online Principles, "[t]he nature of online communications makes counting undercover 'contacts' much more difficult than in the physical world. Generally, a physical-world contact consists of a single communication or conversation, either face-to-face or over the telephone, naturally circumscribed in time." The Principles state that "[c]ommunicating in cyberspace is different"

[4] The FGUSO was last updated on July 25, 2003. The current AGG-UCO was issued on May 30, 2002 and was modified on March 5, 2008, November 26, 2008, and November 22, 2015.

[5] Further, "untrue representations by a person participating in the undercover operation concerning the activities or involvement of any third person" without that person's knowledge or consent were considered "sensitive circumstances" under FBI policy and required FBIHQ approval. FGUSO § 3.2(F)(13). The undercover agent who communicated with Jenkins did not use the "online identity" of a person who was a member of the media, nor did he make untrue representations about any third person. Rather, the agent used the identity of a third party – the AP – without that party's knowledge or consent.

because the online conversation between the OCE and the subject is broken up by the send/receipt nature of online communications.

The FGUSO provided guidance to FBI agents about how to count online communications for purposes of undercover activities. The FGUSO stated that agents should count a discrete online "conversation" as one contact and identified numerous factors that agents should consider when deciding how to group distinct online transmissions into a single conversation. The FGUSO, quoting the AGG-UCO, stated that:

> In the context of online communications, such as e-mail and Internet Relay Chat (IRC), multiple transmissions or e-mail messages can constitute one contact, much like a series of verbal exchanges can comprise a single conversation. Factors to be considered in determining whether multiple online transmissions constitute a single contact or multiple contacts include the time between transmissions, the number of transmissions, the number of interruptions, topical transitions, and the media by which the communications are exchanged (i.e., e-mail versus IRC).

If based on these factors, an agent determined the undercover activity was expected to involve three or fewer "contacts," it was sufficient to obtain approval from the agent's supervisor. If the agent determined the activity was expected to involve more than three "contacts," the activity would constitute an "undercover operation" and required SAC approval. As discussed below, regardless of the number of contacts, if undercover activity or an undercover operation involved "sensitive circumstances," the field office was required to obtain FBIHQ approval.

2. Sensitive Circumstances

Under the FGUSO, undercover activity that involved "sensitive circumstances" constituted an undercover operation regardless of the number of contacts involved. Among the categories of "sensitive circumstances" identified in the FGUSO were "privileged relationships" in which:

> there [was] a reasonable expectation that the undercover operation [would] involve . . . [a] significant risk that a third party [would] enter into a professional or confidential relationship with a person participating in an undercover operation who [was] acting as an attorney, physician, clergyman, or *member of the news media*.

(Emphasis added) According to commentary included in the FGUSO regarding this provision, the professional or confidential relationships are listed in order to identify potential operational scenarios, including those in which "a relationship with a subject is established which the subject believes to be privileged." The commentary further states that while "[i]t is often the case in these scenarios that

these apparent problems never actually materialize or that, if they do, measures can be taken to mitigate them . . . their existence alone is a sensitive matter. . . ."[6]

The FGUSO required that in all undercover operations involving any sensitive circumstances, including online undercover operations, the SAC had to submit an application to FBIHQ seeking approval to begin the undercover operation. This application would then be reviewed by appropriate supervisory personnel at FBIHQ and, if favorably recommended, sent to the Criminal Undercover Operations Review Committee (CUORC) for consideration. The application would then be forwarded to the Director or a designated Assistant Director to approve or disapprove.

In regard to online undercover operations, Section 7.3 of the FGUSO permitted a SAC, or a designated Assistant Special Agent-in-Charge (ASAC), to grant interim authority for online undercover contacts involving sensitive circumstances. The interim authority, which must have been documented in writing, could be granted for up to 30 days and had to be followed by a report explaining the reason for granting the authority "as soon as practical."

3. Limitations on Online Undercover Activity

Section 10-18.3(1)(d) of MIOG 2 prohibited FBI agents from hacking into computers, including those belonging to subjects of FBI investigations, without legal authorization. Section 10-18.3 stated that "[s]oftware tools cannot be used to defeat the security system of [a] targeted electronic facility or access areas that are not already publicly viewable by general users of the system or the public absent a search warrant or other legal authorization." As an example, the provision identified Internet Protocol addresses as information that could not be obtained through software tools without legal authorization.

B. Applicable Policies and Guidelines Currently in Effect

In 2008, the FBI replaced the MIOG 2 with the Domestic Investigations and Operations Guide (DIOG). The DIOG was updated in October 2011.[7] In August

---

[6] Another category of "sensitive circumstances" under the FGUSO was "third party liability" and included:

> Untrue representations by a person participating in the [undercover operation] concerning the activities or involvement of any third person without that individual's knowledge or consent; [and]
>
> . . .
>
> Activities which create a realistic potential for significant claims against the United States arising in tort, contract, or for compensation for the "taking" of property, or a realistic potential for significant claims against individual government employees alleging Constitutional torts.

AGG-UCO, Section IV(C)(2)(o); FGUSO, Section 3.2(F). We did not find these provisions applicable to the undercover activities at issue in the Jenkins investigation: the undercover agent did not make untrue representations to Jenkins about any third person, and we do not believe the FBI's activities created a "realistic potential for significant claims against the United States" as contemplated by the FGUSO.

2011, the FBI replaced the FGUSO with the Undercover and Sensitive Operations Policy Implementation Guide (USOPIG). The DIOG and the USOPIG, like the FGUSO, incorporate the AGG-UCO. As such the USOPIG retained many of the provisions of the FGUSO, including the provisions relating to "sensitive circumstances," and is the FBI policy currently in effect regarding undercover activities and operations.[8] While these revised FBI policies included an additional provision that might have caused a field office to seek FBIHQ approval before an employee acted in an undercover capacity as a member of the media, the revised undercover policies did not require such a step.

On June 8, 2016, the FBI adopted an interim policy – referred to as Policy Notice (PN) 0907N, "Undercover Activities and Operations – Posing as a Member of the News Media or a Documentary Film Crew" – specifically governing situations in which FBI employees represent, pose, or claim to be members of the news media. The new policy sets forth the approval required to engage in such activity.[9] In essence it created an additional "sensitive circumstance" for undercover activity and is the operative policy currently in effect for purposes of our review.[10]

The new interim policy incorporates the DIOG's definitions of "undercover activity" and "undercover operation," which mirror the definitions contained in the FGUSO, as described earlier. In short, "undercover activity" is any investigative activity involving the use of an assumed identity by an undercover employee; an "undercover operation" is one that involves a "series of related undercover activities" – defined as five or more substantive contacts by an undercover employee with the individuals under investigation – over a period of time. However, under the new interim policy, the number of substantive contacts with an investigative subject is not a relevant factor in determining the level of approval required when posing as a member of the news media. This is because the policy expressly prohibits FBI employees from engaging in any undercover activity in which they represent, pose, or claim to be members of the news media, unless the activity is authorized at FBIHQ as part of an undercover operation. DIOG § 8.1.3.1. and 11.9.1.

---

[7] All references to the DIOG in this section of the report are referring to the 2011 edition.

[8] The USOPIG and the DIOG include provisions that expressly address an FBI employee's use of another person's "online identity" in undercover online communications and the use of "untrue representations . . . concerning the activities or involvement of any third person" without that person's knowledge or consent. *See* DIOG 2, Appendix L; USOPIG § 3.2.6. However, similar to the FGUSO and the MIOG 2, neither the DIOG nor the USOPIG includes provisions that require special approval to use the identity of an organization or business in undercover online communications or in other undercover activities.

[9] The phrase "member of the news media" is defined as a person who "gathers, reports, or publishes news through the news media;" the phrase "news media" is defined as an entity that is "organized and operated for the purpose of gathering, reporting, or publishing news." DIOG § 10.1.2.2.5.

[10] As indicated by its title, the new interim policy applies to FBI employees posing as members of the news media or a documentary film crew. Our review addresses the policy only as it relates to employees posing as members of the news media.

Similar to undercover operations involving any of the "sensitive circumstances" delineated in the DIOG and USOPIG, the approval process for an undercover operation that involves an FBI employee posing as a member of the media requires the relevant FBI field office to submit an application to the Undercover Review Committee at FBIHQ for review. *Id.* § 8.2.2.1. In addition, the application can only be approved by the FBI Deputy Director, after consultation with the Deputy Attorney General. The FBI Deputy Director's approval cannot be delegated. *Id.*§ 8.2.2.1.3. The involvement of the Deputy Attorney General and the nondelegable nature of the FBI Deputy Director's authority are unique to applications for undercover operations involving FBI employees posing as members of the news media or a documentary film crew.[11]

C. Summary of Approval Requirements

The chart below summarizes the approval requirements for FBI undercover activities and operations, as well as the definition of "sensitive circumstances." Until recently, the approval requirements had remained essentially unchanged since 2007, when the Timberline bomb threat investigation was conducted. However, in November 2015, the Attorney General approved revisions to the AGG-UCO that included, among other changes, the requirement that a Department of Justice prosecutor and FBIHQ approve undercover activities that involve sensitive circumstances. None of those revisions impact this review. The more significant change for purposes of our review occurred in June 2016, when the FBI adopted interim policy, PN 0907N. This new policy prohibits FBI employees from posing as members of the news media, except as part of an undercover operation that is approved by the FBI Deputy Director after consultation with the Deputy Attorney General. The chart below reflects these changes in FBI policy.

[11] The new interim policy also includes procedures for authorizing undercover operations involving employees posing as members of the media under emergency circumstances, such as an immediate or grave threat to life or property, a threat to the national security, or the loss of a significant investigative opportunity. *See* DIOG §§ 8.2.4. to 8.2.4.2.

Type of Undercover Event	Current Review & Approval Requirements
Undercover Activity (not involving FBI employees posing as members of news media)	Supervisory Special Agent
Undercover Operation without sensitive circumstances[12]	Head of Field Office (Assistant Director in Charge or Special Agent in Charge)
Undercover Activity with Sensitive Circumstance(s)	Federal Prosecutor and FBIHQ
Undercover Operation with Sensitive Circumstance(s)	Review by Criminal Undercover Operations Review Committee and FBIHQ Approval
Undercover Operation involving FBI employees posing as members of the news media (not applicable in 2007)	Undercover Review Committee review and Deputy Director approval, after consultation with Deputy Attorney General

IV. OIG Factual Findings

A. The Timberline High School Investigation

On May 30, 2007 Timberline High School in Lacey, Washington was evacuated after a handwritten note containing a bomb threat was discovered at the school. On Sunday, June 3, 2007 an unknown subject, ultimately identified by the FBI as Timberline High School student Charles Jenkins, used a Gmail account to send an e-mail containing a bomb threat to numerous Timberline High School teachers and administrators. In the same e-mail, Jenkins threatened a "Distributed Denial of Service" (DDoS) attack on the school's computer network. The next day, school administrators evacuated the high school as a result of the threat and Jenkins launched his DDOS attack causing the school's networks to receive 24 million hits within a 24-hour period.[13]

[12] As noted above, in 2007, an undercover operation occurred when there were more than three substantive undercover communications. Under current policies, an undercover operation occurs where there are more than five substantive undercover communications.

[13] In a denial-of-service (DoS) attack, an individual attempts to prevent legitimate users from accessing information or services – such as on a website or in e-mail – by, for example, overloading the server that hosts the information or services with requests. In a DDoS attack, an individual uses multiple computers, sometimes thousands, to launch a DoS attack. *See* https://www.us-cert.gov/ncas/tips/ST04-015.

On June 5, 2007 Jenkins sent another e-mail containing a bomb threat from a different Gmail account to the high school principal and other high school staff. School administrators again evacuated Timberline High School as a result of this threat. That same day, and using a third Gmail account, Jenkins sent a fourth bomb threat to Timberline High School staff in which he taunted school officials, stating:

> Maybe you should hire Bill Gates to tell you that [this e-mail] is coming from Italy. HAHAHA Oh wait I already told you that. So stop pretending to be "tracing it" because I have already told you it's coming from Italy. That is where any trace will stop so just stop trying. Oh and this email will be behind a proxy behind the Italy server.[14]

The Lacey Police Department investigated the bomb threats by interviewing persons of interest and identifying the Internet Protocol (IP) addresses that were the source of the e-mails.[15] Investigators were able to establish that Jenkins was using two IP addresses based in Italy and one based in the Czech Republic. The investigators believed that these IP addresses were proxies and did not indicate Jenkins's true location.

On June 6, 2007 Jenkins used a fourth Gmail account to send an e-mail to Timberline High School's principal stating, "ENJOY YOUR LIFE ENDING." In another e-mail, from the same Gmail account, Jenkins sent a bomb threat to Timberline High School teachers in which he again taunted authorities' efforts to identify him. School administrators evacuated Timberline High School as a result of this threat.

That same day, officers from the Lacey Police Department contacted the Northwest Cybercrime Task Force (NWCTF), which was supervised by SSA Lucas Johnson of the FBI's Seattle Division, and requested assistance in identifying and apprehending Jenkins.[16] The FBI opened its investigation immediately and confirmed that the IP addresses being used to send the bomb threats were based in Grumello Del Monte, Italy and the Czech Republic. The FBI agents also contacted Assistant U.S. Attorney (AUSA) Chloe Watson for assistance, which she provided by working with agents to prepare the court documents in the case, as discussed below.[17]

Also on June 6, 2007 Detective Tyler Dawson of the NWCTF sent an e-mail to the FBI's Legal Attaché in Rome, Italy, requesting his assistance in working with the

---

[14] A "proxy" is a server that functions as a relay between the user and a destination website. A proxy hides the IP address of the user's machine from the website.

[15] An "IP Address" is a code made up of a unique set of numbers that identifies a computer on the Internet.

[16] Lucas Johnson is a pseudonym.

[17] Chloe Watson is a pseudonym.

Italian government to identify Jenkins.[18] In his request, Dawson included all of the potentially identifying information contained in the bomb threats made by Jenkins, including known IP addresses.

The next day, June 7, 2007, Jenkins sent another bomb threat from the e-mail address thisisfromitaly@gmail.com. School administrators again evacuated Timberline High School. Jenkins also posted three threatening messages in the comments section of the "theolympian," the online version of a Washington state newspaper, *The Olympian*.

That same day, Jenkins created a profile on the social networking site, Myspace.com, entitled "Timberlinebombinfo" and invited 33 Timberline High School students to post a link to the Myspace page. Jenkins also threatened at least one student by telling her that if she failed to post the link, her name would be associated with future bomb threats. Two of the students who received the request to link to Jenkins's Myspace.com page reported the request to local police.

On June 7, 2007 law enforcement officials from the Lacey Police Department met with Johnson, FBI Special Agent Mason Grant, Detective Dawson, other FBI officials, and Watson.[19] During the meeting, the FBI agents agreed that they would seek a court order authorizing the use of a trap and trace device for the phone of a suspect, and request the FBI's Behavioral Analysis Unit to develop a behavioral assessment of Jenkins.[20] The agents also agreed to pursue court authorization to utilize a Computer & Internet Protocol Address Verifier (CIPAV) that would allow the FBI to "identify the computer and/or user of the computer that [were] involved in" making the bomb threats against Timberline High School. According to FBI documents, "[t]he deployment of the CIPAV would require an undercover scenario to entice [Jenkins] to download the code concealing the CIPAV." The same day as the meeting of law enforcement officials, Grant began drafting the affidavit in support of a warrant seeking authority to surreptitiously install a CIPAV.

On June 8, 2007 the school district received two additional bomb threats that resulted in the evacuation of Timberline High School. That same day, Johnson contacted SSA Keith Pratt, a certified behavioral analyst with an FBI Behavioral Analysis Unit, to obtain Pratt's help developing a behavioral assessment of Jenkins.[21]

On June 10, 2007 Grant submitted a "Notification of SAC/ASAC Authority Granted for Use of Telephonic and/or Nontelephonic Consensual Monitoring Equipment in Criminal Matters" (the Notification) to ASAC Mike Higgins seeking

---

[18] Tyler Dawson is a pseudonym.

[19] Mason Grant is a pseudonym.

[20] On June 8, 2014, Watson filed under seal the application to use the pen register device. The U.S. District Court for the Western District of Washington approved the application that same day. The FBI determined that the suspect for whom they obtained the pen register was not the individual e-mailing the bomb threats.

[21] Keith Pratt is a pseudonym.

approval to use the CIPAV.[22] Among other things, the Notification required Grant to provide a synopsis of the case and to identity the individual whose communications would be consensually monitored. The Notification form listed six specific situations that required written DOJ approval prior to proceeding with the consensual monitoring, none of which applied to the bomb threat investigation.[23] The Notification did not describe how the agents intended to deploy the CIPAV. Although not required, the request did not include any mention that agents intended to pose as a journalist in order to facilitate the successful use of the CIPAV. Higgins approved Grant's request to use the CIPAV the same day it was submitted.

The Seattle Division requested a CIPAV from the FBI's Operational Technology Division/Cryptologic and Electronic Analysis Unit (OTD/CEAU) on June 11. The agents from OTD/CEAU were responsible for creating the CIPAV that would be used to locate Jenkins. Johnson and Grant also spoke with Pratt, the certified behavioral analyst who conducted the behavioral assessment of Jenkins. Pratt told us that Jenkins appeared to be very narcissistic and was feeding off of the attention he was receiving as a result of the bomb threats. Pratt stated that he recommended that the agents use that narcissism to override any suspicions that Jenkins might have about clicking on the link that would deploy the CIPAV, and suggested the link could have "some type of story or media report about him." Watson told us that she did not recall participating in a conference call with Pratt, but that Grant might have told her about the consultation with the Behavioral Analysis Unit and about Pratt's recommendation that the FBI use a media approach to deploy the CIPAV.

---

[22] Mike Higgins is a pseudonym.

[23] The six situations identified on the form as requiring Department approval were the following:

> 1. Monitoring relates to an investigation of a member of Congress, a federal judge, a member of the Executive Branch at Executive Level IV or above, or a person who has served in such capacity within the previous 2 years;
>
> 2. Monitoring relates to an investigation of the Governor, Lieutenant Governor, or Attorney General of any state or territory, or a judge or justice of the highest court of any State or Territory, & the offense investigated is one involving bribery, conflict of interest, or extortion relating to the performance of his/her official duties;
>
> 3. Consenting/nonconsenting party is a member of the diplomatic corps of a foreign country;
>
> 4. Consenting/nonconsenting party is or has been a member of the Witness Security Program & that fact is known to the agency involved or its officers;
>
> 5. Consenting/nonconsenting party is in the custody of the Bureau of Prisons or the U.S. Marshals Service; and
>
> 6. Attorney General, Deputy Attorney General, Associate Attorney General, Assistant Attorney General for the Criminal Division, or the U.S. Attorney in the district where an investigation is being conducted has requested the investigating agency to obtain prior written consent for making a consensual interception in a specific investigation.

Johnson told us that his investigative team had spent some time discussing the possible scenario proposed by Pratt. He stated that he believed that posing as a reporter could be problematic because a reporter's name could be easily verified. For this reason, the team decided to use a publisher or editor's name because it would not be readily identifiable by Jenkins. On the subject of whether the scenario would qualify as a "sensitive circumstance," Grant told us that he could not recall anyone considering that. However, Johnson told us that he consulted the FGUSO to assess this issue and concluded that the scenario was not a sensitive circumstance. Johnson said that even though the undercover employee would pose as a member of the news media, the contact would be limited to building the credibility necessary to convince Jenkins to click on the link and activate the CIPAV. Johnson also said they had no intention to publish anything or contact a third party.

Johnson told us that while he was not aware of a legally-recognized "reporter-source" privilege, he believed that a person acting as a source of information for a reporter could enter into a privileged relationship with that reporter. Asked whether he had any concerns that Jenkins would enter into or believe he was entering into a privileged relationship with the undercover agent, Johnson told us that he did not. Johnson also said it was his responsibility to research the applicable FBI policies and make the "judgment call" that the proposed undercover contact was not a sensitive circumstance.

AUSA Watson told us that she did not recall anyone telling her about a plan to impersonate a member of the news media to deploy the CIPAV. She told us that she was not involved in the operational aspect of the undercover activities and that the agents did not need her approval for how they would deploy the CIPAV. Consistent with Watson's recollection, we found no FBI documents which reflect or suggest knowledge or approval by Watson of the ruse to impersonate a journalist. Based on our investigation, we found no evidence that any other attorney at the U.S. Attorney's Office or the FBI was asked to consider whether such a tactic was appropriate.

Also on June 11, 2007 SSA Johnson briefed ASAC Higgins "on the facts of the investigation and the need to engage in limited on-line [undercover] communication with [Jenkins] for the purpose of deploying the CIPAV." According to an FBI document describing the briefing, the investigative team did not anticipate more than three substantive contacts with Jenkins and there was no expectation that there would be a face-to-face meeting between an undercover agent and Jenkins. The document did not reflect the plan to pose as a member of the media, but Johnson told us that he discussed at the briefing the fact that the undercover agent would attempt to get Jenkins to click on a link that would deploy the CIPAV by posing as a member of the media. Johnson also said that he believes he would have given Higgins his opinion, based on his review of FBI policy, that the undercover activities did not involve sensitive circumstances.

Higgins told us that it was common for Johnson to brief him on matters for cases that required approval above Johnson's level, especially for matters involving electronic eavesdropping requests, which required approval before applications

could be submitted to the court. However, Higgins told us that he had no "independent recollection" of the Timberline High School bomb threat investigation.

On June 12, 2007 the investigative team drafted a fake news article with an Associated Press (AP) byline entitled "Bomb threat at high school downplayed by local police department." Grant attached the fake news article to a draft e-mail that he proposed to send to Jenkins. The proposed e-mail contained a hyperlink to the fake news article that read: "http://seattletimes.nwsource.com/html/nationworld/2003743231_webteensex11.html" and included advertisements relating to *The Seattle Times*. He forwarded the proposed e-mail and fake news article to the special agents in OTD/CEAU who were creating the CIPAV, and to Johnson. The assigned OTD/CEAU agent responded to Grant that he would be able to use the fake article to deploy the CIPAV into Jenkins's computer.

That same day, AUSA Watson filed an application with the U.S. District Court for the Western District of Washington in Seattle that requested permission for the FBI to use the CIPAV to target "any computer accessing electronic message(s) directed to administrator(s) of myspace account 'timberlinebombinfo' and opening message(s) delivered to that account by the government, without notice to the owner/operator of that computer." Watson filed an affidavit with the application that was written and affirmed by Grant. The affidavit did not provide specific details about the contents of the FBI's message that would be sent to the unknown subject or advise the judge that agents intended to impersonate a journalist as part of their ruse.

Watson told us that while she did not write the affidavit, it was her practice to review first drafts of affidavits and communicate with agents regarding any questions relating to probable cause. In the affidavit, Grant described the facts and circumstances of the investigation and explained how the CIPAV worked. The affidavit stated that a communication containing the CIPAV would be delivered to the unknown subject's computer "through an electronic messaging program from an account controlled by the FBI" that would be "directed to the administrator(s) of the 'Timberlinebombinfo' account." The affidavit also stated that "[o]nce the CIPAV is successfully deployed, [the CIPAV] will conduct a one-time search of the activating computer and capture" the computer's IP address and other information, which would then be sent to a computer controlled by the FBI.[24] The Court approved the government's application the same day it was filed.[25]

Grant told us that he did not include in the affidavit the information about how the FBI intended to deliver the CIPAV, including the fact that they intended to

[24] At no time did the FBI file a Title III wiretap application as some news organizations had reported.

[25] The application and Sander's supporting affidavit were reviewed by AUSA Watson and an attorney from the Office of General Counsel for OTD prior to being filed with the Court. Although there was no requirement that they do so, neither document mentioned the existence of the FBI's plan to impersonate a journalist.

pose as a member of the media, because it was not needed to secure the court order. He stated further that law enforcement agencies typically do not want to expose details of undercover techniques in case they need to use the techniques in future investigations. Watson told us that information regarding how the FBI would execute a search warrant was not typically included in the affidavit supporting the search warrant because information was not needed to obtain the Court's approval. She also said that she could not recall any search warrant she had ever worked on that described how the warrant "would be affected."

That evening, at 5:38 p.m., Grant used an undercover e-mail account to send an e-mail containing a link to the fake news article containing the CIPAV to the Myspace page, "Timberlinebombinfo." Jenkins did not respond to this e-mail. The next day, at 2:51 p.m. on June 13, 2007, Grant used the same undercover e-mail account to send a second e-mail with the link to the fake news article containing the CIPAV to "timberlinebombinfo."[26] Grant's e-mail stated:

> Disappointed that I did not get a response from my "anonymous" interview request. The article was not published in today's papers, but my Staff Writer drafted an updated version and we left blanks if you would like to comment. . . .

Grant identified himself in the e-mail as "Norm Weatherill," an "AP Staff Publisher."

At 2:55 p.m. Jenkins responded, "leave me alone." Grant replied at 3:21 p.m.:

> I respect that you do not want to be bothered by the Press. Please let me explain my actions. I am not trying to find out your true identity. As a member of the Press, I would rather not know who you are as writers are not allowed to reveal their sources.
>
> The school has continually requested that the Press NOT cover this story. After the School Meeting last night, it is obvious to me that this needs coverage.
>
> Readers find this type of story fascinating. People don't understand your actions and we are left to guess what message you are trying to send. . . .

According to Grant, this message was intended to get Jenkins to click the link to the fake news story. He said the entire investigative team was present during this and the other communications with Jenkins, and consulted together about what to say before the message was sent. According to Johnson, the 3:21 p.m. reply to Jenkins drew upon the recommendation of the Behavioral Analysis Unit to play on Jenkins's ego and to build rapport. Johnson said the investigative team was trying to take

[26] The agents identified the link to the unknown subject as "news article." The hyperlink, which was not visible Glazebrook, was: "http://reporting.homeip.net:81/private/596169732/articlestuff.exe."

advantage of the desire for attention Jenkins demonstrated with his online activity, while also assuring Jenkins that he was only being asked for his side of the story, and not to disclose his identity.

Jenkins responded to Grant's message 2 minutes later by inquiring, "how can i (sic) help." Grant responded by asking Jenkins if the article and pictures were accurate. At approximately 3:30 p.m., Jenkins clicked on the link to the fake news article with the embedded CIPAV. However, because of certain settings on Jenkins's computer, the CIPAV did not deploy. At 3:47 p.m. Jenkins e-mailed Grant and asked him to engage in a live chat on Gmail. The two began their conversation at 3:48 p.m. Among other things, Jenkins asked Grant what organization he was with. Grant responded that he was with the "Associated Press," and added that "AP [articles] can be found in [the] NY Times, Seattle Times, Washington Post, US[A] Today or even local papers – such as the Olympian."

At 5:07 p.m., Jenkins contacted Grant through live chat on Gmail asking if he had "any news yet." At 5:50 p.m., Grant responded via e-mail that "they are crunching the article now," and sent him the link to some photographs related to the article that were embedded with a CIPAV. Jenkins clicked on the link to the photographs and e-mailed Grant at 5:53 p.m. stating, "dont (sic) care about which pics you use." This time, when Jenkins clicked on the link to the photographs, the CIPAV deployed properly and the FBI obtained his true IP address.

Using the true IP address, the FBI was able to locate and then identify Jenkins, a 10th grade student at Timberline High School, as the individual who had been e-mailing the bomb threats to the school. At approximately 2:00 a.m. on June 14, 2007, the Lacey Police Department executed an arrest warrant on Jenkins and arrested him at his parents' house. Upon arrest, Jenkins immediately confessed to sending multiple bomb threats to the Timberline School District. Two additional draft bomb threats were found on his computer at the time of his arrest.

That same day, Johnson drafted and submitted an "FBI Urgent Report" addressed to then-FBI Director Robert Mueller and other FBI divisions. The report, entitled "Other Matter Warranting the Immediate Attention of FBIHQ Executives," included a synopsis of the FBI's investigation of Jenkins and specifically stated that the "CIPAV was deployed through an undercover electronic message session between Seattle undercover employees and Jenkins." The report did not describe the tactic of impersonating a journalist.

The State of Washington prosecuted Jenkins after the U.S. Attorney's Office declined prosecution because Jenkins was a juvenile. On July 16, 2007 Jenkins pleaded guilty to three counts of identity theft (Class C Felony), two counts of Threat to Bomb or Injure Property (Class B Felony), and one count of Felony Harassment (Class B Felony). He was sentenced that same day to 90 days of juvenile detention, 2 years of supervised release, 2 years of mental health counseling, and 2 years of probation with restrictions on internet and computer usage. Jenkins was also expelled from the Timberline School District.

B. Media Response to the FBI's Investigation of Jenkins

The FBI did not publicize the assistance its agents provided to the Lacey Police Department during the investigation of Jenkins's bomb threats. However, on July 18, 2007, 2 days after Jenkins pleaded guilty, the online technology news website, Wired.Com, released an article entitled "FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats." The article explained how the CIPAV worked and how the FBI used it to locate Jenkins. The article did not reference the fact that the FBI had impersonated a member of the news media.

Seven years later, on October 27, 2014, *The Seattle Times* released an article based upon e-mails obtained by the Electronic Frontier Foundation (EFF) through a Freedom of Information Act request. The e-mails obtained by the EFF disclosed the fact that the FBI posed as a member of the press when it contacted and then identified Jenkins as the author of the bomb threats.

On October 30, 2014, the AP sent a letter to then-Attorney General Eric Holder protesting the FBI's use of a fake AP news story in connection with its investigation of the bomb threats. In its letter, the AP's General Counsel, Karen Kaiser, complained that the AP learned, "more than seven years after the incident occurred," that "the FBI both misappropriated the trusted name of the Associated Press and created a situation where our credibility could have been undermined on a large scale." Kaiser added, "It is improper and inconsistent with a free press for government personnel to masquerade as The Associated Press or any other news organization." She said the FBI's actions "undermined the most fundamental component of a free press – its independence." In addition, several newspapers wrote articles questioning the tactics the FBI used to identify and arrest Jenkins.

In response to these news articles in 2014, FBI employees in the Cyber Division worked with attorneys in the FBI's Office of General Counsel (OGC), Cyber Law Unit, to draft a "Situation Action Background" (SAB) report that described the facts and circumstances surrounding the FBI's investigation and identification of Jenkins. The OGC attorney primarily responsible for drafting the SAB told us that the document was created to inform FBI executive leadership about the FBI's actions to identify and apprehend Jenkins. The SAB also included OGC's analysis of the applicable Department and FBI policies in effect at the time of the investigation, as well as OGC's analysis of the applicable Department and FBI policies currently in effect.

One week later, on November 6, 2014, FBI Director James Comey wrote a letter to the editor of *The New York Times* defending the FBI's investigation. Consistent with OGC's analysis in the SAB, Comey stated that the "technique [the FBI used to identify and apprehend Jenkins] was proper and appropriate under Justice Department and F.B.I. guidelines at the time" and that "[t]oday, the use of such an unusual technique would probably require higher level approvals than in 2007, but it would still be lawful and, in a rare case, appropriate."

The same day, the Reporters Committee for Freedom of the Press (RCFP), on behalf of 25 other news organizations, wrote a letter to Holder and Comey voicing

its objection to the FBI impersonating journalists. In the letter, the RCFP complained, "[t]he utilization of news media as a cover for delivery of electronic surveillance software is unacceptable. This practice endangers the media's credibility and creates the appearance that it is not independent of the government. It undermines media organizations' ability to independently report on law enforcement. It lends itself to the appearance that media organizations are compelled to speak on behalf of the government." The RCFP urged "the Attorney General and FBI to clarify that impersonation of the media is unacceptable. . . ." The letter further asserted that the operation "should have been subjected to heightened review and scrutiny, disclosed to OGC and the magistrate judge, and evaluated for what it was – an investigation that involved significant First Amendment concerns."

V. OIG Analysis, Conclusions, and Recommendation

In this section, we assess whether, under Department and FBI policies in effect at the time of the 2007 investigation, appropriate approval was obtained for the undercover activities the FBI conducted to locate Jenkins. We concluded that Department and FBI policies in effect in 2007 did not prohibit agents from impersonating journalists or from posing as a member of a news organization, nor was there any requirement that agents seek special approval to engage in such practice. The only policies in effect at the time that might have required elevated consideration regarding the FBI's plans turned on whether the undercover activity involved a "sensitive circumstance." We concluded, given the lack of clarity in the policy language, that making a determination about the required approvals was a challenging one and that the judgments made by the agents were not unreasonable. However, we also concluded that after the plan was launched and Jenkins indicated to the undercover agent that he wanted to be left alone, the investigative team should have considered whether a message to Jenkins that included an implied offer of confidentiality would create a "sensitive circumstance" requiring a higher level of approval before the message was sent.

We also assess in this section whether those same undercover activities conducted in 2007 would require a higher level of approval under Department and FBI policies currently in effect. We concluded that an interim policy change adopted by the FBI on June 8, 2016 would prohibit the 2007 undercover activities unless they were part of an undercover operation reviewed by the Undercover Review Committee at FBIHQ and authorized by the FBI Deputy Director, after consultation with the Deputy Attorney General.

A. Policies in effect in 2007

In 2007, FBI policies did not prohibit the practice of agents impersonating journalists, nor was there any requirement that agents seek special approval to engage in such practice. Instead, agents were left to consult with the more general undercover policies which implicitly prohibited impersonation of a member of the news media only if there was a "significant risk" that a third party would enter into a confidential relationship with the undercover FBI employee.

There essentially were three questions that had to be answered in 2007 regarding the proposed online undercover activity to determine what level of approval was required before the activity was initiated. First, was the proposed activity in fact "undercover activity"? Second, how many "substantive undercover contacts" were expected to occur between the undercover employee and the subject of the investigation? Third, did the undercover activity involve any "sensitive circumstances"? As summarized in the following table, the answers to these questions established the level of approval required:

Type of Undercover Event	**Review and Approval Requirements**
Undercover Activity with 3 or fewer contacts	Supervisory Special Agent
Undercover Operation (*i.e.*, undercover activity more than 3 contacts)	Head of Field Office
Undercover Activity with Sensitive Circumstance(s)	Review by Criminal Undercover Operations Review Committee and FBIHQ Approval
Undercover Operation with Sensitive Circumstance(s)	Review by Criminal Undercover Operations Review Committee and FBIHQ approval

The FBI's plan to locate Jenkins clearly was undercover activity, that is, "any investigative activity involving the use of an assumed name or cover-identity by an employee of the FBI . . . ." The plan called for an agent to pose as an editor working for the AP and contact Jenkins by e-mail for purpose of surreptitiously installing a computer program – the CIPAV – that would reveal the location of the computer Jenkins was using. This plan constituted "undercover activity" under FBI policy.

The agents involved in the development of the plan anticipated that it would require three or fewer substantive contacts with Jenkins to install the CIPAV. We do not believe this was an unreasonable expectation. The bomb threats alone were brazen, and in the e-mails communicating the threats, Jenkins was arrogant and dismissive of the authorities' efforts to locate and identify him. Further, Jenkins created a public profile on Myspace.com and invited 33 of his classmates to post links to the page, even threatening one student that if she failed to do so, he would associate her with the next bomb threat. We believe that in view of Jenkins's display of conceit and his contempt for the efforts to locate him, it was not unreasonable to expect that he would respond quickly to an inquiry from the media about the bomb threats, and that it would therefore probably not take more than three online "contacts" to deploy the CIPAV.

We believe that the third question that had to be addressed – whether the undercover activity involved a "sensitive circumstance" – was a difficult one.

However, we ultimately concluded that SSA Johnson's judgment that the plan did not involve a sensitive circumstance was not unreasonable.

As described in this report, the plan to get the CIPAV installed on Jenkins's computer would implicate the category of sensitive circumstances referenced in the FGUSO involving "privileged relationships" if there was:

> a reasonable expectation that the undercover operation would involve . . . [a] significant risk that a third party [would] enter into a professional or confidential relationship with a person participating in an undercover operation who [was] acting as . . . [a] member of the news media.

According to FBI policy guidance, this sensitive circumstance extended to scenarios where a relationship with a subject was established that the subject believed was privileged. The plan in the Jenkins investigation was for the undercover agent to represent himself to Jenkins as a journalist working for the AP in order to entice Jenkins to click on a link to a fake news article. The idea to use a "press angle" originated with the FBI analyst who conducted a behavioral assessment of Jenkins. The analyst told the agents and the AUSA that this approach would "play on [Jenkins's] ego." Also, SSA Johnson told us that he consulted the relevant policy manual and concluded that the plan did not present a sensitive circumstance because, even though the undercover agent would pose as a member of the media, the communication would be limited to establishing the credibility needed to get Jenkins to click the link to the fake news article. There was no intention or expectation that they would be engaging in protracted discussions with Jenkins, or any need or attempt to enter into a confidential or privileged relationship with him.

According to witnesses, the press angle they decided to use in the contact with Jenkins was intended to take advantage of his ego and to establish the undercover agent's credibility. The plan did not entail an attempt to develop a confidential relationship with Jenkins. Considering this, and the agents' belief that it would take three or fewer contacts with Jenkins to get the CIPAV deployed, we found that it was not unreasonable for SSA Johnson to conclude at the outset of the undercover activity that there was not a "significant risk" that Jenkins would enter into a confidential relationship with a member of the media, and that therefore the undercover activity did not include a sensitive circumstance.

Having concluded that the judgments the agents made about the anticipated number of online contacts between the FBI and Jenkins and whether any "sensitive circumstances" existed were not unreasonable, we found – as indicated in the table above – that it was permissible for SSA Johnson to approve the online undercover activity.

However, the FBI knew little about Jenkins and could not predict with any reasonable degree of confidence how he would react to the undercover contact. Indeed, Jenkins did not respond to the agent's first communication, and when he did reply to the second, it was to tell the agent to "leave me alone." It was only after the agent told Jenkins that he was not trying to determine his true identity, and that he "would rather not know who you are as writers are not allowed to

reveal their sources," that Jenkins expressed a willingness to help.[27] We highlight this – that is, how the plan actually unfolded – not because it proves the agents' advance assessment of the plan was wrong, but to demonstrate the plan's inherent unpredictability and of the potential need to reassess the necessary approval requirements.

We considered whether the level of approval required for the undercover activity changed after the plan was launched based upon either the number of substantive contacts the undercover agent was having with Jenkins or the content of the communications. With respect to the number of substantive contacts, and considering the guidance the FBI provided agents for counting online contacts, we did not find a basis to question whether the level of approval required should have been reevaluated as the plan unfolded. However, with respect to the content of the communications, we found that the message to Jenkins assuring him that his identity would not be revealed had the potential to cause Jenkins to believe he was entering into a confidential relationship with the undercover agent. At this point, we believe the investigative team should have re-evaluated the situation and consulted with their SAC before sending the additional message.

As noted above and described in Section III, Jenkins did not respond to the undercover agent's first e-mail message, and in response to the agent's second message replied, "leave me alone." At that point, the investigative team discussed what to say in response. The message that was sent to Jenkins included assurances that they were not trying to identify him – "[a]s a member of the Press, I would rather not know who you are as writers are not allowed to reveal their sources." According to SSA Johnson, the message was intended to play on Jenkins's ego and build rapport, and to take advantage of his desire for attention while assuring him that he was not being asked to disclose his identity. As described earlier, Jenkins responded to this message 2 minutes after it was sent with his offer to help.

We believe the assurance made to Jenkins – particularly the statement that "writers are not allowed to reveal their sources" – was an implied promise of confidentiality. As such, it created a risk that Jenkins would believe he was entering into a confidential relationship with an undercover agent acting as a member of the news media. The investigative team did not adequately consider whether that risk was "significant" and therefore whether a "sensitive circumstance" existed under the FGUSO's "privileged relationships" provision. Had the team concluded that the message prepared for Jenkins created a significant risk, FBI policy accommodated operational needs by authorizing the SAC, or designated ASAC, to grant interim authority for online undercover contacts involving a sensitive circumstance. Thus, although FBIHQ and CUORC ultimately would have had to

[27] This implicit promise of confidentiality, made by an undercover agent posing as a journalist, was one of the objections the media raised about this practice out of a concern that it could make potential sources leery of trusting journalists for fear they might actually be police or agents posing as journalists.

approve the activity, there was a mechanism by which the investigative team could have continued its engagement with Jenkins with little delay.

After reviewing a draft of this report, the FBI told us that it concurred with our conclusion that the "privileged relationships" provision applies to scenarios involving subjects of investigations as well as third parties. However, the FBI provided the OIG with comments that indicated to us that the scope and application of the FGUSO's "privileged relationships" provision is potentially susceptible to multiple interpretations. This was also evident in interviews we conducted during the course of this review. In light of the fact the current FBI policy – the USOPIG – fully incorporates the FGUSO provision, including the associated commentary, we believe it is important that the FBI provide clear guidance to employees about the circumstances to which the provision is meant to apply. Therefore, we recommend the FBI consider whether revisions to the USOPIG are required to ensure that undercover activity involving a significant risk that a subject believes he has entered into a privileged relationship with an undercover agent, is treated as a "sensitive circumstance."[28]

B. Policies in effect today

We also assessed whether those same undercover activities conducted in 2007 would require a higher level of approval if conducted under Department and FBI polices currently in effect today. As described in Section III.B. of this report, on June 8, 2016, the FBI adopted an interim policy – PN 0907N – that prohibits FBI employees from engaging in undercover activities that involve posing as members of the news media, unless those activities are authorized as part of an undercover operation by the Deputy Director, after consultation with the Deputy Attorney General. The number of substantive contacts by an undercover employee with the individual under investigation is no longer a relevant factor under this policy as it applies to employees posing as members of the news media.

The AP is "organized and operated for the purpose of gathering, reporting, or publishing news" and clearly falls within the definition of "news media" under FBI policy. It is equally clear under FBI policy currently in effect, that any undercover activity that would involve an employee posing as a member of the AP would have to be approved as an undercover operation at FBIHQ. The head of the FBI field office proposing the activity would first have to approve the application for the undercover operation to be submitted for approval to FBIHQ; the Undercover Review Committee at FBIHQ would then be required to review the application; and the Deputy Director, after consulting with the Deputy Attorney General, would be responsible for approving the application.

[28] As discussed earlier, the FBI's June 2016 interim policy applies to employees posing as members of the news media or as a documentary film crew. The types of privileged relationships covered by the USOPIG include those with an attorney, physician, or clergyman, as well as with a member of the news media. Therefore, the June 2016 interim policy does not obviate the need to provide clear guidance on the scope and application of the discussed USOPIG provision.

We believe the June 2016 policy on FBI employees posing as members of the news media is a significant and important improvement to FBI policies that existed in 2007 during the Timberline investigation, as well as to those policies that would have governed similar undercover activities prior to June 8, 2016. The Department and the FBI have previously implemented a number of policies addressing the use of law enforcement tools to obtain information from or about members of the news media in criminal and civil investigations. Since 1980, federal regulations have required the Attorney General to authorize subpoenas issued to or for the telephone records of any member of the news media. *See* 28 C.F.R. § 50.10(e). Those regulations, which also governed the interrogation, indictment, or arrest of members of the news media, were re-examined by the Attorney General in 2013 at the direction of the President. The re-examination followed public criticism of the Department's actions in issuing subpoenas for 2 months of records related to 20 telephone lines used by AP staff as part of a criminal investigation into the unauthorized disclosure of classified information.[29]* Following the Attorney General's review, the Department amended these regulations in February 2014 in order to "provide protection to members of the news media from certain law enforcement tools, whether criminal or civil, that might unreasonably impair newsgathering activities," *see* 28 C.F.R. § 50.10(a), and to "ensure more robust oversight by senior Department officials; centralize the internal review and evaluation process; [and] set out specific standards for the use and handling of information obtained from, or records of, members of the news media . . . ." Policy Regarding Obtaining Information From, or Records of, Members of the News Media; and Regarding Questioning, Arresting, or Charging Members of the News Media, 79 F.R. § 10989-01 (2014).

While impersonating a member of the media potentially implicates different First Amendment concerns than using tools such as subpoenas and court orders to obtain information directly from news organizations, the activity also has the potential to "impair newsgathering activities" by, for example, making it less likely that sources will share information with journalists, fearing they might actually be FBI agents posing as journalists. The FBI's June 2016 interim policy on undercover activities that involve agents posing as members of the news media is an important and appropriate addition to the policies the Department previously implemented to regulate certain law enforcement activities that affect members of the news media.

Finally, as we described in Section III of this report, we learned during the course of this review that while FBIHQ approval is required to use a third person's "online identity" in undercover online communications or to make "untrue representations . . . concerning the activities or involvement of any third person" without that person's knowledge or consent, special approval was not required to use the identity of an organization or business in undercover online communications

---

[29] *See, e.g.*, https://www.washingtonpost.com/world/national-security/under-sweeping-subpoenas-justice-department-obtained-ap-phone-records-in-leak-investigation/2013/05/13/11d1bb82-bc11-11e2-89c9-3be8095fe767_story.html (accessed August 3, 2016).

* An earlier version of this report incorrectly stated that the subpoenas were issued to the AP.

or in other undercover activities. The new interim policy changes that policy as it relates to news organizations, but does not address this issue with regard to non-news organizations or businesses. We think the Department should consider the appropriate level of review necessary before agents in a criminal investigation are allowed to use the name of a third-party organization or business without its knowledge or consent, in light of the potential impact that use might have on the third party's reputation.[30]

C. Conclusion and Recommendations

We found that Department and FBI policies in effect in 2007 did not prohibit agents from impersonating journalists or from posing as a member of a news organization, nor was there any requirement that agents seek special approval to engage in such undercover activities. The only policies in effect at the time that might have required elevated consideration regarding the FBI's plans turned on whether the undercover activity involved a "sensitive circumstance." We concluded, given the lack of clarity in the policy language, that making a determination whether a situation was a "sensitive circumstance" was a challenging one and that the judgments made by the agents were not unreasonable given the lack of clarity. However, we also concluded that after the plan was launched, the investigative team should have considered whether a message to Jenkins that included an implied offer of confidentiality would create a "sensitive circumstance" requiring a higher level of approval before the message was sent.

We also found that prior to the adoption of the new interim policy in June 2016, FBI policy would not have prohibited FBI employees from engaging in the undercover activities agents conducted during the 2007 Timberline investigation. The new interim policy, however, clearly prohibits FBI employees from engaging in an undercover activity in which they represent, pose, or claim to be members of the news media, unless the activity is authorized as part of an undercover operation. In order for such an operation to be authorized, the undercover application must first be approved by the head of the FBI field office submitting the application to FBIHQ, reviewed by the Undercover Review Committee at FBIHQ, and approved by the Deputy Director, after consultation with the Deputy Attorney General.

We believe the new interim policy on undercover activities that involve FBI employees posing as members of the news media is a significant improvement to FBI policies that existed in 2007 during the Timberline investigation, as well as to those policies that would have governed similar undercover activities prior to June

[30] After reviewing a draft of this report, the FBI provided comments explaining that the heightened level of review and approval required for FBI employees to pose as members of the news media was introduced because such activity potentially could "impair newsgathering activities" under the First Amendment, but that such constitutional considerations do not apply to businesses and other third parties. Our recommendation, however, does not rely on equating the reputational interests of some third party organizations and businesses with the constitutional interests of others. We believe that reputational interests, and the potential impact FBI investigations can have on those interests, are themselves sufficiently important to merit some level of review before FBI employees use the names of third party organizations or businesses without their knowledge or consent.

2016. The new interim policy also is an important extension of policies the Department has previously implemented to regulate certain law enforcement activities that affect members of the news media, such as obtaining information from or about members of the news media in criminal and civil investigations. The FBI should move expeditiously to update its undercover policy guide to incorporate this new interim policy, and widely inform and educate FBI employees about the policy's existence and application.

Based upon our review, we make three recommendations to help ensure that FBI policies governing certain undercover activities and operations are well known, clear, and understood. The FBI concurs with the recommendations.

Recommendation 1: The FBI should move expeditiously to update its undercover policy guide to incorporate the June 2016 interim policy on undercover activities in which FBI employees represent, pose, or claim to be members of the news media or a documentary film crew; and widely inform and educate FBI employees about the policy's existence and application.

Recommendation 2: The FBI should consider the appropriate level of review required before FBI employees in a criminal investigation use the name of third-party organizations or businesses without their knowledge or consent.

Recommendation 3: The FBI should consider whether revisions to the USOPIG are required to ensure that undercover activity involving a significant risk that a subject believes he has entered into a privileged relationship with an undercover agent, is treated as a "sensitive circumstance."

The Department of Justice Office of the Inspector General (DOJ OIG) is a statutorily created independent entity whose mission is to detect and deter waste, fraud, abuse, and misconduct in the Department of Justice, and to promote economy and efficiency in the Department's operations. Information may be reported to the DOJ OIG's hotline at www.justice.gov/oig/hotline or (800) 869-4499.

Office of the Inspector General
U.S. Department of Justice
www.justice.gov/oig

EXHIBIT K

COMEY, JAMES B. (DO) (FBI)

From: COMEY, JAMES B. (DO) (FBI)
Sent: Monday, November 03, 2014 2:38 PM
To: KORTAN, MICHAEL P. (OPA) (FBI); ROSENBERG, CHUCK P. (DO) (FBI)
Cc: GIULIANO, MARK F (DO) (FBI)
Subject: DRAFT letter to NY Times UNCLASSIFIED

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

TRANSITORY RECORD

Editor:

[redacted] b5 -1

[redacted] b5 -1

[redacted] b5 -1

[redacted] b5 -1

[redacted] b5 -1

b5 -1

==========

Classification: UNCLASSIFIED

COMEY, JAMES B. (DO) (FBI)

From:	COMEY, JAMES B. (DO) (FBI)
Sent:	Monday, November 03, 2014 6:16 PM
To:	COMEY, JAMES B. (DO) (FBI); KORTAN, MICHAEL P. (OPA) (FBI); ROSENBERG, CHUCK P. (DO) (FBI)
Cc:	GIULIANO, MARK F (DO) (FBI)
Subject:	RE: DRAFT letter to NY Times UNCLASSIFIED

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

TRANSITORY RECORD

And after reading the Cyber write up I would add the language below in red.

From: COMEY, JAMES B. (DO) (FBI)
Sent: Monday, November 03, 2014 2:38 PM
To: KORTAN, MICHAEL P. (OPA) (FBI); ROSENBERG, CHUCK P. (DO) (FBI)
Cc: GIULIANO, MARK F (DO) (FBI)
Subject: DRAFT letter to NY Times --- UNCLASSIFIED

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

TRANSITORY RECORD

Editor:

	b5 -1
	b5 -1

[redacted] b5 -1

[redacted] b5 -1

[redacted] b5 -1

[redacted] b5 -1

==========

Classification: UNCLASSIFIED

==========

Classification: UNCLASSIFIED

Rosenberg, Chuck P.

From: Rosenberg, Chuck P.
Sent: Tuesday, November 11, 2014 2:37 PM
To: James B. Comey
Subject: Re: INQUIRY FROM USA TODAY EDITORIAL PAGE

That makes sense. USA Today gives space to the other side, which I admire. [redacted] b5 -1

[redacted]

----- Original Message -----
From: James B. Comey
To: Rosenberg, Chuck P.
Sent: Tue Nov 11 14:31:42 2014
Subject: Re: INQUIRY FROM USA TODAY EDITORIAL PAGE

[redacted]

[redacted] b5 -1

[redacted]

> On Nov 11, 2014, at 2:03 PM, "Rosenberg, Chuck P." [redacted] wrote: b6 -1 b7C -1
>
> [redacted] What do you think? b5 -1
>
> ----- Original Message -----
> From: Rosenberg, Chuck P.
> To: Kortan, Michael P.
> Sent: Tue Nov 11 13:56:17 2014
> Subject: Re: INQUIRY FROM USA TODAY EDITORIAL PAGE
>
> [redacted] What do you recommend? [redacted] b5 -1
>
> ----- Original Message -----
> From: Kortan, Michael P.
> To: Rosenberg, Chuck P.
> Sent: Tue Nov 11 12:30:47 2014
> Subject: FW: INQUIRY FROM USA TODAY EDITORIAL PAGE
>
> Chuck: [redacted] .....Thanks. M > b5 -1

_____ > From: Torry, Saundra [redacted] > Sent: Tuesday, November 11, 2014 12:16 PM > To: Kortan, Michael P.
b6 -4
b7C -4
> Subject: INQUIRY FROM USA TODAY EDITORIAL PAGE
>
> Mr. Kortan - I write for the editorial page here and I am working on editorial scheduled for Thursday's paper on the 2007 investigation in which an agent sent a bogus news story to a suspect, that appeared to come from the Associated Press. Of course I've read Mr. Comey's response in the letter to the NY Times.
>
> We are going to be critical of the use of the AP's name because of the damage it could do to the credibility of journalists. If people wonder when they get a call or email from a journalist whether it is really a law enforcement agent contacting them, it will make it far more difficult to get honest answers and to get honest information for the public. This is not about making our job harder, but about making it more difficult for the public to get honest news reports.
>
> We are hoping that Director Comey would be interested in writing a 340-word response to our editorial, which will appear next to our editorial at the top of our page.
> If you are not familiar with our format, we run a debate every day to give the public both sides of the issues we tackle. It would give the FBI an opportunity to get its positon on this issue out to a wider audience.
>
> We'd like to know today if you are interested (or not interested) and get the piece tomorrow by 5 p.m.
>
> Please let me know soon. Also happy to answer any questions.
>
> Best,
> Saundra Torry
> [redacted]

b6 -4
b7C -4

EXHIBIT L

[redacted] b6 -1 b7C -1

From: [redacted]
Sent: Tuesday, August 16, 2016 4:48 PM
To: GAVIN, MICHAEL T. (CID) (FBI)
Subject: FW: OIG-DOJ Review of the FBI's Use of a Fictitious Associated Press News Article in a Criminal Investigation --- UNCLASSIFIED
Attachments: [redacted] b5 -1

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

FYI

From: [redacted]
Sent: Tuesday, August 16, 2016 4:35 PM
To: [redacted] HUGHES, ROBERT (CID) (FBI); [redacted] b6 -1 b7C -1
Cc: [redacted]
Subject: FW: OIG-DOJ Review of the FBI's Use of a Fictitious Associated Press News Article in a Criminal Investigation --- UNCLASSIFIED

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

[redacted] I'm currently on a sabbatical, but I've cc'd the new CID Spec Assistant [redacted] and the SCs that may need to review this, also the OTD UCs [redacted] just in case. b6 -1 b7C -1

Thank you!

[redacted]

From: [redacted]
Sent: Tuesday, August 16, 2016 9:14 AM
To: [redacted] b6 -1 b7C -1 b7E -4
Subject: FW: OIG-DOJ Review of the FBI's Use of a Fictitious Associated Press News Article in a Criminal Investigation --- UNCLASSIFIED

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

Good Morning,

Please be advised that there was an error in the deadline date. I have noted the actual deadline date below.

I apologize for the inconvenience.

Kind regards,

b6 -1
b7C -1

[redacted]

From: [redacted]
Sent: Thursday, August 11, 2016 9:51 AM
To: [redacted]
Cc: [redacted]
Subject: OIG-DOJ Review of the FBI's Use of a Fictitious Associated Press News Article in a Criminal Investigation --- UNCLASSIFIED

b6 -1
b7C -1
b7E -4

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

Good Morning,

The OIG delivered the Working Draft for the **Review of the FBI's Use of a Fictitious Associated Press News Article in a Criminal Investigation**. A copy of the draft report is attached for your review. The FBI must now review the draft for [redacted] Also, review the draft for [redacted] wherein a section or portion of the draft, in your opinion, [redacted]

b5 -1

[redacted]

b5 -1

Please use the [redacted]

b5 -1

[redacted] by **COB Thursday, August 19th**.

[redacted]

b5 -1

If you have any questions or concerns please contact MAPA [redacted] at [redacted] or UC [redacted] at [redacted] Thank you in advance for your time and attention to this matter.

b6 -1
b7C -1

[redacted]

b6 -1
b7C -1

Management & Program Analyst

Inspection Divsion

External Audit

Office: [redacted]

b6 -1
b7C -1

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

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

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

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

GAVIN, MICHAEL T. (CID) (FBI)

b6 -1
b7C -1

From: GAVIN, MICHAEL T. (CID) (FBI)
Sent: Wednesday, November 12, 2014 6:03 PM
To: DELANEY, TIMOTHY J (CID)(FBI)
Cc: GAVIN, MICHAEL T. (CID) (FBI); [redacted]
Subject: UCOs and the news media UNCLASSIFIED

Classification: UNCLASSIFIED
~~DELIBERATIVE PROCESS PRIVILEGED DOCUMENT~~
==========

Mr. Delaney,

I am writing to follow up on our conversation regarding UCOs and the news media.

Please let me know if you have any questions,

Michael T. Gavin

b6 -1
b7C -1
b7E -3

Chief [redacted]

[redacted]

Synopsis:

b5 -1

[redacted]

Discussion:

Undercover operations which involve a sensitive circumstance, as defined by the AGG UCOs, must be reviewed by the Undercover Review Committee and authorized (minimally) by the Assistant Director. These are the sensitive circumstances involving the news media, none of which applies to the scenario in which the UCE represents to the target of the investigation that he/she is associated with the news media:

AGG UCO §IV.C.(2) Sensitive Circumstances

(c) an investigation of possible criminal conduct by any foreign official or government, religious organization, political organization, or the news media;

(j) A significant risk that a third party will enter into a professional or confidential relationship with a person participating in an undercover operation who is acting as an attorney, physician, clergyman, or

member of the news media;

(k) A request to an attorney, physician, member of the clergy, or other person for information that would ordinarily be privileged or to a member of the news media concerning an individual with whom the news person is known to have a professional or confidential relationship.

Recommendation:

b5 -1

==========

Classification: UNCLASSIFIED

[redacted]

From: [redacted]
Sent: Thursday, January 29, 2015 5:53 PM
To: GAVIN, MICHAEL T. (CID) (FBI)
Cc: [redacted]
Subject: [redacted] UNCLASSIFIED~~//FOUO~~
Attachments: [redacted]

b5 -1
b6 -1
b7C -1

Classification: UNCLASSIFIED~~//FOUO~~

TRANSITORY RECORD

Sir,

Here's my first cut at the [redacted] you requested last night.

Please advise and I'll make any/all corrections.

[redacted]

[redacted]

b5 -1
b6 -1
b7C -1

Classification: UNCLASSIFIED~~//FOUO~~

[redacted]

From: [redacted]
Sent: Monday, February 02, 2015 2:30 PM
To: GAVIN, MICHAEL T. (CID) (FBI)
Subject: [redacted] UNCLASSIFIED//~~LES~~
Attachments: [redacted]

b5 -1
b6 -1
b7C -1

Classification: UNCLASSIFIED//~~LES~~

==========

TRANSITORY RECORD

Sir,

Here's version 3, based upon our Friday conversation.

Please advise!

[redacted]

[redacted]

b5 -1
b6 -1
b7C -1

==========

Classification: UNCLASSIFIED//~~LES~~

EXHIBIT M

James B. Comey

From: James B. Comey
Sent: Wednesday, August 10, 2016 9:05 PM
To: Rybicki, James E. (DO) (FBI)
Subject: RE: E2014019 Office of the Inspector General's draft report [redacted]

b5 per DoJ/OIG and -1 per FBI

[redacted]

b5 -1

-------- Original message --------
From: "Rybicki, James E. (DO) (FBI)" [redacted]
Date: 08/10/2016 2:23 PM (GMT-08:00)
To: "James B. Comey" [redacted]
Subject: FW: E2014019 Office of the Inspector General's draft report [redacted]

b5 per DoJ/OIG and -1 per FBI
b6 -1
b7C -1

[redacted]

b5 per DoJ/OIG and -1 per FBI
b6 -3
b7C -3

Draft OIG report-

[redacted]

b5 per DoJ/OIG and -1 per FBI

[redacted]

b5 per DoJ/OIG and -1 per FBI
b6 -3
b7C -3

[redacted]

From: [redacted] (OIG) [mailto[redacted]@usdoj.gov] **On Behalf Of** OIG, Oversight&Review (OIG)
Sent: Wednesday, August 10, 2016 4:59 PM
To: Rybicki, James E. (DO) (FBI); [redacted] Baker, James A. (OGC) (FBI); [redacted]
McNamara, Nancy (INSD) (FBI); [redacted]
Subject: E2014019 Office of the Inspector General's draft report [redacted]

[redacted]

Attached is a copy of the Office of the Inspector General's draft report [redacted]

[redacted]

b5 per DoJ/OIG and -1 per FBI
b6 per DoJ/OIG and -1 per FBI
b7C per DoJ/OIG and -1 per FBI

If you have any questions about this draft report, please contact me.

Michael E. Horowitz
Inspector General

Rybicki, James E. (DO) (FBI)

From:	Rybicki, James E. (DO) (FBI)
Sent:	Wednesday, September 14, 2016 6:12 PM
To:	James B. Comey; Mccabe, Andrew G. (DO) (FBI); Bowdich, David L. (DO) (FBI)
Subject:	FW: Department of Justice Office of the Inspector General Report of A Review of the FBI's Impersonation of a Journalist in a Criminal Investigation
Attachments:	E2014019 FBI AP Impersonation OIG Report OR-16-07 FBI.pdf

b6 per DoJ/OIG and -1 per FBI
b7C per DoJ/OIG and -1 per FBI

From: [redacted] (OIG) [mailto:[redacted]@usdoj.gov] **On Behalf Of** OIG, Oversight&Review (OIG)
Sent: Wednesday, September 14, 2016 6:12 PM
To: Rybicki, James E. (DO) (FBI); [redacted] Baker, James A. (OGC) (FBI); [redacted]
McNamara, Nancy (INSD) (FBI); [redacted]
Subject: Department of Justice Office of the Inspector General Report of A Review of the FBI's Impersonation of a Journalist in a Criminal Investigation

The Office of the Inspector General has completed its report entitled *A Review of the FBI's Impersonation of a Journalist in a Criminal Investigation.* Attached is a copy of the final report.

Please contact my Chief of Staff Jay Lerner if you have any questions about this report.

Michael E. Horowitz
Inspector General

U.S. Department of Justice

Office of the Inspector General

September 14, 2016

MEMORANDUM FOR JAMES B. COMEY
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

FROM: MICHAEL HOROWITZ
INSPECTOR GENERAL

b5 per DoJ/OIG and -1 per FBI

SUBJECT: OIG Report [redacted]

The Office of the Inspector General (OIG) has completed its report entitled *A Review of the FBI's Impersonation of a Journalist in a Criminal Investigation.* [redacted]

b5 per DoJ/OIG and -1 per FBI

Attached is a copy of the final report. We are also providing the report today to the Department. We intend to release the report to Congress and the public on September 14, 2016.

Please contact me or my Chief of Staff Jay Lerner if you have any questions about this report.
Attachment

cc: James Rybicki
Chief of Staff to the Director

James A. Baker
General Counsel

Nancy McNamara
Assistant Director
Inspection Division

EXHIBIT N

FBI_COMMUNICATIONS_MBX

From: FBI_COMMUNICATIONS_MBX
Sent: Monday, June 13, 2016 4:13 PM
To: FBI_ALL
Subject: Employee E Brief: Director Briefs Reporters on Orlando Investigation
UNCLASSIFIED

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

TRANSITORY RECORD

Employee E-BRIEF
The Office of EMPLOYEE COM
A WEEKLY UPDATE FOR ALL BUREAU EMPLOYEES

June 13, 2016

NEWS

- Director Briefs Reporters on Orlando Investigation 6/13/2016
- 15 Minutes with FBI [redacted] 6/13/2016 b6 -1 b7C -1
- More News and Information and Photo of the Day

EVENTS AND TRAINING

- Equal Employment Opportunity [redacted] will speak at the FBI's LGBT Pride Month program on Wednesday, 6/22/2016 (**note date correction**), at 11:00 a.m., in the FBIHQ Bonaparte Auditorium. The event will be webcast b6 -2 b7C -2
- Employees interested in creating a Thrift Savings Plan (TSP) account or better managing an existing account can attend two separate briefings on Friday,

or questions, contact the staff at leb@ic.fbi.gov. Follow the *Bulletin* on Twitter at @FBILEB. Articles in this issue include: *"International Efforts by Police Leadership to Combat Human Trafficking," "New Technology Benefits Law Enforcement by Tracking Sidearm Use," "Helium vs. Helicopter,"* and *"Cops and Clergy Breakfast,"* the third submission to our new department, Community Outreach Spotlight, from the Galveston, Texas, Police Department

[redacted] b7E -1

- Read *The Dispatch*, the Directorate of Intelligence's weekly publication for intelligence professionals

INTEGRITY, COMPLIANCE, AND ETHICS

- Did you know it's a criminal offense for you to participate in any official matter in which you, your spouse, or dependent child has a financial interest? Don't risk it; contact your CDC or OIC if you have any doubt about whether you should participate in that next case! For additional information, look here: Conflicting Financial Interests

- Federal employees cannot accept gifts offered from "prohibited sources" OR by virtue of their official position UNLESS an exception applies. Not sure whether there is an exception that covers your situation? Call your CDC or OIC BEFORE you accept that gift. For additional information, look here: Gifts from outside sources

- Help us recognize those who are leading by example. Nominate a colleague for a Core Values award. Nominations for this quarter are due on Friday, 7/15/2016. June's core values are Respect and Compassion, but you can nominate a colleague for excellence in any category

POLICY

- This week, the Internal Policy Office published two policies: [redacted] Undercover Activities and Operations - Posing as a Member of the News Media or a Documentary Film Crew b7E -1

- Remember, if it is not in the Policy Library, it is NOT considered official FBI policy

- For your convenience, the Internal Policy Office (IPO) is implementing the use of quick reference guides as an aid to policy guides. Do you have a suggestion for a quick reference guide to make policy easier for you? Contact IPO with your suggestions

HUMAN RESOURCES

- The 2016 Virtual Retirement Conference (VRC) is now available on HRD's Retirement

EXHIBIT O

From: GAVIN, MICHAEL T. (CID) (FBI)
To: [redacted] GAVIN, MICHAEL T. (CID) (FBI); [redacted] MARSHALL, HOWARD S. (LS) (FBI); [redacted] HUGHES, ROBERT (CID) (FBI); [redacted] TABB, JAY S. (CTD) (FBI); [redacted]
Cc: [redacted] PAARMANN, C BRYAN (CTD) (FBI); HERSEM, STEVEN W. (CTD) (FBI); [redacted] LANGENBERG, JAMES C. (INSD) (FBI); [redacted]
Subject: Policy Notice - Posing as a Member of the News Media or a Documentary Film Crew --- UNCLASSIFIED~~//FOUO~~
Date: Wednesday, June 08, 2016 4:04:16 PM
Importance: High

b6 -1
b7C -1
b7E -4

Classification: UNCLASSIFIED~~//FOUO~~

In February of this year, I notified headquarters and field office Undercover Coordinators (UCCs) that a policy revision was being negotiated with DOJ that would raise the approval level for undercover activity and operations which utilize any variation of a documentary/news media scenario. Those negotiations are complete and a policy notice, designated 0907N, was authorized and published today and is available in RPO's Internal Policy Office library. It can be accessed via this link: Undercover Activities and Operations - Posing as a Member of the News Media or a Documentary Film Crew Policy Notice.

While I refer to you the policy notice for details, the bottom line is that Deputy Director (DD) authorization and ODAG consultation is now required to use documentary/news media scenarios in undercover operations. There are specific conditions and restrictions which apply to the approval and use of these scenarios in exigent and emergency circumstances as well as in undercover activity (five or less substantive contacts outside of an authorized undercover operation). This policy notice applies to all investigative program. I refer you to the DIOG for the definition of "News Media."

In the event you need to seek DD authorization pursuant to this new policy, contact your [redacted] representative and we will coordinate review and authorization on your behalf. While we will discuss this policy notice in more detail via SVTC in the coming weeks and at our annual UCC conference scheduled for July, I wanted to give you the latest information on the subject. Please ensure all appropriate personnel in your field office or FBIHQ division are aware of this new policy. Contact me or your [redacted] representative for additional details or with questions.

b7E -3

Thank you,

Michael T. Gavin

Chief [redacted]

[redacted]

b6 -1
b7C -1
b7E -3

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

GAVIN, MICHAEL T. (CID) (FBI)

From: GAVIN, MICHAEL T. (CID) (FBI)
Sent: Wednesday, June 08, 2016 9:40 AM
To: MARSHALL, HOWARD S. (LS) (FBI)
Cc: [redacted] b6 -1 b7C -1
Subject: FW: Notification to FBIHQ and the field regarding heightened interim approval levels for use of "documentary" related undercover scenarios UNCLASSIFIED//~~FOUO~~
Attachments: Deputy Director approval now required for use of the "Documentary" scenario in Undercover Operations UNCLASSIFIED//~~FOUO~~.msg; UCO UNCLASSIFIED//~~FOUO~~.msg; Message to HQ PMs regarding UC Operations Approval UNCLASSIFIED.msg

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

Mr. Marshall,

See below for your situational awareness. Pursuant to a request for information from [redacted] b6 -1 b7C -1 assigned to the DD's staff), I provided the following information to her regarding the use of News Media and Documentary scenarios in undercover operations.

Michael T. Gavin

Chief, [redacted] b6 -1 b7C -1 b7E -3

[redacted]

From: GAVIN, MICHAEL T. (CID) (FBI)
Sent: Wednesday, June 08, 2016 9:17 AM
To: [redacted] b6 -1 b7C -1
Cc: [redacted] GAVIN, MICHAEL T. (CID) (FBI); [redacted]
Subject: Notification to FBIHQ and the field regarding heightened interim approval levels for use of "documentary" related undercover scenarios --- UNCLASSIFIED//~~FOUO~~

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

[redacted] b6 b7C

There have been a number of communications to HQ components and the field in 2016 regarding the use of "documentary" and similar type scenarios in undercover operations. In early February 2016, I was notified that a discussion had been initiated with DOJ regarding a potential FBI policy change that would require DD authorization for the use of such scenarios. Until such time as the negotiations with

DOJ were resolved, I was subsequently directed to implement an interim procedure that ensured the DD authorized these types of operations across all investigative programs.

Below are three emails pertaining to the implementation of an interim procedure requiring DD authorization for undercover scenarios using documentary or similar scenarios. I have not included any emails regarding our discussions or efforts to craft the actual policy change.

Email #1, dated 2/18/2016, is from NSB EAD Steinbach to NSB components on this issue. Email #2, dated 2/19/2016, is an email from me to all Undercover Coordinators (UCCs), both in the field and FBIHQ, notifying them of the interim requirements. Email #3, dated 2/23/2016, is an email from CID AD Campbell to CID components reiterating the interim requirements.

Let me know if you need additional information.

Michael T. Gavin

Chief, [redacted]

b6 -1
b7C -1
b7E -3

[redacted]

#1

<<UCO --- UNCLASSIFIED~~//FOUO~~>>

#2

<<Deputy Director approval now required for use of the "Documentary" scenario in Undercover Operations --- UNCLASSIFIED~~//FOUO~~>>

#3

<<Message to HQ PMs regarding UC Operations Approval --- UNCLASSIFIED>>

==========

Classification: UNCLASSIFIED~~//FOUO~~

==========

Classification: UNCLASSIFIED~~//FOUO~~

GAVIN, MICHAEL T. (CID) (FBI)

From: GAVIN, MICHAEL T. (CID) (FBI)
Sent: Friday, February 19, 2016 2:57 PM
To: [redacted]
Cc: GAVIN, MICHAEL T. (CID) (FBI); [redacted]; HUGHES, ROBERT (CID) (FBI); CAMPBELL, JOSEPH S (CID) (FBI); [redacted]
Subject: Deputy Director approval now required for use of the "Documentary" scenario in Undercover Operations UNCLASSIFIED~~//FOUO~~
Importance: High

b6 -1
b7C -1
b7E -4

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

Undercover Coordinators,

Pursuant to an ongoing dialogue between FBIHQ and DOJ, I was contacted recently by OGC regarding the use of the "documentary" scenario in undercover operations. You may already be aware of the situation, but I wanted to ensure you heard it directly from [redacted]

b7E -3

Pending the outcome of consultations with DOJ, Deputy Director approval is required for utilization of the "Documentary Film Crew" scenario, or similar scenarios, in undercover operations (UCO). This applies to both Group I and Group II UCOs and is effective immediately. Please ensure appropriate personnel, including executive management, in your field office are aware of this requirement. Contact your [redacted] representative for additional details or with questions.

b7E -3

Thank you,
Michael T. Gavin
Chief, [redacted]

b6 -1
b7C -1
b7E -3

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

STEINBACH, MICHAEL B. (DO) (FBI)

From: STEINBACH, MICHAEL B. (DO) (FBI)
Sent: Thursday, February 18, 2016 10:09 AM
To: GAVIN, MICHAEL T. (CID) (FBI); PAARMANN, C BRYAN (CTD) (FBI); HERSEM, STEVEN W. (CTD) (FBI); TABB, JAY S. (CTD) (FBI); UPCHURCH, L D (LR)(FBI); REES, STEPHEN (CTD) (FBI); MENTZER, LARISSA L. (CTD) (FBI); ROBERTS, GERALD (WFO) (FBI); [redacted] PAUL, MICHAEL F (CTD) (FBI)
Subject: UCO UNCLASSIFIED~~//FOUO~~

b6 -1
b7C -1

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

I want to ensure everyone understands that all UCOs that involve the use of a fictional media company, news entity, documentary crew, etc as a part of the scenario must have Deputy Director approval.

Michael B. Steinbach
Assistant Director
Counterterrorism Division
[redacted]
(Unclass) [redacted]
(BB) [redacted]

b6 -1
b7C -1
b7E -4

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

b6 -1
b7C -1

From:
Sent: Tuesday, February 23, 2016 9:42 AM
To: HUGHES, ROBERT (CID) (FBI); GAVIN, MICHAEL T. (CID) (FBI)
Cc:
Subject: Message to HQ PMs regarding UC Operations Approval UNCLASSIFIED

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

All,

The information below was sent to Undercover Coordinators in the field late last week. We are providing you with this information so that you are aware of the change and approval level required for the use of "documentary" scenarios in undercover operations.

Please contact with any questions or concerns. b7E -3

Thank you,

Joe C.

AD Joseph S. Campbell
Criminal Investigative Division

Message to Undercover Program Coordinators

Pursuant to an ongoing dialogue between FBIHQ and DOJ, [redacted] was contacted recently by OGC regarding the use of the "documentary" scenario in undercover operations. b7E -3

Pending the outcome of consultations with DOJ, Deputy Director approval is required for utilization of the "Documentary Film Crew" scenario, or similar scenarios, in undercover operations (UCO). This applies to both Group I and Group II UCOs and is effective immediately. Please ensure appropriate personnel, including executive management, in your field office are aware of this requirement. Contact your [redacted] representative for additional details or with questions. b7E -3

==========

Classification: UNCLASSIFIED

[redacted] b6 -1 b7C -1

From: [redacted]
Sent: Wednesday, June 08, 2016 4:06 PM
To: GAVIN, MICHAEL T. (CID) (FBI)
Subject: RE: Policy Notice Posing as a Member of the News Media or a Documentary Film Crew UNCLASSIFIED~~//FOUO~~

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

Congrats Mike! I know this was a heavy lift!

From: GAVIN, MICHAEL T. (CID) (FBI)
Sent: Wednesday, June 08, 2016 4:04 PM
To: [redacted] GAVIN, MICHAEL T. (CID) (FBI); [redacted] MARSHALL, HOWARD S. (LS) (FBI); [redacted] HUGHES, ROBERT (CID) (FBI); [redacted] TABB, JAY S. (CTD) (FBI); [redacted] PAARMANN, C BRYAN (CTD) (FBI); HERSEM, STEVEN W. (CTD) (FBI) b6 -1 b7C -1 b7E -4
Cc: [redacted] LANGENBERG, JAMES C. (INSD) (FBI); [redacted]
Subject: Policy Notice - Posing as a Member of the News Media or a Documentary Film Crew --- UNCLASSIFIED~~//FOUO~~
Importance: High

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

In February of this year, I notified headquarters and field office Undercover Coordinators (UCCs) that a policy revision was being negotiated with DOJ that would raise the approval level for undercover activity and operations which utilize any variation of a documentary/news media scenario. Those negotiations are complete and a policy notice, designated 0907N, was authorized and published today and is available in RPO's Internal Policy Office library. It can be accessed via this link: Undercover Activities and Operations Posing as a Member of the News Media or a Documentary Film Crew Policy Notice.

While I refer to you the policy notice for details, the bottom line is that Deputy Director (DD) authorization and ODAG consultation is now required to use documentary/news media scenarios in undercover operations. There are specific conditions and restrictions which apply to the approval and use of these scenarios in exigent and emergency circumstances as well as in undercover activity (five or less substantive contacts outside of an authorized undercover operation). This policy notice applies to all investigative program. I refer you to the DIOG for the definition of "News Media."

LANGENBERG, JAMES C. (INSD) (FBI)

From: LANGENBERG, JAMES C. (INSD) (FBI)
Sent: Wednesday, June 08, 2016 5:45 PM
To: GAVIN, MICHAEL T. (CID) (FBI)
Subject: RE: Policy Notice Posing as a Member of the News Media or a Documentary Film Crew UNCLASSIFIED~~//FOUO~~

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

SC Gavin,

It was great meeting you today. I appreciate your prompt attention to my inquiries. I look forward to working with you in the future.

Jim Langenberg
INSD-Section Chief
External Audit and Compliance Section
FBIHQ
[redacted](desk)
[redacted](cell)
[redacted]

b6 -1
b7C -1

From: GAVIN, MICHAEL T. (CID) (FBI)
Sent: Wednesday, June 08, 2016 4:04 PM
To: [redacted]; GAVIN, MICHAEL T. (CID) (FBI); [redacted]; MARSHALL, HOWARD S. (LS) (FBI); [redacted]; HUGHES, ROBERT (CID) (FBI); [redacted]; TABB, JAY S. (CTD) (FBI); [redacted]; PAARMANN, C BRYAN (CTD) (FBI); HERSEM, STEVEN W. (CTD) (FBI)
Cc: [redacted]; LANGENBERG, JAMES C. (INSD) (FBI); [redacted]
Subject: Policy Notice - Posing as a Member of the News Media or a Documentary Film Crew --- UNCLASSIFIED~~//FOUO~~
Importance: High

b6 -1
b7C -1
b7E -4

GAVIN, MICHAEL T. (CID) (FBI)

From: GAVIN, MICHAEL T. (CID) (FBI)
Sent: Tuesday, June 28, 2016 7:44 AM
To: [redacted] b6 -1 b7C -1
Subject: RE: Policy Notice Posing as a Member of the News Media or a Documentary Film Crew UNCLASSIFIED~~//FOUO~~

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

All good. Great to hear from you.

Michael

From: [redacted] b6 -1 b7C -1
Sent: Thursday, June 23, 2016 10:52 PM
To: GAVIN, MICHAEL T. (CID) (FBI)
Subject: RE: Policy Notice - Posing as a Member of the News Media or a Documentary Film Crew --- UNCLASSIFIED~~//FOUO~~

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

Great to see this done! I hope you are doing well! [redacted] b6 -1 b7C -1

From: GAVIN, MICHAEL T. (CID) (FBI)
Sent: Wednesday, June 08, 2016 10:04 AM
To: [redacted] b6 -1 b7C -1 b7E -4
GAVIN, MICHAEL T. (CID) (FBI); [redacted]
MARSHALL, HOWARD S. (LS) (FBI); [redacted]
HUGHES, ROBERT [redacted]
TABB, JAY S. (CTD) (FBI); [redacted]
[redacted]
PAARMANN, C BRYAN (CTD) (FBI); [redacted]
HERSEM, STEVEN W. (CTD) (FBI)
Cc: [redacted]
LANGENBERG, JAMES C. (INSD) (FBI); [redacted]
Subject: Policy Notice - Posing as a Member of the News Media or a Documentary Film Crew --- UNCLASSIFIED~~//FOUO~~
Importance: High

[redacted] b6 -1 b7C -1

From: [redacted]
Sent: Thursday, June 09, 2016 9:21 AM
To: GAVIN, MICHAEL T. (CID) (FBI)
Subject: RE: Policy Notice Posing as a Member of the News Media or a Documentary Film Crew UNCLASSIFIED~~//FOUO~~

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

Great email, Michael!!

From: GAVIN, MICHAEL T. (CID) (FBI)
Sent: Wednesday, June 08, 2016 4:04 PM
To: [redacted] GAVIN, MICHAEL T. (CID) (FBI); [redacted] MARSHALL, HOWARD S. (LS) (FBI); [redacted] HUGHES, ROBERT (CID) (FBI); [redacted] TABB, JAY S. (CTD) (FBI); [redacted] PAARMANN, C BRYAN (CTD) (FBI); HERSEM, STEVEN W. (CTD) (FBI)
Cc: [redacted] LANGENBERG, JAMES C. (INSD) (FBI) [redacted]
Subject: Policy Notice - Posing as a Member of the News Media or a Documentary Film Crew --- UNCLASSIFIED~~//FOUO~~
Importance: High

b6 -1 b7C -1 b7E -4

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

In February of this year, I notified headquarters and field office Undercover Coordinators (UCCs) that a policy revision was being negotiated with DOJ that would raise the approval level for undercover activity and operations which utilize any variation of a documentary/news media scenario. Those negotiations are complete and a policy notice, designated 0907N, was authorized and published today and is available in RPO's Internal Policy Office library. It can be accessed via this link: Undercover Activities and Operations Posing as a Member of the News Media or a Documentary Film Crew Policy Notice.

While I refer to you the policy notice for details, the bottom line is that Deputy Director (DD) authorization and ODAG consultation is now required to use documentary/news media scenarios in undercover operations. There are specific conditions and restrictions which apply to the approval and use of these scenarios in exigent and emergency circumstances as well as in undercover activity (five or less substantive contacts outside of an authorized undercover operation). This policy notice applies to all investigative program. I refer you to the DIOG for the definition of "News Media."

From: [redacted]
To:
Subject: FW: Undercovers Utilizing Documentary Film Crew --- ~~SECRET~~
Date: Friday, February 05, 2016 4:24:19 PM

b6 -1
b7C -1
b7E -4

Classification: ~~SECRET~~

~~Classified By:~~ [redacted]
~~Derived From: Multiple Sources~~
~~Declassify On: 20411231~~

b6 -1
b7C -1

==========

TRANSITORY RECORD

From: UPCHURCH, L DIANE (CTD)(FBI)
Sent: Friday, February 05, 2016 4:23 PM
To: [redacted]

b6 -1
b7C -1

Subject: FW: Undercovers Utilizing Documentary Film Crew --- ~~SECRET~~

Classification: ~~SECRET~~

~~Classified By:~~ [redacted]
~~Derived From: Multiple Sources~~
~~Declassify On: 20411231~~

b6 -1
b7C -1

==========

TRANSITORY RECORD

fysa

From: PAARMANN, C. (CTD) (FBI)
Sent: Friday, February 05, 2016 3:32 PM
To: [redacted]
Cc [redacted] GAVIN, MICHAEL T. (CID) (FBI)
Subject: Undercovers Utilizing Documentary Film Crew --- ~~SECRET~~

b6 -1
b7C -1
b7E -4

Classification: ~~SECRET~~

~~Classified By:~~ [redacted]
~~Derived From: Multiple Sources~~
~~Declassify On: 20411231~~

b6 -1
b7C -1

==========

TRANSITORY RECORD

By verbal order of the Deputy Director -- Henceforth, due to the nature and potential sensitivity of the technique, Deputy Director approval is henceforth required for any UCO scenario utilizing the cover of a Documentary Film Crew or similar scenario. This is a change to both policy and the implementation guide and being put out to you all as you staff and run the CUORC. NSB and OGC will be making the appropriate paper changes. In the meantime,

please take note and comply as this order is effective immediately.

C. Bryan Paarmann

Deputy Asst. Director

Counterterrorism Division, FBI

(o) [redacted]

(cell) [redacted]

(secure) [redacted]

b6 -1
b7C -1
b7E -4

==========

Classification: ~~SECRET~~

==========

Classification: ~~SECRET~~

==========

Classification: ~~SECRET~~

From: [redacted] b6 -1 b7C -1
To:
Cc:
Subject: FW: Undercovers Utilizing Documentary Film Crew --- ~~SECRET~~
Date: Monday, February 08, 2016 3:45:32 PM

Classification: ~~SECRET~~

Classified By: [redacted] b6 -1 b7C -1
Derived From: ~~Multiple Sources~~
Declassify On: ~~20411231~~
==========

TRANSITORY RECORD

[redacted] – ummmm. How do I answer this? Did I understand that you and [redacted] were present when the DD said the below? Do we need to push out guidance to our folks? Should I just call Paarman? Thanks for any light you can shed, [redacted] b6 -1 b7C -1

From: [redacted]
Sent: Monday, February 08, 2016 3:18 PM
To: [redacted] b6 -1 b7C -1
Cc: [redacted]
Subject: FW: Undercovers Utilizing Documentary Film Crew --- ~~SECRET~~

Classification: ~~SECRET~~

Classified By: [redacted] b6 -1 b7C -1
Derived From: ~~Multiple Sources~~
Declassify On: ~~20411231~~
==========

TRANSITORY RECORD

[redacted] b6 -1 b7C -1

We at CCOU have just become aware of this new order from the Deputy Director. We have several questions regarding its implementation:

1. Does the order apply to all UCOs, or only to National Security UCOs?

2. Does the order apply to Group I and Group II UCOs?

3. If the order applies to Group II UCOs approved by SACs, what is the mechanism for obtaining DD approval, since previously these UCOs have only required FBIHQ approval (by EC) when Fiscal Circumstances existed?

4. Does the order apply only to future UCOs, or does it apply retroactively to ongoing UCOs that have already been approved with the documentary film crew scenario?

Your guidance here is greatly appreciated.

Thanks,

[redacted]

SSA [redacted]

b6 -1
b7C -1
b7E -3

FBIHQ [redacted]

Criminal Covert Operations Unit

[redacted] (Office)

[redacted] (Cell)

From: [redacted]
Sent: Monday, February 08, 2016 2:40 PM
To: [redacted]
Cc: [redacted]

b6 -1
b7C -1

Subject: FW: Undercovers Utilizing Documentary Film Crew --- ~~SECRET~~

Classification: ~~SECRET~~

~~Classified By:~~ [redacted]
Derived From: ~~Multiple~~ Sources
~~Declassify~~ On: 20411231
==========

b6 -1
b7C -1

TRANSITORY RECORD

Dear SSA [redacted]

[redacted]

b6 -1
b7C -1
b7E -7

Regards,

[redacted]

From: [redacted]
Sent: Monday, February 08, 2016 11:03 AM
To: [redacted]

b6 -1
b7C -1

[redacted] b6 -1 b7C -1

Subject: FW: Undercovers Utilizing Documentary Film Crew --- ~~SECRET~~

~~Classification: SECRET~~

~~Classified By:~~ [redacted] b6 -1
~~Derived From: Multiple Sources~~ b7C -1
~~Declassify On: 20411231~~
==========

TRANSITORY RECORD

FYSA, please see below regarding UCO scenarios involving Documentary Film Crews (or similar situations).

v/r

b6 -1
b7C -1

[redacted]

From: [redacted]
Sent: Friday, February 05, 2016 6:31 PM
To: [redacted] b6 -1 b7C -1

Subject: FW: Undercovers Utilizing Documentary Film Crew --- ~~SECRET~~

~~Classification: SECRET~~

~~Classified By:~~ [redacted] b6 -1
~~Derived From: Multiple Sources~~ b7C -1
~~Declassify On: 20411231~~
==========

FYSA

From: PAARMANN, C. (CTD) (FBI)
Sent: Friday, February 05, 2016 3:32 PM
To: [redacted] b6 -1 b7C -1
Cc: [redacted] GAVIN, MICHAEL T. (CID) (FBI) b7E -4
Subject: Undercovers Utilizing Documentary Film Crew --- ~~SECRET~~

~~Classification: SECRET~~

~~Classified By:~~ [redacted] b6 -1
~~Derived From: Multiple Sources~~ b7C -1
~~Declassify On: 20411231~~
==========

TRANSITORY RECORD

By verbal order of the Deputy Director -- Henceforth, due to the nature and potential sensitivity of the technique, Deputy Director approval is henceforth required for any UCO scenario utilizing the cover of a Documentary Film Crew or similar scenario. This is a change to both policy and the implementation guide and being put out to you all as you staff and run the CUORC. NSB and OGC will be making the appropriate paper changes. In the meantime, please take note and comply as this order is effective immediately.

C. Bryan Paarmann

Deputy Asst. Director

Counterterrorism Division, FBI

(o) [redacted]

(cell) [redacted]

(secure [redacted]

b6 -1
b7C -1
b7E -4

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

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

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

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

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

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

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