

Defendants.

Case No. 12-cv-00127 (RWR)

Exhibit 1 to the Memorandum in Support of Defendants' Motion for Summary Judgment

whose collective mission is to effectively plan, develop, direct, and manage responses to requests for access to Federal Bureau of Investigation (“FBI”) records and information pursuant to the FOIA, 5 U.S.C. § 552; Privacy Act of 1974; Executive Order (“E.O.”) 13526; Presidential, Attorney General and FBI policies and procedures; judicial decisions; and other Presidential and Congressional directives. My responsibilities also include the review of FBI information for classification purposes as mandated by Executive Order 13526, 75 Fed. Reg. 707 (2010), and the preparation of declarations in support of FOIA Exemption 1 claims asserted under the FOIA, 5 U.S.C. § 552(b)(1). I have been designated by the Attorney General of the United States as an original classification authority and a declassification authority pursuant to Executive Order 13526, §§ 1.3 and 3.1. The statements contained in this declaration are based upon my personal knowledge, upon information provided to me in my official capacity, and upon conclusions and determinations reached and made in accordance therewith.

(3) Due to the nature of my official duties, I am familiar with the procedures followed by the FBI in responding to requests for information pursuant to the provisions of the FOIA, 5 U.S.C. § 552 and the Privacy Act (“PA”) of 1974, 5 U.S.C. § 552a. Specifically, I am aware of the FBI’s response to the FOIA request of plaintiff, Electronic Privacy Information Center (“EPIC”), which seeks access to certain FBI records about “individuals targeted for surveillance for support for or interest in WikiLeaks.”

(4) The FBI submits this declaration in support of its motion for summary judgment. In accordance with *Vaughn v. Rosen*, 484 F.2d 820 (D.C. Cir. 1973), this declaration provides an explanation of the FBI’s record-keeping system and the procedures used to search for records responsive to plaintiff’s request, and provides justifications for the FBI’s withholding of information pursuant to FOIA Exemptions 1, 3, 5, 6, 7(A), 7(C), 7(D), 7(E), and 7(F). *See*

5 U.S.C. §§ 552 (b)(1), (b)(3), (b)(5), (b)(6), (b)(7)(C), (b)(7)(D), (b)(7)(E), and (b)(7)(F).

Additional information which cannot be provided publicly regarding FOIA Exemptions 3 and 7(D) is included in my *in camera, ex parte* declaration, which is being submitted in further support of the FBI's motion for summary judgment. *See* 2nd Hardy Decl.

PROCEDURAL HISTORY OF PLAINTIFF'S FOIA REQUEST

(5) A chronology and description of pertinent correspondence concerning plaintiff's FOIA request is set forth below. Copies of the relevant correspondence are attached hereto as **Exhibits A-D**.

(6) Plaintiff submitted a FOIA request letter by facsimile dated June 23, 2011, seeking access to "documents regarding the government's identification and surveillance of individuals who have demonstrated support for or interest in WikiLeaks, as well as any documents relating to records obtained from Internet and financial services companies regarding these individuals," and specifically:

1. All records regarding any individuals targeted for surveillance for support for or interest in WikiLeaks;
2. All records regarding lists of names of individuals who have demonstrated support for or interest in WikiLeaks;
3. All records of any agency communications with Internet and social media companies including, but not limited to Facebook and Google, regarding lists of individuals who have demonstrated, through advocacy or other means, support for or interest in WikiLeaks; and
4. All records of any agency communications with financial services companies including, but not limited to Visa, MasterCard, and PayPal, regarding lists of individuals who have demonstrated, through monetary donations or other means, support or interest in WikiLeaks.

Plaintiff also sought expedited processing and a fee waiver. (***See Exhibit A.***)

(7) By letter dated July 11, 2011, RIDS informed plaintiff that a search of the FBI's Central Records System ("CRS") resulted in no main files being located but if plaintiff had any

additional information, the FBI would conduct an additional search. The FBI further advised that plaintiff's request for expedited processing need not be adjudicated because no files had been located. Finally, the FBI explained plaintiff's right to file an appeal within sixty (60) days by writing to the U.S. Department of Justice, Office of Information Policy ("OIP").

(See Exhibit B.)

(8) Plaintiff appealed to OIP via a facsimile dated September 9, 2011, challenging the FBI's response that its search failed to locate any main files responsive to plaintiff's FOIA request. **(See Exhibit C.)**

(9) OIP acknowledged receipt of plaintiff's appeal in a letter dated September 20, 2011, and informed plaintiff that it would respond to the appeal as soon as possible.

(See Exhibit D.)

(10) OIP had not responded to plaintiff's appeal before plaintiff filed the present lawsuit on January 25, 2012. **(See Docket ("Dkt.") No. 1, Complaint.)**

EXPLANATION OF THE FBI'S CENTRAL RECORDS SYSTEM

(11) The Central Records System ("CRS") enables the FBI to maintain information which it has acquired in the course of fulfilling its mandated law enforcement responsibilities. The records maintained in the CRS consist of administrative, applicant, criminal, personnel, and other files compiled for law enforcement purposes. This system consists of a numerical sequence of files, called FBI "classifications," which are broken down according to subject matter. The subject matter of a file may relate to an individual, organization, company, publication, activity, or foreign intelligence matter (or program). Certain records in the CRS are maintained at FBIHQ. Records that are pertinent to specific field offices of the FBI are maintained in those field offices. Although the CRS is primarily designed to serve as an

investigative tool, the FBI searches the CRS for documents that are potentially responsive to FOIPA requests. The mechanism that the FBI uses to search the CRS is the Automated Case Support System (“ACS”).

(12) The retrieval of data from the CRS is made possible through the ACS using the General Indices, which are arranged in alphabetical order.¹ The General Indices consist of index cards on various subject matters that are searched either manually or through the automated indices. The entries in the General Indices fall into two categories:

(a) A “main” entry, or “main” file, carries the name corresponding with a subject of a file contained in the CRS.

(b) A “reference” entry, or a “cross reference,” is generally only a mere mention or reference to an individual, organization, or other subject matter, contained in a document located in another “main” file on a different subject matter.

(13) Access to the CRS files in FBI Field Offices is also obtained through the General Indices (automated and manual), which are likewise arranged in alphabetical order, and consist of an index on various subjects, including the names of individuals and organizations. Searches made in the General Indices to locate records concerning a particular subject, such as WikiLeaks, are made by searching the subject requested in the index. FBI Field Offices have automated indexing functions.

(14) On or about October 16, 1995, the ACS system was implemented for all Field Offices, Legal Attaches (“Legats”), and FBIHQ in order to consolidate portions of the CRS that were previously automated. ACS can be described as an internal computerized subsystem of the CRS. Because the CRS cannot electronically query the case files for data, such as an individual’s name or social security number, the required information is duplicated and moved to

¹ The General Indices also include index cards that allow a manual search for records prior to September 24, 1987, the date on which they became fully automated.

the ACS so that it can be searched. Over 105 million records from the CRS were converted from automated systems previously utilized by the FBI. Automation did not change the CRS; instead, automation has facilitated more economic and expeditious access to records maintained in the CRS.

(15) The ACS consists of three integrated, yet separately functional, automated applications that support case management functions for all FBI investigative and administrative cases:

(a) Investigative Case Management (“ICM”) – ICM provides the ability to open, assign, and close investigative and administrative cases as well as set, assign, and track leads. The Office of Origin (“OO”), which sets leads for itself and other field offices, as needed, opens a case. The field offices that receive leads from the OO are referred to as Lead Offices (“LOs”), formerly known as Auxiliary Offices. When a case is opened, it is assigned a Universal Case File Number (“UCFN”), which is used by all FBIHQ, as well as all FBI field offices and Legats that are conducting or assisting in the investigation. Using the file number “163-SA-12345” as an example, an explanation of the UCFN is as follows: “163” indicates the classification for the specific type of investigation, in this example “Foreign Police Cooperation”; “SA” is the abbreviated form used for the OO of the investigation, in this example San Antonio; and “12345” denotes the individual case file number for the particular investigation.

(b) Electronic Case File (“ECF”) – ECF serves as the central electronic repository for the FBI’s official text-based documents. ECF supports the universal serial concept in that only the creator of a document serializes it into a file. This provides a single-source entry of serials into the computerized ECF system. All original serials are maintained in the OO case file.

(c) Universal Index (“UNI”) – UNI continues the universal concepts of ACS by providing a complete subject/case index to all investigative and administrative cases. Only the OO is required to index; however, the LOs may index additional information as needed. UNI, an index of approximately 115 million records, functions to index names to cases, and to search names and cases for use in FBI investigations. Names of individuals or organizations are recorded with identifying applicable information such as date or place of birth, race, sex, locality, Social Security number, address, and/or date of event.

(16) The decision to index names other than subjects, suspects, and victims is a discretionary decision made by the FBI Special Agent (“SA”) – and on occasion, support employees – assigned to work on the investigation, the Supervisory SA (“SSA”) in the field office conducting the investigation, and the SSA at FBIHQ. The FBI does not index every name in its files; rather, it indexes only that information considered to be pertinent, relevant, or essential for future retrieval. Without a “key” (index) to this enormous amount of data, information essential to ongoing investigations could not be readily retrieved. The FBI files would thus be merely archival in nature and could not be effectively used to serve the mandated mission of the FBI, which is to investigate violations of federal criminal and national security statutes. Therefore, the General Indices to the CRS files are the means by which the FBI can determine what retrievable information, if any, the FBI may have in its CRS files on a particular subject matter, individual, or organization, such as WikiLeaks.

SEARCH FOR RECORDS RESPONSIVE TO PLAINTIFF’S FOIA REQUEST

(17) In response to plaintiff’s June 23, 2011, FOIA request, the FBI conducted a search of the CRS using the search term “WikiLeaks” to identify all potentially responsive main files

indexed to that term. The FBI identified no main files indexed to “WikiLeaks” as a result of this search.

(18) Consistent with the FBI’s current policy of searching for and identifying only main files responsive to FOIA requests at the initial administrative stage, the initial search of the CRS was limited to locating potentially responsive main files.

(19) The FBI subsequently conducted a second search of the CRS to locate any reference entries that might be responsive to plaintiff’s request, using the term “WikiLeaks.”² The second search of the CRS identified a file containing reference entries pertaining to WikiLeaks. The case agents assigned to this file were contacted about whether it might contain information responsive to plaintiff’s request for “all records regarding any individual targeted for surveillance for support for or interest in WikiLeaks,” for “lists of names of individuals who have supported or shown interest in WikiLeaks,” and for communications with internet, social media, and financial services companies regarding “lists of individuals who have demonstrated ... support for or interest in WikiLeaks.” As a result of these consultations, the FBI identified investigative files that likely contain information responsive to plaintiff’s FOIA request.³

(20) The files containing information potentially responsive to plaintiff’s request are part of active, ongoing criminal investigations. The FBI has determined that all potentially responsive records in these files are exempt from disclosure pursuant to FOIA Exemption 7(A),

² Reference entries, or cross-references, are mere mentions of a subject, individual, or organization in files that are indexed to other subjects, individuals, organization, events, or activities.

³ Plaintiff’s request seeks “[a]ll records regarding any individuals targeted for surveillance for support for or interest in WikiLeaks,” as well as certain information regarding “lists of individuals who have demonstrated support for or interest in WikiLeaks.” The FBI is not investigating individuals who simply support or have an interest in WikiLeaks. However, reading Plaintiff’s request broadly, the FBI concluded that records concerning its investigation of the disclosure of classified information that was published on the WikiLeaks website would be responsive to Plaintiff’s request. The FBI does not, however, maintain lists of individuals who have demonstrated support for or interest in WikiLeaks, and thus has no records responsive to this portion of Plaintiff’s request.

5 U.S.C. § 552(b)(7)(A). Further, the FBI has determined that responsive records in these files are also exempt under one or more other FOIA exemptions, as described below.

(21) In its complaint, plaintiff suggests that the FBI's search should have included the names of various individuals that it mentioned in its request in reference to various news stories related to WikiLeaks. *See* Dkt. No. 1, p. 10, ¶ 61. Plaintiff did not specifically request records about the individuals it mentioned – Julian Assange, Rop Gonggrijp, and David House – or any other individuals. Furthermore, plaintiff did not provide privacy waivers from any individuals, including Messrs. Assange, Gonggrijp, and House. Without privacy waivers, or proof that an individual is deceased, the FBI cannot confirm or deny the existence of information about third parties.

JUSTIFICATION FOR NON-DISCLOSURE UNDER THE FOIA

EXEMPTION 7 THRESHOLD

(22) FOIA Exemption 7 exempts from mandatory disclosure records or information compiled for law enforcement purposes when disclosure could reasonably be expected to cause one of the harms enumerated in the subparts of the exemption. *See* 5 U.S.C. § 552(b)(7). Here, the FBI is relying on Exemption 7 to prevent interference with ongoing law enforcement investigations and proceedings.

(23) In order to rely on Exemption 7, an agency first must demonstrate that the records or information it seeks to withhold were compiled for law enforcement purposes. *See id.* Law enforcement agencies such as the FBI must demonstrate that the records at issue are related to the enforcement of federal laws and that the enforcement activity is within its law enforcement duties. Here, responsive records are contained in files pertaining to the FBI's investigation of the disclosure of classified information that was published on the WikiLeaks website. The FBI's

Washington Field Office opened these files in 2010 and maintains them per applicable Attorney General Guidelines. The investigations are ongoing and clearly are within the law enforcement duties of the FBI to detect and undertake investigations into possible violations of Federal criminal laws. *See* 28 U.S.C. § 533. Thus, all of the records responsive to plaintiff's FOIA request were compiled for law enforcement purposes and readily meet the threshold for applying FOIA Exemption 7.⁴

EXEMPTION 7(A) – PENDING ENFORCEMENT PROCEEDINGS

(24) FOIA Exemption 7(A) exempts from disclosure:

records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information ... could reasonably be expected to interfere with enforcement proceedings.

5 U.S.C. § 552(b)(7)(A).

(25) Application of this exemption requires: the existence of law enforcement records; a pending or prospective law enforcement proceeding; and a determination that release of the information could reasonably be expected to interfere with the enforcement proceeding. The FBI has withheld all responsive records pursuant to Exemption 7(A). As established above, these records are law enforcement records related to pending FBI investigations. The FBI has determined that disclosure of any responsive records in the midst of these active, on-going investigations is reasonably expected to interfere with those investigations as well as any resulting prosecutions. Moreover, disclosure of records from the FBI's pending investigative files is reasonably expected to interfere with the U.S. Department of the Army's pending

⁴ The FBI's files contain potentially responsive records originating from other government agencies ("OGAs"). Because the FBI is withholding all records pursuant to Exemption 7(A), it has not referred these records to their originating OGAs for review and application of other exemptions. The FBI believes that these records are also subject to one or more of the other exemptions described in this declaration. If the FBI's Exemption 7(A) withholdings are not upheld, it will refer the records to the originating OGAs for review and a direct response to plaintiff.

prosecution of Private Bradley Manning in relation to the disclosure of classified information that was published on the WikiLeaks website. As such, the release of these records would interfere with pending and prospective enforcement proceedings, including investigations and prosecutions.

Types of Documents Protected By Exemption 7(A)

(26) Providing a document-by-document description or listing of the records potentially responsive to plaintiff's request would undermine the very interests that the FBI seeks to protect under Exemption 7(A), in addition to the other exemptions identified below. In order to protect these interests, the FBI instead has described the types of potentially responsive records in the pending investigative files that are being withheld in full pursuant to Exemption 7(A).⁵ The pending investigative files contain the following types of documents:

(a) Electronic Communication ("EC"): The purpose of an EC is to communicate within the FBI in a consistent format that can be uploaded by the originating Division or office, transmitted, and downloaded by recipient Divisions or offices within the FBI's internal computer network.

(b) FBI Letter: This is a letter or formal correspondence in a format used by the FBI to communicate with the Department of Justice ("DOJ"), U.S. Attorneys' Offices, other government agencies ("OGAs"), other law enforcement agencies (including federal, state, local, and tribal), commercial businesses, and private citizens. Its format is identical to the business letters utilized by commercial agencies except that it contains the FBI Seal at the top of the first

⁵ Similarly, disclosing the total volume of responsive information protected by Exemption 7(A) and/or another exemption would reveal information about the nature, scope, focus, and conduct of active, on-going investigations, and thus cannot be publicly disclosed without undermining the law enforcement interests the FBI is seeking to protect by application of Exemption 7(A) in this case.

page, as well as specific identifying information regarding the originating office within the FBI that sent the letter (e.g., Omaha Division or FBIHQ).

(c) FD-302 (Interview Form)⁶: This is an internal FBI form on which the results of FBI interviews of persons are recorded. Such interview information may later be used as evidence at criminal trials. These interview forms are often incorporated into FBI Investigative Reports. The contents of these forms may also be incorporated into ECs for purposes of setting/covering leads.

(d) FD-542 (Investigative Accomplishment Form): This is an internal FBI form on which employees claim accomplishments and investigative methods used in investigations.

(e) FD-794 (Payment Request): This is an internal FBI form used by employees to request payment for reimbursement of expenses incurred during an investigation.

(f) Memorandum: This is ordinarily a communication from the FBI to the Attorney General and/or other DOJ component officials; from one employee/official to another at FBIHQ; or from one employee/official to another within an FBI field division. It serves to assist in the overall supervision of a case by summarizing pertinent details of an investigation.

(g) E-mails: These documents include electronic messages exchanged between and among FBI Special Agents, other FBI employees, and personnel from OGAs, concerning these investigations.

(h) Letterhead Memorandum ("LHM"): This memorandum is an interim summary that reports information, usually derived from FD-302s, concerning the subject of an investigation. It is designed to alert other field offices and/or FBIHQ about pertinent developments in an investigation. Usually, an LHM is attached to a cover sheet, which is

⁶ All forms with the designation "FD-" are forms created and utilized internally by the FBI.

typically an FBI letter. The LHM can also be detached from the cover sheet and disseminated to other Government agencies, as a “Law Enforcement Sensitive/For Official Use Only” document.

(i) FBI Records Checks: These are computerized print-outs of the results of checks of databases concerning FBI records, local law enforcement records and/or business records. The information from these records checks is often incorporated into Investigative Reports and ECs for lead purposes.

(j) FBI Investigative Reports: These are summaries of investigations as of the date of the report. The purpose of these documents is to advise FBIHQ and FBI field offices of the investigative information that has been obtained concerning a particular investigation.

(k) FBI Computer Printouts: These are printouts from internal FBI computer systems that describe information concerning FBI investigations. The information included on the documents may include file numbers, names, and addresses of subjects and suspects, key dates and places of crimes, names of Special Agents (“SAs”) assigned to investigations, and other similar information.

(l) FBI Investigative Inserts: Internal FBI forms used to record investigative actions such as an FBI records check of a database of law enforcement records. These inserts are often incorporated into FBI Investigative Reports.

(m) Other Investigative Documents: This category consists of various types of documents reflecting information and evidence gathered during an FBI investigation, the sources from/by which such information and evidence was gathered, methods used to obtain the information and evidence, and methods used to analyze the information and evidence. To describe the documents in this category any more specifically would reveal the scope of the FBI’s investigations, as well as the sources and methods being utilized by the FBI.

(n) Miscellaneous Administrative Documents: The FBI uses various types of forms throughout a criminal investigation, which include storage envelopes, bulky exhibit cover sheets, transmittal forms (i.e., facsimile cover sheets), letters, and routing slips. Also included are forms that are placed in a file to document when a serial has been removed and placed elsewhere. For example, an FD-5A (Automated Serial Permanent Charge-Out) is placed in a file to show that a serial was transferred to a sub-file. Other documents in this category include notes, memoranda, letters, telegrams, and other attachments of an administrative nature which do not fall into an official government format.

Reasonable Expectation of Interference

(27) In processing requests under the FOIA, the FBI has established procedures to implement the FOIA as efficiently as possible. When the FBI receives a request for records about a pending investigation, it commonly asserts FOIA Exemption 7(A) to protect the pending investigation and/or any related prospective investigations and prosecutions. Nonetheless, the FBI reviews the records to identify and release any reasonably segregable information contained in the responsive file(s) that would not jeopardize ongoing or future enforcement proceedings. As discussed below, the FBI's review of the potentially responsive records in the pending cases reveals no materials that can be released without jeopardizing current or prospective investigative and/or prosecutive efforts.⁷

(28) Here, RIDS has reviewed and categorized the types of documents described above into two categories – Evidentiary/Investigative Materials and Administrative Materials. Each record located in the responsive files, and the information contained in each record, falls into one or both of these categories. For example, a single record – e.g., an FBI Investigative Report –

⁷ The FBI has compiled a report listing each document reviewed by the FBI and the exemptions, other than Exemption 7(A), being applied to the document. That report is classified at the "Secret" level. The FBI can provide the report should the Court determine that it would aid its review of this case.

may serve several purposes and may contain multiple categories of information, such as witness statements, administrative directions, and/or evidentiary materials. Therefore, such a report could be included in both categories, as could the information contained in the report.

Evidentiary/Investigative Materials

(29) This category includes copies of records or evidence, analyses of evidence, and derivative communications discussing or incorporating evidence. A derivative communication describes, verbatim or in summary, the contents of the original record, how it was obtained, and how it relates to the investigation. Other derivative communications report this information to other FBI field offices, other law enforcement agencies, or other Federal agencies, either to advise them about the progress of the investigation, or to elicit their assistance in handling investigative leads. The following subparagraphs describe the types of evidentiary materials in the responsive records and the anticipated harm that could reasonably result from the release of the materials.

(30) Confidential Source Statements: Statements made to the FBI by sources based on express or implied assurances of confidentiality are one of the principal tools used in proving facts that form the basis for a prosecution. These statements contain information obtained from individuals or organizations that have knowledge of potential criminal activities in these investigations into the disclosure of classified information. If the FBI were to release this information, the sources that have chosen to cooperate with law enforcement could be subjected to retaliation, intimidation, or physical or mental harm. This would have a chilling effect on these investigations and any future prosecutions resulting from these cases, inasmuch as potential witnesses and/or sources might fear exposure and reprisals from the subjects of these investigations and/or from other individuals. Implicit in conducting interviews in investigations

of this nature is the notion that a source's identity and the information he/she/it provided will be afforded confidentiality. The FBI goes to great lengths to protect and maintain sources' confidentiality because it is an integral part of successful investigations and prosecutions. The release of source statements would disrupt and harm ongoing investigative actions and/or pending or prospective prosecutions.

(31) Exchange of Information Between FBI and Other Law Enforcement Agencies:

Release of information exchanged between the FBI and its law enforcement partners would disclose evidence, investigative information, and criminal intelligence developed by agencies that have cooperated with and provided information to the FBI, and that are still doing so, in the pending investigations. Inherent in this cooperative effort is the mutual understanding that information provided to the FBI by these agencies will not be prematurely released. This information was gathered, and is continuing to be gathered, to help identify subjects, suspects, and/or other individuals of potential investigative interest; to identify and assist in locating witnesses and/or confidential sources; and to further the progress of the investigations. Release of this information at this point in the investigative process would reveal the scope and focus of the investigations; identify and tip off individuals of interest to law enforcement; and provide suspects or targets to destroy evidence and alter their behavior to avoid detection.

(32) Documentary Evidence/Information Concerning Documentary Evidence:

Disclosure of documentary evidence being gathered in the ongoing investigations, or information that discusses, describes, or analyzes the documentary evidence, would undermine any pending or prospective prosecutions by prematurely revealing the scope and focus of the investigations, as well as the subjects of and persons of investigative interest in those investigations. Once subjects and persons of interest become aware of the FBI's attention, they are able to take

defensive actions to conceal their activities, elude detection, and/or suppress or fabricate evidence. Additionally, disclosure of documentary evidence and/or information concerning documentary evidence also could reasonably lead to the identification of the sources of the evidence. This too would adversely impact the ongoing investigations, and any pending or prospective prosecutions, because it could result in possible intimidation of or harm to those witnesses and sources. This evidence and information about this evidence in other documents is pertinent and integral to the FBI's ongoing investigations, the U.S. Army's pending prosecution of PFC Bradley Manning, and any potential future prosecutions.

Administrative Materials

(33) Materials that fall within this category include items such as case captions, serial numbers, identities of FBI field offices, dates of investigations, and detailed instructions designed to ensure that investigative procedures are conducted within the appropriate FBI and DOJ guidelines. The following subparagraphs describe the types of administrative materials contained in the files and the anticipated harms that could reasonably result from the disclosure of such materials in the midst of these ongoing investigations and prosecution, and prior to any prospective prosecutions. In many instances, administrative information is contained at the beginning or end of correspondence or documents that fall within the Investigative/Evidentiary Material category, such that release of the administrative information would also reveal the investigative interests of the FBI and could enable suspects, targets, and individuals of interest to the FBI to discern a "road map" of the investigations.

(34) Reporting Communications: These communications permit an agency to monitor the progress of the investigation and facilitate its conduct. These communications have the potential to reveal or confirm the cooperation of other Government agencies in the

investigations. These communications also are replete with detailed information about the FBI's investigative activities and about potential witnesses/sources to be interviewed. Additionally, they contain background information about third party individuals, the origins of information connecting them to the investigations, and their connections to subjects and individuals of investigative interest to the FBI. The release of this information would prematurely reveal the nature and scope of these active and ongoing investigations by revealing: the investigative steps taken to obtain witness and source interviews; techniques and investigative methods used to compile and/or solicit information from various sources; and any potential or perceived challenges in the investigations.

(35) Miscellaneous Administrative Documents: These materials include items such as storage envelopes, transmittal forms, and standardized forms used for a variety of particular purposes. These types of materials have been used throughout these investigations for many routine purposes; however, the manner in which they have been used and organized in the files in and of itself reveals information of investigative value, the premature disclosure of which could undermine the pending investigations as well as pending and prospective prosecutions.

(36) An example is the evidentiary envelope used to store records obtained from a source under an express or implied assurance of confidentiality. While the envelope is not specific to these investigations, handwritten notations on the envelope identify dates, places, and the identities of the sources providing the information. In addition, the mere fact that an FBI Special Agent used an envelope for the storage of records he/she has obtained from a source is revealing on its own. The disclosure of these materials could harm the investigation by providing details that, when viewed in conjunction with knowledge possessed by subjects or

others knowledgeable about the disclosure of classified information, would provide information useful in identifying witnesses and ascertaining investigative strategies and items of evidence.

(37) Administrative Instructions: This type of information, whether it originates in communications from the FBI or other government or law enforcement agencies, would disclose specific investigative procedures employed in these investigations. Release of this information would thus permit subjects or individuals of investigative interest to the FBI to anticipate law enforcement actions and to alter, destroy, or fabricate evidence.

(38) Specific examples of these instructions include the setting out of investigative guidelines and requests for specific investigative inquiries and affirmative taskings to various FBI field offices or to other government or law enforcement agencies. These are commonly referred to as “investigative leads” and are set forth in documents throughout the course of these investigations.

OTHER APPLICABLE FOIA EXEMPTIONS

(39) As previously explained, the FBI has determined that all responsive records in this case are exempt under FOIA Exemption 7(A). However, in light of the D.C. Circuit’s ruling in Maydak v. DOJ, 218 F.3d 760 (D.C. Cir. 2000), the FBI is also asserting FOIA Exemptions 1, 3, 5, 6, 7(C), 7(D), 7(E), and 7(F) as additional grounds for withholding records and information in this case. See 5 U.S.C. §§ 552(b)(1), (b)(3), (b)(5), (b)(6) and (b)(7)(C) – (F). The Maydak decision requires the simultaneous assertion of all applicable exemptions, in addition to Exemption 7(A). In the following paragraphs, the FBI justifies its withholding of Investigative/Evidentiary and Administrative records and information, to the extent that public disclosure and discussion of the additionally applicable exemptions will not itself adversely affect the active, on-going criminal investigations in this case by revealing the nature, scope,

focus, and conduct of the investigations, including the types and origins of sources upon which the FBI is relying. Where public disclosure of any more detailed information about the FBI's application of these exemptions at this time would undermine the very interests the FBI seeks to protect through its application of Exemption 7(A) in this case, the FBI has justified its application of those exemptions in my *in camera, ex parte* declaration, which is being submitted in further support of the FBI's motion for summary judgment. *See* 2nd Hardy Decl.

EXEMPTION 1 – CLASSIFIED INFORMATION

(40) Exemption 1 exempts from disclosure records that are:

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

5 U.S.C. § 552(b)(1).

(41) Before I consider an Exemption 1 claim for withholding agency records, I determine whether the information in those records is information that satisfies the requirements of E.O. 13526, the Executive Order which governs the classification and protection of information that affects the national security,⁸ and whether the information complies with the various substantive and procedural criteria of the Executive Order. E.O. 13526, which was signed by President Barack Obama on December 29, 2009, is the Executive Order that currently applies to the protection of national security information. I am bound by the requirements of E.O. 13526, when making classification determinations.

⁸ Section 6.1 (cc) of E.O. 13526, defines "National Security" as "the national defense of foreign relations of the United States."

(42) For information to be properly classified, and thus properly withheld from disclosure pursuant to Exemption 1, the information must meet the requirements set forth in E.O. 13526 § 1.1(a):

- (1) an original classification authority must have classified the information;
- (2) the information must be owned by, produced by or for, or be under the control of the United States Government;
- (3) the information must fall within one or more of the categories of information listed in § 1.4 of this order; and
- (4) the original classification authority must determine that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, which includes defense against transnational terrorism, and the original classification authority must be able to identify or describe the damage.

(43) All information that I determined to be classified is marked at the “Secret” level because the unauthorized disclosure of this information reasonably could be expected to cause serious damage to national security. See E.O. 13526 § 1.2 (a)(2). In addition to this substantive requirement, certain procedural and administrative requirements of E.O. 13526, must be followed before information can be considered to be properly classified, such as proper identification and marking of documents. I made certain that all procedural requirements of E.O. 13526, were followed in order to ensure that the information was properly classified. I made certain that:

- (a) each document was marked as required and stamped with the proper classification designation;
- (b) each document was marked to indicate clearly which portions are classified and which portions are exempt from declassification as set forth in E.O. 13526 § 1.5 (b);
- (c) the prohibitions and limitations on classification specified in E.O. 13526 § 1.7, were adhered to;
- (d) the declassification policies set forth in E.O. 13526 §§ 3.1 and 3.3 were followed; and

(e) any reasonably segregable portion of these classified documents that did not meet the standards for classification under E.O. 13526, were declassified and marked for release, unless withholding was otherwise warranted under applicable law.

Findings of Declarant Regarding Exemption 1

(44) With the above requirements in mind, I personally and independently examined the information withheld from plaintiff pursuant to FOIA Exemption 1. I determined that this classified information is owned by, was produced by or for, and/or is under the control of the U.S. Government. I further determined that the classified information continues to warrant classification at the “Secret” level and is exempt from disclosure pursuant to E.O. 13526, § 1.4, categories (b) foreign government information; (c) intelligence activities (including covert action), intelligence sources or methods, or cryptology; and (d) foreign relations or foreign activities of the United States, including confidential sources.

E.O. 13526, § 1.4(b) – Foreign Government Information

(45) E.O. 13526, § 1.4(b) authorizes the classification of foreign government information. E.O. 13526, § 6.1(s) defines foreign government information as: “(1) information provided to the United States Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence; (2) information produced by the United States Government pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or (3) information received and treated as ‘foreign government information’ under the terms of a predecessor order.”

(46) Many foreign governments do not officially acknowledge the existence of some of their intelligence and security services, or the scope of their activities or the sensitive information generated by them. The free exchange of information between United States intelligence and law enforcement services and their foreign counterparts is predicated upon the understanding that these liaisons, and information exchanged between them, must be kept in confidence.

(47) The release of official United States Government documents that show the existence of a confidential relationship with a foreign government reasonably could be expected to strain relations between the United States and the foreign governments and lead to diplomatic, political, or economic retaliations. A breach of this relationship can be expected to have at least a chilling effect on the free flow of vital information to the United States intelligence and law enforcement agencies, which may substantially reduce their effectiveness. Although the confidential relationship of the United States with certain countries may be widely reported, they are not officially acknowledged.

(48) Disclosure of such a relationship predictably will result in the careful analysis and possible compromise of the information by hostile intelligence services. The hostile service may be able to uncover friendly foreign intelligence gathering operations directed against it or its allies. This could lead to the neutralization of friendly allied intelligence activities or methods or the death of live sources, cause embarrassment to the supplier of the information, or result in economic or diplomatic retaliation against both the United States and the supplier of the information.

(49) Even if the government from which certain information is received is not named in or identifiable from the material it supplies, the danger remains that if the information were to

be made public, the originating government would likely recognize the information as material it supplied in confidence. Thereafter, it would be reluctant to entrust the handling of its information to the discretion of the United States.

(50) The types of classified information provided by foreign government intelligence components can be categorized as: (a) information that identifies a named foreign government and detailed information provided by that foreign government; (b) documents received from a named foreign government intelligence agency and classified “Secret” by that agency; and (c) information that identifies by name, an intelligence component of a specific foreign government, an official of the foreign government, and information provided by that component official to the FBI. A more detailed explanation regarding the categories of foreign government information withheld follows:

(A) ***Foreign Government Identities With Detailed Information:*** Exemption 1 has been asserted to protect information that identifies named foreign governments and detailed information provided by those governments. The detailed information is being withheld to protect the relationship and cooperative endeavors between these foreign governments and the FBI with regard to the pending investigations into the disclosure of classified information that was subsequently published on the WikiLeaks website.

(B) ***Documents Classified “Secret” By A Foreign Government:*** Exemption 1 has been asserted to protect communications and/or documents received from foreign government intelligence agencies and classified “Secret” by the foreign governments. The communications and/or documents relayed information pertinent to the FBI’s on-going investigations into the disclosure of classified information that was subsequently published on the WikiLeaks website.

(C) ***Identity of a Foreign Government Official and Information Provided:***

Exemption 1 has been asserted to protect information received from foreign intelligence agencies, in which the identities of the foreign government officials who provided the information is revealed. The information provided to the FBI was pertinent to the FBI's on-going investigations into the disclosure of classified information that was subsequently published on the WikiLeaks website.

(51) The cooperative exchange of intelligence information between the foreign governments and the FBI was, and continues to be, with the express understanding that the information will be kept classified and not released to the public. Disclosure of the withheld information would violate the FBI's promise of confidentiality. A breach could reasonably be expected to strain relations between the United States and the foreign governments, chill the free flow of vital information to the intelligence and law enforcement agencies, and cause serious damage to the national security and the war on transnational terrorism. This information, which is under the control of the United States Government, is properly classified at the "Secret" level and withheld pursuant to E.O. 13526, § 1.4(b), and is exempt from disclosure pursuant to Exemption 1.

E.O. 13526, § 1.4(c) – Intelligence Activities, Sources and Methods

(52) E.O. 13526, § 1.4(c), exempts intelligence activities (including covert action), intelligence sources or methods, or cryptology from disclosure. An intelligence activity or method includes any intelligence action or technique utilized by the FBI against a targeted individual or organization that has been determined to be of national security interest. An intelligence method is used to indicate any procedure (human or non-human) utilized to obtain information concerning such individual or organization. An intelligence activity or method has

two characteristics. First, the intelligence activity or method -- and information generated by it -- is needed by U. S. Intelligence/Counterintelligence agencies to carry out their missions. Second, confidentiality must be maintained with respect to the activity or method if the viability, productivity and usefulness of its information is to be preserved. Information was withheld pursuant to Exemption 1 to protect intelligence methods utilized by the FBI for gathering intelligence data.

(53) This material is classified because its release would reveal actual intelligence activities and methods used by the FBI against specific targets of foreign counterintelligence investigations or operations; identify a target of a foreign counterintelligence investigation; or disclose the intelligence-gathering capabilities of the activities or methods directed at specific targets. The information obtained from the intelligence activities or methods is very specific in nature, provided during a specific time period, and known to very few individuals.

(54) It is my determination that disclosure of specific information describing the intelligence activities or methods that have been or are being used in this case, and which are still used by the FBI to gather intelligence information in other cases, could reasonably be expected to cause serious damage to the national security for the following reasons: (1) disclosure would allow hostile entities to discover the current intelligence-gathering methods used by the FBI; (2) disclosure would reveal current specific targets of the FBI's national security investigations; and (3) disclosure would reveal the determination of the criteria used and priorities assigned to current intelligence or counterintelligence investigations. With the aid of this detailed information, hostile entities could develop countermeasures which would, in turn, severely disrupt the FBI's intelligence-gathering capabilities. This severe disruption would also result in

severe damage to the FBI's efforts to detect and apprehend violators of the United States' national security and criminal laws.

(55) The FBI protected the following categories of information specific to intelligence activities and methods because disclosure reasonably could be expected to cause serious damage to the national security: (A) detailed intelligence activity information compiled regarding a specific individual or organization of national security interest; (B) file numbers; (C) character and/or title of case; (D) targets of foreign counterintelligence/espionage investigations; (E) acronyms; (F) numerical designators; (G) code words; and (H) intelligence sources. Below is a more detailed discussion of each of these categories.

Detailed Intelligence Activities

(56) The classified information withheld within these documents contains detailed intelligence activity information gathered or compiled by the FBI on a specific individual or organization of national security interest. The disclosure of this information could reasonably be expected to cause serious damage to the national security, as it would: (a) reveal the actual intelligence activity or method utilized by the FBI against a specific target; (b) disclose the intelligence-gathering capabilities of the method; and (c) provide an assessment of the intelligence source penetration of a specific target during a specific period of time. This information is properly classified at the "Secret" level and withheld pursuant to E.O. 13526, § 1.4(c), and is exempt from disclosure pursuant to Exemption 1.

File Numbers

(57) The classified information withheld includes FBI file numbers assigned to specific intelligence activities, including channelization and dissemination instructions. Their release would lead to exposure of the particular intelligence activities and methods at issue.

Individual file numbers are assigned by FBIHQ and field offices and contain a geographical prefix or the originating office and case number, which includes the numerical characterization of the type of investigation followed by a chronological number assigned to a specific investigation/activity.

(58) The disclosure of an intelligence file number in the aggregate will enable a hostile analyst to attribute any information released from the documents containing such a file number to that particular file. A hostile analyst can identify the specific intelligence activity by supplying further missing pieces. Hence, a partial mosaic of the activity begins to appear as more information is identified with the file leading to the exposure of actual current activities or methods. Disclosure of file numbers will allow a hostile analyst, or anyone not privileged to this information, to patch bits and pieces of information together until the actual use of the application of the source or method can be determined. The identification of these intelligence methods, which continue to furnish positive intelligence information to this day, will severely limit its application. In addition, disclosure will inform hostile intelligence of the possible range of our intelligence capabilities, as well as the probable intelligence that the FBI has gathered, or can collect, concerning them. This knowledge provides potential or actual violators of the United States' national security laws a means of deflection or avoidance of lawful regulations. Disclosure will allow countermeasures to be implemented, making future operations more difficult, and compromise other ongoing planned intelligence operations. Accordingly, the release of the file numbers can lead to the exposure of the actual intelligence activity or method utilized in FBI investigations, and can reasonably be expected to cause serious damage to national security. The file numbers are properly classified at the "Secret" level and withheld pursuant to E.O. 13526, § 1.4(c), and is exempt from disclosure pursuant to Exemption 1.

Character and/or Title of Case

(59) The classified information withheld identifies the character and/or title of the case for a specific type of intelligence activity directed at a specific target of national security interest. Disclosure of the characterization and/or title of the case could reasonably be expected to cause serious damage to the national security, as it would (a) disclose a particular intelligence or counterintelligence investigation; (b) disclose the nature, scope or thrust of the investigation; and (c) reveal the manner of acquisition of the intelligence or counterintelligence information. This information is properly classified at the “Secret” level and withheld pursuant to E.O. 13526, § 1.4(c), and is exempt from disclosure pursuant to Exemption 1.

Targets of Foreign Counterintelligence/Espionage Investigations

(60) The classified information withheld identifies targets of FBI foreign counterintelligence/espionage investigations. The disclosure of this information could reasonably be expected to cause serious damage to the national security, as it would: (a) reveal the actual intelligence activity or method utilized by the FBI against a specific target; (b) disclose the intelligence-gathering capabilities of the method; and (c) provide an assessment of the intelligence source penetration of a specific target during a specific period of time.

(61) It is my determination that the release of this information could permit hostile individuals and foreign governments to appraise the scope, focus, location, target and capabilities of the FBI's intelligence-gathering methods and activities, and allow hostile agents to devise countermeasures to circumvent these intelligence activities or methods and render them useless in providing intelligence information. This would severely disrupt the FBI's intelligence-gathering capabilities. This information is properly classified at the “Secret” level and withheld pursuant to E.O. 13526, § 1.4(c), and is exempt from disclosure pursuant to Exemption 1.

Acronyms

(62) The classified information withheld contains acronyms that identify specific intelligence methods utilized by the FBI in its intelligence activities. The disclosure of this information could permit hostile analysts to ascertain the specific nature of the FBI's investigations. This information is properly classified at the "Secret" level and withheld pursuant to E.O. 13526, § 1.4(c), and is exempt from disclosure pursuant to Exemption 1.

Numerical Designators

(63) The classified information withheld contains numerical designators for sensitive non-live sources. The numerical designator serves as a singular identifier for the actual intelligence method utilized to provide information. A singular identifier is any word, term, or phrase which is used in lieu of the true nature of a source. The numerical designator is assigned to a specific intelligence method which is unique to -- and solely used for -- this source. The numerical designator is assigned sequentially and is usually prefixed with the geographic location of the FBI office which is operating that particular intelligence method. As a result, the withheld information is properly classified at the "Secret" level and withheld pursuant to E.O. 13526, § 1.4(c), and is exempt from disclosure pursuant to FOIA Exemption 1.

Code Words

(64) The classified information withheld consists of code words that have never been publicly revealed and which, if disclosed, will reveal a specific intelligence subject of continuing value to the FBI in its ongoing investigations. Code words are unique and assigned solely to one particular intelligence subject. They are used in lieu of the actual name, description, and information concerning a specific investigation of national security interest. The withheld code words are sensitive and synonymous with on-going investigations that are still active today in

collecting intelligence information. Public disclosure of a code word will allow a hostile analyst, or one not privileged to this code word, to patch bits and pieces of information together until the actual use of this application can be determined. In addition, the disclosure of a code word will inform hostile intelligence of the possible range of our intelligence capabilities, as well as the probable intelligence that the FBI has gathered, or can collect, concerning them. This information is properly classified at the "Secret" level and withheld pursuant to E.O. 13526, § 1.4(c), and is exempt from disclosure pursuant to Exemption 1.

Intelligence Sources

(65) An intelligence source who requires continued classification is an individual who provided or is currently providing information that pertains to national security matters, the disclosure of which could reasonably be expected to result in serious damage to the FBI's intelligence and counterintelligence-gathering capabilities.

(66) My review determined that the information contained in these documents, which pertains to classified intelligence sources, is likely to identify these sources if released. The withheld information and material provided by -- or which pertains to -- these sources is specific and, if disclosed, reasonably could be expected to reveal the identities of the contributing sources. I considered a number of factors in reaching this conclusion, including most importantly, the damage to the national security that would result by publicly identifying sources utilized in intelligence investigations, and the FBI's ability to protect and recruit intelligence sources in the future.

(67) Disclosure of the identities of FBI intelligence sources, regardless of whether they are active or inactive, alive or deceased, can reasonably be expected to cause current and potential intelligence sources to fear that their identities will be publicly revealed at some point,

despite the FBI's express or implied assurances of confidentiality. The disclosure of sources' identities could jeopardize the emotional and physical well-being of the source or the sources' family or associates, and/or subject them to public ridicule and ostracism.

(68) Thus, the release of information I determined to be source-identifying could reasonably be expected to cause damage to the national security by causing current intelligence sources to cease providing information, and discourage potential intelligence sources from cooperating with the FBI for fear their identities would be publicly revealed at some point. Such a source reaction would eliminate one of the most crucial means of collecting intelligence information and, therefore, severely hamper the FBI's law enforcement efforts to detect and apprehend individuals who seek to damage the national security through violation of the United States criminal and national security laws. The classified information provided by intelligence sources on certain pages is properly classified at the "Secret" level and withheld pursuant to E.O. 13526, § 1.4(c), and is exempt from disclosure pursuant to Exemption 1.

(69) The following categories of intelligence source information were withheld: (1) detailed intelligence source information; (2) intelligence source symbol numbers; (3) intelligence source symbol numbers with character of case; and (4) source file numbers. Below is a more detailed discussion of each of these categories.

(70) Detailed Intelligence Source Information: The classified information withheld contains detailed information provided by human intelligence sources. This information is specific in nature and reflects the specific vantage point of the source(s). If disclosed, this information would identify the intelligence source(s). As a result, this information is properly classified at the "Secret" level and withheld pursuant to E.O. 13526, § 1.4(c), and is exempt from disclosure pursuant to Exemption 1.

(71) Intelligence Source Symbol Numbers: The classified information withheld contains numerical designators for intelligence sources. Numerical designators serve as a singular identifier for an intelligence source used to provide information for a specific individual or organization determined to be of national security interest. A singular identifier is any word, term or phrase which could identify an intelligence source, either if released by itself or in the aggregate. This includes code names or sources, numerical designators and file numbers. A singular identifier is used in lieu of the true identity of a source. The numerical designator is assigned to a specific source and is unique to, and solely used for, this source. The numerical designator is assigned sequentially and is typically prefixed with the particular FBI field office from which the source is operated. The classified symbol numbers withheld relate to sources who provided information of value on individuals and/or organizations of national security interest. The disclosure of this information could permit a hostile analyst to correlate the documents and whatever information that can be gleaned from the documents. By matching source identifiers, such as file numbers and numerical designators, with bits and pieces of other inadvertently released information, one can begin to discern the true identity of the intelligence sources. Public identification of a source will limit the effectiveness of these sources, and also have a significant chilling effect on the FBI's ability to recruit future sources. This information is properly classified at the "Secret" level and withheld pursuant to E.O. 13526, § 1.4(c), and is exempt from disclosure pursuant to Exemption 1.

(72) Intelligence Source Symbol Numbers with Character of Case: The classified information contains the character of the case and a numerical designator, which serves as a singular identifier for an intelligence source. The justifications for withholding this information is the same as ¶¶ 57-59 and 71, supra. This information is properly classified at the "Secret"

level and withheld pursuant to E.O. 13526, § 1.4(c), and is exempt from disclosure pursuant to Exemption 1.

(73) Intelligence Source File Numbers: The classified information withheld contains file numbers assigned by FBI field offices to intelligence sources for the channelization and dissemination of intelligence information gathered by or attributed to the sources. See ¶¶ 57-58 supra. The release of these file numbers could reasonably be expected to cause serious damage to the national security, as it would result in the disclosure of the sources' identities, which thereby would neutralize the sources and compromise information previously provided by the sources. As a result, this information is properly classified at the "Secret" level and withheld pursuant to E.O. 13526, § 1.4(c), and is exempt from disclosure pursuant to Exemption 1.

E.O. 13526, § 1.4(d) – Foreign Relations or Foreign Activities

(74) E.O. 13526, § 1.4 (d), exempts foreign relations or foreign activities of the United States, including confidential sources. The classified information withheld contains sensitive intelligence information gathered by the United States either about or from a foreign country. This information is sensitive due in part to the delicate nature of international diplomacy, and must be handled with care so as not to jeopardize the fragile relationships that exist between the United States and certain foreign governments.

(75) The unauthorized disclosure of information concerning foreign relations or foreign activities of the United States can reasonably be expected to lead to diplomatic or economic retaliation against the United States; identify the target, scope, or time frame of intelligence activities of the United States in or about a foreign country, which may result in the curtailment or cessation of these activities; enable hostile entities to assess United States intelligence gathering activities in or about a foreign country and devise countermeasures against

these activities; or compromise cooperative foreign sources, which may jeopardize their safety and curtail the flow of information from these sources. Thus, the information about foreign relations or foreign activities which are withheld by the FBI is properly classified at the "Secret" level and withheld pursuant to E.O. 13526, § 1.4 (d), and is exempt from disclosure pursuant to Exemption 1.

Defendant's Burden of Establishing Exemption 1 Claims

(76) The information withheld in this case pursuant to Exemption 1 was examined in light of the body of information available to me concerning the national defense and foreign relations of the United States. This information was not examined in isolation. Instead, it was evaluated with careful consideration given to the impact that its disclosure will have on other sensitive information contained elsewhere in the United States intelligence community's files. Equal consideration was given to the impact that other information either in the public domain or likely known or suspected by present or potential adversaries of the United States, would have upon the information I examined.

(77) In those instances where, in my judgment, the disclosure of this information could reasonably be expected to cause serious damage to the national security, and its withholding outweighed the benefit of disclosure, I exercised my prerogative as an original classification authority and designated that information as classified in the interest of national security, and invoked Exemption 1 of the FOIA to prevent disclosure. Likewise, the justifications for the withheld classified information were prepared with the intent that they be read with consideration given to the context in which the classified information is found. This context includes not only the surrounding unclassified information, but also other information already in the public domain, as well as information likely known or suspected by other hostile intelligence

entities. It is my judgment that any greater specificity in the descriptions and justifications set forth with respect to information relating to foreign activities and intelligence sources and methods of the United States could reasonably be expected to jeopardize the national security of the United States.

EXEMPTION 3 – INFORMATION EXEMPTED FROM DISCLOSURE BY STATUTE

(78) Exemption 3 exempts from disclosure information that is:

specifically exempted from disclosure by statute ... provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld.

5 U.S.C. § 552(b)(3).

(79) The FBI has determined that an Exemption 3 statute applies and protects responsive information from the pending investigative files from disclosure. However, to disclose which statute or further discuss its application publicly would undermine interests protected by Exemption 7(A), as well as by the withholding statute. I have further discussed this exemption in my *in camera*, *ex parte* declaration, which is being submitted to the Court simultaneously with this declaration (“2nd Hardy Decl.”)

EXEMPTION 5 – PRIVILEGED INFORMATION

(80) Exemption 5 exempts from disclosure:

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

5 U.S.C. § 552(b)(5).

(81) Exemption 5 has been construed to exempt documents or information normally privileged in the civil discovery context, and incorporates the attorney work product, attorney-

client, and deliberative process privileges. Generally, the attorney work product privilege protects documents and other memoranda prepared by an attorney or under the direction of an attorney as part of, or in reasonable anticipation of litigation. The attorney-client privilege protects confidential communications from a client to an attorney and from an attorney to a client for the purpose of seeking and providing legal advice. The privilege covers client-supplied information and opinions given by an attorney based on and reflecting that information. The deliberative process privilege protects predecisional, deliberative communications that are part of a process by which agency decisions are made. It protects materials prepared as part of an agency decisionmaker's formulation of opinions, advice, evaluations, deliberations, policies, proposals, conclusions, or recommendations.

Attorney Work Product Privilege

(82) Exemption 5 has been asserted to protect material protected by the attorney work product privilege. The attorney work product privilege protects such tangible and intangible items as interviews, memoranda, correspondence, mental impressions, and personal beliefs prepared or developed by an attorney in anticipation of litigation.⁹ The privilege is predicated on the recognition that proper preparation of a case depends on an attorney's ability to assemble information, sort relevant from irrelevant facts, and prepare his/her legal theories and strategies without intrusive or needless scrutiny. The FBI has relied on this privilege to protect materials created by and communications between FBI, DOJ, and other Government attorneys in relation to the pending prosecution of PFC Bradley Manning. The privilege also protects materials created or compiled by such attorneys in anticipation of potential other prosecutions arising out of the pending investigations into the disclosure of classified information that was subsequently

⁹ For purposes of the attorney work product privilege, litigation is anticipated when the Government is investigating specific wrongdoing in an attempt to gather evidence and build a case against the suspected wrongdoer.

published on the WikiLeaks website. Accordingly, the FBI properly withheld this information pursuant to Exemption 5.

Attorney-Client Privilege

(83) Exemption 5 has also been asserted to protect privileged attorney-client communications. The attorney-client privilege is appropriately asserted to protect confidential communications between a client seeking legal advice from a professional legal adviser in his/her capacity as a lawyer. Such communications are permanently protected from disclosure by the legal adviser unless the client waives the protection. This privilege encompasses confidential communications made to an agency attorney by decision-making personnel as well as lower echelon employees who possess information relevant to an attorney's advice-rendering function. Disclosure of the communications between FBI attorneys and their clients would impede the full disclosure of all of the information that relates to the client's reasons for seeking legal advice, which is necessary if the professional mission is to be accomplished.

(84) The FBI has protected communications between and among FBI counsel and their FBI clients and employees that reflect the seeking and/or providing of legal advice with respect to aspects of the ongoing investigations and related pending/prospective prosecutions. The communications being protected were made in confidence. Disclosure of the two-way communications between the FBI attorneys and their clients would inhibit clients from being completely candid with their attorneys in relation to the issues about which they are seeking legal advice. Such candor and full disclosure is necessary in order to ensure that thorough and sound legal advice is provided.

Deliberative Process Privilege

(85) Finally, Exemption 5 has been asserted to protect deliberative materials. The general purpose of the deliberative process privilege is to prevent injury to the quality of agency decisions. Thus, material that contains or was prepared in connection with the formulation of opinions, advice, evaluations, deliberations, policies, proposals, conclusions, or recommendations may properly be withheld. Disclosure of this type of information would have an inhibiting effect upon agency decision-making and the development of policy because it would chill full and frank discussions between agency personnel and decision makers regarding a decision. If agency personnel know that their preliminary impressions, opinions, evaluations, or comments would be released for public consumption, they would be less candid and more circumspect in expressing their thoughts, which would impede the fulsome discussion of issues necessary to reach a well-reasoned decision.

(86) In order to invoke the deliberative process privilege, the protected information must be both “predecisional” and “deliberative.” Information is “predecisional” if it temporally precedes the decision or policy to which it relates. It is “deliberative” if it played a direct part in the decision-making process because it consists of recommendations or opinions on legal or policy matters, or reflects the give-and-take of the consultative process.

(87) The deliberative process privilege applies to documents in the pending investigative files that reflect decision-making by the FBI, alone or in conjunction with other DOJ components, regarding the scope and focus of the investigations, as well as pending and prospective prosecutions. The materials are predecisional in that they precede final investigative and/or prosecutive decisions, and deliberative in that they played, and/or continue to play, a part

in the process by which decisions were made about the scope and focus of the investigations and pending/prospective prosecutions.

EXEMPTIONS 6 AND 7(C) – UNWARRANTED INVASIONS OF PERSONAL PRIVACY

(88) Exemption 6 exempts from disclosure:

personnel and medical files and similar files when the disclosure of such information would constitute a clearly unwarranted invasion of personal privacy.

5 U.S.C. § 552(b)(6).

(89) Exemption 7(C) exempts from disclosure:

records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information . . . could reasonably be expected to constitute an unwarranted invasion of personal privacy.

5 U.S.C. § 552(b)(7)(C).

(90) When withholding information pursuant to these two exemptions, the FBI is required to balance the privacy interests of the individuals mentioned in these records against any public interest in disclosure.¹⁰ For purposes of this analysis, a public interest exists when information would shed light on the FBI's performance of its mission to protect and defend the United States against terrorist and foreign intelligence threats, to uphold and enforce the criminal laws of the United States, and to provide leadership and criminal justice services to federal, state, municipal, and international agencies and partners. In each instance where information was withheld pursuant to Exemptions 6 and 7(C), the FBI determined that the individuals' privacy interests outweighed the public interest, if any, in the information.

¹⁰ The FBI's practice is to assert Exemption 6 in conjunction with Exemption 7(C). Although the balancing test for Exemption 6 uses a "*would* constitute a clearly unwarranted invasion of personal privacy" standard and the test for Exemption 7(C) uses the lower standard of "*could* reasonably be expected to constitute an unwarranted invasion of personal privacy," the analysis and balancing required by both exemptions is sufficiently similar to warrant a consolidated discussion. The privacy interests are balanced against the public's interest in disclosure under the analysis of both exemptions.

**Names and/or Identifying Information of
FBI Special Agents and Support Personnel**

(91) Exemptions 6 and 7(C) were applied, at times in conjunction with Exemption 7(F), to protect the names and identifying information of FBI Special Agents (“SAs”) who are responsible for conducting, supervising, and/or maintaining the investigative activities in the pending files. The FBI SAs who are investigating these cases have privacy interests in avoiding publicity, adverse or otherwise, regarding any particular investigation, that may seriously impair their effectiveness in conducting these and future investigations. FBI SAs conduct official inquiries into violations of various criminal statutes, as well as counter-terrorism and national security investigations. They come into contact with all strata of society, conduct searches and make arrests, both of which result in reasonable but nonetheless serious disturbances in the lives of individuals. It is possible for a person targeted by such law enforcement action to carry a grudge which may last for years, and seek revenge on the SAs involved in the investigation. The publicity associated with the release of the identity of an FBI SA’s name in connection with a particular investigation could trigger hostility towards the SA by such persons. Finally, privacy considerations protect FBI SAs from unnecessary, unofficial questioning as to the conduct of an investigation, whether or not they are currently employed by the FBI.

(92) The names of FBI support personnel have also been withheld pursuant to Exemptions 6 and 7(C), at times in conjunction with Exemption 7(F). Support personnel are assigned to handle tasks relating to FBI investigations. These individuals are in positions to access information concerning official law enforcement, counter-terrorism and national security investigations. They could therefore become targets of harassing inquiries for unauthorized access to FBI investigations if their identities were released. Accordingly, FBI support personnel

have personal privacy interests in the non-disclosure of their names which are associated with the investigation in this case.

(93) The FBI examined the documents containing the names and/or identifying information of FBI SAs and support personnel to determine whether there was any public interest that outweighs the substantial privacy interests in the responsive records. The FBI could not identify any discernible public interest. In particular, the FBI could not determine how the disclosure of the names and identifying information of the FBI SAs and support personnel would shed any light on the operations and activities of the FBI. Thus, the FBI determined that the privacy interests of the SAs and support personnel in protecting their names and identifying information from disclosure outweighed any public interest in disclosure, and that disclosure of the names and identifying information of the FBI SAs and support personnel would constitute a clearly unwarranted and unwarranted invasion of personal privacy.¹¹

**Names and/or Identifying Information of
Non-FBI Federal Employees**

(94) Exemptions 6 and 7(C) have been applied, at times in conjunction with Exemption 7(F), to protect the names and identifying information of non-FBI federal government employees (including agents) whose names appear in the pages.

(95) The relevant inquiry here is whether public access to this information would violate a viable privacy interest of the subject of such information. Disclosure of this identifying information could subject the personnel to unauthorized inquiries and harassment, which would constitute a clearly unwarranted invasion of personal privacy. The rationale for protecting non-FBI federal employees is the same as that for FBI agents and employees.

¹¹ For the convenience of the Court, rather than repeat the phrase “clearly unwarranted invasion of personal privacy” under the standard of Exemption 6 and “an unwarranted invasion of personal privacy” under the standard of Exemption 7(C) every time we assert these two exemptions, we will simply use the phrase “clearly unwarranted and unwarranted invasion of personal privacy” to refer to both standards.

(96) After identifying the substantial privacy interests of the non-FBI federal employees, the FBI balanced those interests against the public interest in disclosure. The FBI could identify no discernible public interest in the disclosure of this information because the disclosure of non-FBI federal employees' names and/or identifying information will not shed light on the operations and activities of the FBI. Accordingly, the FBI determined that the disclosure of this information would constitute a clearly unwarranted and unwarranted invasion of personal privacy.

**Names and/or Identifying Information of
Third Parties Merely Mentioned In Responsive Documents**

(97) Exemptions 6 and 7(C) have been applied to protect the names and/or identifying information of third parties that were merely mentioned in the documents responsive to plaintiff's request. These individuals are not of investigative interest to the FBI. Release of this type of information about private citizens, without notarized authorizations permitting such a release, violates these individuals' substantial privacy interests. If the FBI disclosed their names and/or other personal information, the disclosure would reveal that these third parties were at one time connected with an FBI investigation in some way. Disclosure of their identities could subject these individuals to possible harassment or criticism, and focus derogatory inferences and suspicion on them.

(98) The FBI also examined the records at issue to determine whether there was any public interest that outweighed the substantial privacy interests of the third parties merely mentioned in the responsive records. The FBI could not identify any discernible public interest. In particular, the FBI could not determine how the disclosure of the names and/or identifying information of these individuals would shed any light on the operations and activities of the FBI. Thus, the FBI determined that these individuals' privacy interests substantially outweighed any

public interest in disclosure, and that disclosure of the names and/or identifying information of the third parties merely mentioned in FBI criminal investigation files would constitute a clearly unwarranted and unwarranted invasion of privacy.

**Names and/or Identifying Information of
Third Parties Who Provided Information to the FBI**

(99) Exemptions 6 and 7(C) have been applied, at times in conjunction with Exemptions 7(D) and/or 7(F), to protect the names and/or identifying information of individuals who were interviewed by the FBI during the course of the FBI's investigations of the disclosure of classified information that was subsequently published on the WikiLeaks website. Identifying information withheld concerning these third parties may include addresses, dates of birth, social security numbers, and other personally identifying information.

(100) The FBI has found that information provided by individuals during an interview is one of the most productive investigative tools used by law enforcement agencies. The largest roadblock to successfully obtaining the desired information through an interview is fear by the interviewee that his/her identity will possibly be exposed and consequently he/she could be harassed, intimidated, or threatened with legal, economic reprisal or possible physical harm. To surmount these obstacles, persons interviewed by the FBI must be assured that their names and personal identifying information will be held in the strictest confidence. The continued access by the FBI to persons willing to honestly relate pertinent facts bearing upon a particular investigation far outweighs any benefit plaintiff might derive from being furnished the names of those who cooperated with the FBI.

(101) Thus, the FBI has determined that the third party interviewees maintain a substantial privacy interest in not having their identities disclosed. After identifying the substantial privacy interests of the third parties interviewed during the course of the FBI's

investigations of the disclosure of classified information that was subsequently published on the WikiLeaks website, the FBI balanced their privacy interests against the public interest in the disclosure. The FBI could identify no discernible public interest in the disclosure of third parties' names and identifying information because it would not shed light on the operations and activities of the FBI. Accordingly, the FBI concluded that the disclosure of this information would constitute a clearly unwarranted and unwarranted invasion of their personal privacy. The FBI properly withheld this information pursuant to Exemptions 6 and 7(C).

**Names and/or Identifying Information Concerning
Third Parties of Investigative Interest**

(102) Exemptions 6 and 7(C) have been asserted to protect the names and/or identifying information of third party individuals who are of investigative interest to the FBI and/or other law enforcement agencies. Identifying information withheld concerning these third parties may include addresses, dates of birth, social security numbers, and other personally identifying information. Being linked with any law enforcement investigation carries a strong negative connotation and a stigma. To release the identities of these individuals to the public could subject them to harassment or embarrassment, as well as undue public attention. Accordingly, the FBI has determined that these individuals maintain a substantial privacy interest in not having their identities disclosed. In deciding whether to release the names and personal information concerning these third parties, the public's interest in disclosure was balanced against their privacy interests. It was determined that this information would not enlighten the public on how the FBI conducts its internal operations and investigations. Accordingly, the FBI concluded that the disclosure of this information would constitute a clearly unwarranted and unwarranted invasion of their personal privacy. The FBI properly withheld this information pursuant to Exemptions 6 and 7(C).

EXEMPTION 7(D) – CONFIDENTIAL SOURCE MATERIAL

(103) Exemption 7(D) exempts from disclosure:

records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information . . . could reasonably be expected to disclose the identity of a confidential source, including a State, local or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of a record or information compiled by a criminal law enforcement authority in the course of a criminal investigation or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source.

5 U.S.C. § 552(b)(7)(D). Exemption 7(D) has been applied, at times, in conjunction with Exemptions 6, 7(C), and/or 7(F).

(104) Numerous informants report to the FBI on a regular basis and are informants in the common meaning of the term. Some sources provide information under an express assurance of confidentiality and others are interviewed during the course of an investigation under circumstances from which an assurance of confidentiality can reasonably be inferred. These individuals are considered to be confidential informants or sources, because they furnish information only with the understanding that their identities and the information they provided will not be divulged outside the FBI. Information provided by these individuals is singular in nature, and if released, could reveal their identities.

(105) During the course of the FBI's investigations, FBI SAs have sought and continue to seek the assistance of various individuals to obtain information in aid of the investigations. Information has been provided by individuals under both express and implied assurances of confidentiality.

(106) These individuals have been placed directly in positions that could subject them to acts of reprisal or harassment, or that could draw an unnecessary amount of public attention if

the FBI disclosed their cooperation. The FBI has learned through experience that individuals who provide information about subjects under investigation must be able to do so without fearing that their identities and the information they provided will be disclosed outside their confidential relationship with the FBI. Individuals who provide investigative information must be free to furnish that information with complete candor and without the understandable tendency to hedge or withhold information out of fear of public disclosure. Those individuals who have provided information in these investigations must be secure in the knowledge that their assistance and their identities will be held in confidence. This is of particular importance here, where the Government has cause to be concerned about potential harassment and threats to individuals who have cooperated in these investigations.

(107) Exemption 7(D) has been asserted to protect various categories of information responsive to plaintiff's FOIA request. Some of those categories are identified and described below. However, the FBI is unable to publicly identify and describe some of the categories because publicly disclosing such information would adversely affect the active, on-going criminal investigations in this case by revealing the nature, scope, focus, and conduct of the investigations, including the types and origins of sources upon which the FBI is relying. Consequently, public disclosure of any more detailed information about these categories at this time would undermine the very interests the FBI seeks to protect through application of Exemption 7(A) to the responsive records in this case. The categories of information protected by Exemption 7(D) that cannot be publicly disclosed are discussed in my *in camera, ex parte* declaration. See 2nd Hardy Decl.

**Names, Identifying Information, and/or Information
Provided Under Implied Assurances of Confidentiality**

(108) Exemption 7(D) has been asserted, in conjunction with Exemptions 6, 7(C), and/or 7(F) to protect the names and/or identifying information about cooperating witnesses who have provided information to the FBI under implied assurances of confidentiality during the course of the FBI's investigations into the disclosure of classified information that was subsequently published on the WikiLeaks website. Exemption 7(D) has also been asserted to protect the information these individuals provided to the FBI under implied assurances of confidentiality. These individuals provided specific and detailed information that is singular in nature about the matters under investigation. The disclosure of their identities could have disastrous consequences. Given the nature of these investigations and also prior incidents of harassment and threats toward individuals associated with these investigations, the FBI has legitimate cause to conclude that disclosure of the identities of cooperating witnesses could subject them to reprisals and have a chilling effect on future cooperation by them in these or other cases. These individuals have provided information of value to the FBI in relation to these investigations, and in doing so, have placed themselves in harm's way should their cooperation with/participation in these investigations become publicly known.

(109) Accordingly, witnesses who have cooperated in the on-going investigations under implied assurances of confidentiality, as well as the information they provided, are entitled to protection and the FBI has properly invoked Exemption 7(D), in conjunction with Exemptions 6, 7(C), and/or 7(F), to protect this information.

**Names, Identifying Information, and/or Information
Provided Under Express Assurances of Confidentiality**

(110) Exemption 7(D) has been asserted, in conjunction with Exemptions 6, 7(C), and/or 7(F) to protect the names and/or identifying information about cooperating witnesses who have provided information to the FBI under express assurances of confidentiality during the course of the FBI's investigations into the disclosure of classified information that was subsequently published on the WikiLeaks website. Exemption 7(D) has also been asserted to protect the information these individuals provided to the FBI under express assurances of confidentiality. These individuals provided specific and detailed information that is singular in nature about the matters under investigation. Prior to conducting interviews, the FBI expressly promised these individuals that their identities and the information they provided would not be disclosed. This is evidenced by the insertion of the words "PROTECT IDENTITY" when these individuals' names are referenced in the files. The FBI uses "PROTECT IDENTITY" as a positive indication of an express assurance of confidentiality. These individuals cooperated with the FBI and provided valuable information about the criminal activities currently under investigation, and some are continuing to do so, with the express understanding that their identities and the information they provided would only be for law enforcement purposes and would not be disclosed to the public.

(111) These individuals provided, and continue to provide, valuable information that is detailed and singular in nature. The disclosure of their identities could have disastrous consequences. Given the nature of these investigations and also prior incidents of harassment and threats toward individuals associated with these investigations, the FBI has legitimate cause to conclude that disclosure of the identities of cooperating witnesses could subject them to reprisals and have a chilling effect on future cooperation in these or other cases. These

individuals have provided information of value to the FBI in relation to these investigations, and in doing so, have placed themselves in harm's way should their cooperation with/participation in these investigations become publicly known. In addition, disclosure of the identities of these individuals who cooperated with the FBI under express assurances of confidentiality has wider implications. If the FBI were to disclose the identities of sources who entered into express agreements of confidentiality, that revelation would have a chilling effect on the activities and cooperation of other sources in the future. The FBI has found that it is only with the understanding of complete confidentiality that the aid of such sources can be enlisted, and that only through this confidence can these sources be persuaded to continue to provide valuable assistance in the future. Thus, the FBI properly asserted Exemption 7(D), in conjunction with Exemptions 6, 7(C), and/or 7(F), to protect the identities of, and information provided by, individuals who were expressly promised confidentiality in relation to their cooperation in these investigations.

EXEMPTION 7(E) – INVESTIGATIVE TECHNIQUES AND PROCEDURES

(112) Exemption 7(E) exempts from disclosure:

records or information compiled for law enforcement purposes, but only to the extent that production of such law enforcement records or information ... would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law.

5 U.S.C. § 552(b)(7)(E).

(113) Exemption 7(E) has been asserted to protect records compiled in these investigations to prevent the disclosure of law enforcement techniques and procedures being used in these investigations, and of guidelines for the investigations and any pending or prospective prosecutions. The types of information being protected by Exemption 7(E) are

generally categorized below. Providing further details about the techniques, procedures, and/or guidelines used in these investigations and any pending prosecutions would disclose the very information the FBI seeks to protect through Exemption 7(E), would risk circumvention of the law, and would trigger harm under Exemption 7(A) by prematurely revealing the scope and direction of the ongoing investigations and the focus of pending and prospective prosecutions.

Investigative Techniques and Procedures

(114) Exemption 7(E) has been asserted to protect procedures and techniques used by FBI SAs to conduct criminal and national security investigations. Disclosure of this information could enable subjects of these and other FBI investigations to circumvent similar currently-used law enforcement techniques and procedures. The relative benefit of these techniques and procedures could be diminished if the actual techniques and procedures were revealed here. This, in turn, could facilitate the accumulation of information by subjects in these on-going investigations as well as other investigations regarding the circumstances under which these techniques and procedures were used or requested and the value of the information obtained. Release of this type of information could enable the subjects of these investigations and other investigations to educate themselves about the law enforcement investigative techniques and procedures employed in order to locate and apprehend individuals and gather and analyze evidence. This would allow such individuals to take countermeasures to circumvent the effectiveness of these techniques and procedures and to continue to violate the law. Thus, the FBI has properly protected this information from disclosure pursuant to Exemption 7(E).

Location and Identity of FBI Units

(115) Exemption 7(E) has also been asserted to protect methods and techniques involving the location and identity of FBI units that are or have been involved in the underlying

investigations. The office locations and units are usually found in administrative headings of internal FBI documents. These headings identify the location of the office and unit that originated or received documents. Disclosure of the location of the units conducting the investigations would reveal the targets, the physical areas of interest of the investigation, and/or the areas of analysis being conducted in the case. When taken together with any other locations identified, this could establish a pattern or “mosaic” that identification of a single location would not. If the locations are clusters in a particular area, it would allow individuals to avoid or circumvent these locations, especially if one or more location appeared with frequency or in a pattern. This would disrupt the method of the investigative process and deprive the FBI of valuable information. The withholding of the identities of units is justified under a similar rationale. Once identified, the units’ areas of expertise become known and an individual would be aware of exactly what the FBI’s interest is and what types of procedures and techniques are being employed in these investigations. For example, knowing that the investigation involves a unit responsible for financial analysis is quite different than knowing that the investigation involves a unit responsible for explosives analysis. The revelation of the involvement of one or more units of differing expertise is critical information that can allow the adjustment of behaviors and activities to avoid detection. This knowledge could allow an individual to avoid activities in the area of the unit’s expertise and circumvent law enforcement. Because disclosure of this information could reasonably be expected to impede the FBI’s effectiveness and aid in the circumvention of the law, the FBI has properly withheld this information pursuant to Exemption 7(E).

**Dates and Types of Investigations (Preliminary or Full Investigations)
and Bases for Initiation**

(116) Exemption 7(E) has been asserted to protect from disclosure information pertaining to the types and dates of investigations referenced in the records at issue in this case, as well as information about the bases for initiation of these investigations. Specifically, the information withheld, when referenced in connection with an actual investigation and not in general discussion, pertains to the type of investigation, whether it is a “preliminary” or “full” investigation, the date it was initiated, and the bases for initiation of the particular investigation. Disclosure of this information would allow individuals to know the types of activities that would trigger a full investigation as opposed to a preliminary investigation and the particular dates that the investigation covers, which would allow individuals to adjust their behavior accordingly. Moreover, the knowledge that a specific activity in general warrants investigation could likewise cause individuals to adjust their conduct to avoid detection. Because disclosure of this information could reasonably be expected to impede the FBI’s effectiveness and potentially aid in circumvention of the law, the FBI has properly withheld this information pursuant to Exemption 7(E).

EXEMPTION 7(F) – DANGER TO LIFE OR PHYSICAL SAFETY

(117) Exemption 7(F) exempts from disclosure:

records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information . . . could reasonably be expected to endanger the life or physical safety of any individual.

5 U.S.C. § 552(b)(7)(F).

(118) Exemption 7(F) has been asserted, at times in conjunction with Exemptions 6, 7(C), and/or 7(D), to protect the identities of FBI and other government employees working on

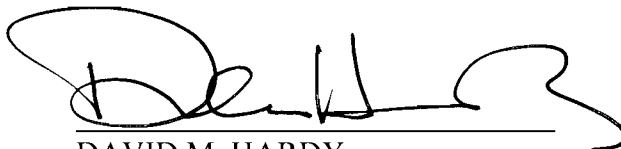
these investigations, as well as individuals who have cooperated in these investigations. Government employees who are working on these cases, or have worked on them in the past, have been threatened and harassed in conjunction with these cases. Based on these experiences, the FBI can reasonably expect that disclosure of the identities of individuals associated with these investigations, including FBI and government employees, cooperating witnesses, and informants, could endanger their lives or physical safety. Accordingly, the FBI has properly withheld this information pursuant to Exemption 7(F), at times in conjunction with Exemptions 6, 7(C), and/or 7(D).

CONCLUSION

(119) The FBI has carefully examined the responsive documents in this case and has determined that all information responsive to plaintiff's request is located in files pertaining to several ongoing, active investigations. The FBI has further determined that all responsive information is exempt from disclosure under Exemption 7(A) because disclosure of any information could reasonably be expected to interfere with the ongoing investigations, as well as pending and prospective prosecutions. The FBI has further determined that the responsive records in this case are also exempt under one or more other exemptions, including Exemptions 1, 3, 5, 6, 7(C), 7(D), 7(E), and/or 7(F). Once Exemption 7(A) is applied, in conjunction with any other applicable exemptions, there is no reasonably segregable information that can be released at this time.

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct, and that Exhibits A through D attached hereto are true and correct copies.

Executed this 30th day of January, 2013.

A handwritten signature in black ink, appearing to read 'D. Hardy', written over a horizontal line.

DAVID M. HARDY
Section Chief
Record/Information Dissemination Section
Records Management Division
Federal Bureau of Investigation
Winchester, Virginia

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION
CENTER,

Plaintiff,

v.

U.S. DEPARTMENT OF JUSTICE CRIMINAL
DIVISION, *et al.*,

Defendants.

Civil Action No. 12-cv-0127 (RWR)

EXHIBIT A

ELECTRONIC PRIVACY INFORMATION CENTER

1718 CONNECTICUT AVENUE NW, SUITE 200
WASHINGTON, D.C. 20009
202-483-1140
FAX 202-483-1248

CONFIDENTIAL – SUBJECT TO ATTORNEY-CLIENT PRIVILEGE

ANY DISSEMINATION, DISTRIBUTION, OR COPYING OF THIS COMMUNICATION BY OTHER THAN
ITS ADDRESSEE IS STRICTLY PROHIBITED. IF THIS FACSIMILE HAS BEEN RECEIVED IN ERROR,
PLEASE IMMEDIATELY NOTIFY THE SENDER

**TO: DAVID HARDY, FOIA
OFFICER**

FROM: ANDREW CHRISTY

COMPANY:

Federal Bureau of Investigation

DATE:

6/23/2011

RECIPIENT'S FAX NUMBER:

(540) 868-4997

SENDER'S EMAIL:

Christy@epic.org

RECIPIENT'S TELEPHONE NUMBER:

SENDER'S TELEPHONE NUMBER:

(202) 483-1140

TOTAL NO. OF PAGES INCLUDING COVER:

6

COMMENTS:

ELECTRONIC PRIVACY INFORMATION CENTER



June 23, 2011

VIA FACSIMILE: (540) 868-4997

David M. Hardy, Section Chief, Record/Information Dissemination Section
Federal Bureau of Investigation
Record/Information Dissemination Section
170 Marcel Drive
Winchester, VA 22602-4483

1718 Connecticut Ave NW
Suite 200
Washington DC 20009
USA
+1 202 483 1140 (tel)
+1 202 483 1248 (fax)
www.epic.org

RE: Freedom of Information Act Request and Request for Expedited Processing

Dear Mr. Hardy:

This letter constitutes a request under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, and is submitted on behalf of the Electronic Privacy Information Center ("EPIC"). EPIC seeks documents regarding the government's identification and surveillance of individuals who have demonstrated support for or interest in WikiLeaks, as well as any documents relating to records obtained from Internet and financial services companies regarding these individuals.

Background

On December 22, 2010, EPIC submitted FOIA requests to the Department of Justice ("DOJ"), the Secret Service, Immigration and Customs Enforcement ("ICE"), and the Financial Crimes Enforcement Network ("FinCEN"). These requests sought communications or agreements between the government and certain corporations regarding donations to WikiLeaks and personally identifiable information for individuals who accessed or attempted to access the WikiLeaks website. The request to the DOJ was referred to the Antitrust Division. As of June 9, 2011, none of the agencies have found or disclosed the records EPIC requested.

On November 28, 2010, WikiLeaks and cooperating news agencies published State Department cables allegedly provided by Pvt. Bradley Manning.¹ On November 29, Attorney General Eric Holder stated that DOJ was conducting a criminal investigation regarding WikiLeaks.² The government filed a sealed request pursuant to 18 U.S.C. § 2703(d) with federal magistrate judge Theresa C. Buchanan in the Eastern District of Virginia in Alexandria.³ On December 14, 2010, Judge Buchanan issued an order ("Twitter Order") pursuant to § 2703(d) compelling Twitter to disclose customer account information, including Internet Protocol addresses and addressing information

¹ Robert Booth, *WikiLeaks Cables: Bradley Manning Faces 52 Years in Jail*, The Guardian, Nov. 30, 2010, <http://www.guardian.co.uk/world/2010/nov/30/wikileaks-cables-bradley-manning>.

² Mark Memmott, *WikiLeaks Update: Justice Investigating*, National Public Radio, Nov. 29, 2010, <http://www.npr.org/blogs/thetwo-way/2010/11/29/131669228/wikileaks-update-justice-investigating>.

³ See *In re Application of the United States for an Order Pursuant to 18 U.S.C. § 2703(d)*, Misc. No. 10GJ3793 (E.D. Va. Dec. 14, 2010).

associated with communications, for Julian Assange, Bradley Manning, Rop Gonggrijp, and Birgitta Jónsdóttir.⁴

The Twitter Order prohibited Twitter from disclosing the existence of the application or order to anyone.⁵ After contesting the seal, Twitter convinced the federal district court to unseal the order and allow Twitter to notify its users of the government's request for their information.⁶ On January 26, 2011, the Electronic Frontier Foundation and the American Civil Liberties Union filed a motion in the Eastern District of Virginia to overturn the Twitter Order, on behalf of Rop Gonggrijp, Birgitta Jónsdóttir, and Jacob Appelbaum (the only U.S. citizen among the plaintiffs).⁷ This litigation remains pending.⁸

As evidence of surveillance of WikiLeaks supporters, Jacob Appelbaum, U.S. WikiLeaks spokesperson, and David House, close friend of Bradley Manning, have been stopped at the border by Customs and Border Patrol ("CBP") agents when entering the United States and specifically questioned about their involvement with WikiLeaks.⁹ Appelbaum has been questioned at least twice at the border, and his electronic devices have been confiscated. The first time was on July 29, 2010 upon reentering the United States from the Netherlands.¹⁰ When he was questioned a second time on January 10, 2011 upon return from Iceland, he traveled with no electronic equipment, causing the customs agents to be "visibly unhappy."¹¹ The CBP agents also indicated they had viewed his Twitter feed ahead of his flight to obtain his flight details.¹² On July 31, 2010, plainclothes FBI agents questioned Appelbaum after he gave a speech at Defcon.¹³ All of the questioning by FBI and DHS focused on his personal views on and work with WikiLeaks.¹⁴

The Washington Post reported that DHS agents at Chicago O'Hare International Airport detained David House and seized his laptop on November 3, 2010.¹⁵ David

⁴ *Id.*

⁵ *See id.*

⁶ Order to Unseal the Order Pursuant to 18 U.S.C. § 2703(D), Misc. No. 10GJ3793 (E.D. Va. Jan. 5, 2010).

⁷ Motion to Vacate Dec. 14, 2010 Order, Misc. No. GJ3793 (E.D. Va. Jan. 26, 2010).

⁸ *See Government Demands for Twitter Records of Birgitta Jonsdottir*, Electronic Frontier Foundation, June 2, 2011, <https://www.eff.org/cases/government-demands-twitter-records>.

⁹ Glenn Greenwald, *Government Harrassing and Intimidating Bradley Manning Supporters*, Salon, Nov. 9, 2010, http://www.salon.com/news/opinion/glenn_greenwald/2010/11/09/manning.

¹⁰ Elinor Mills, *Researcher Detained at U.S. Border, Questioned about WikiLeaks*, CNET, July 31, 2010, http://news.cnet.com/8301-27080_3-20012253-245.html

¹¹ Xenia Jardin, *Wikileaks Volunteer Detained and Searched (again) by US Agents*, Boing Boing, Jan. 12, 2011, <http://www.boingboing.net/2011/01/12/wikileaks-volunteer-1.html>.

¹² *Id.*

¹³ Elinor Mills, *Researcher Detained at U.S. Border, Questioned about WikiLeaks*, CNET, July 31, 2010, http://news.cnet.com/8301-27080_3-20012253-245.html

¹⁴ *Id.*

¹⁵ Ellen Nakashima, *Activist Who Supports Soldier in WikiLeaks Case Sues U.S. over Seizure of Laptop*, *The Washington Post*, May 13, 2011, http://www.washingtonpost.com/national/activist-who-supports-soldier-in-wikileaks-case-sues-us-over-seizure-of-laptop/2011/05/11/AFxxzf1G_story.html.

House created the Bradley Manning Support Network, a defense fund for Bradley Manning.¹⁶ An agent from the FBI Joint Terrorism Task Force questioned David House about his relationship with Manning and WikiLeaks.¹⁷ In an interview with *The Washington Post*, David House claimed he had been stopped and questioned at the border seven times since September and he believes his name is on a government watchlist.¹⁸

There has been widespread suspicion that other online services such as Facebook and Google were served with similar court orders requesting information on WikiLeaks supporters, though neither company has confirmed the existence of such an order.¹⁹ The broad nature of the Twitter Order and the silence of other companies that were likely served with a similar sealed order suggest that DOJ, FBI, DHS, and CBP may be conducting surveillance of WikiLeaks supporters.

Requested Documents

1. All records regarding any individuals targeted for surveillance for support for or interest in WikiLeaks;
2. All records regarding lists of names of individuals who have demonstrated support for or interest in WikiLeaks;
3. All records of any agency communications with Internet and social media companies including, but not limited to Facebook and Google, regarding lists of individuals who have demonstrated, through advocacy or other means, support for or interest in WikiLeaks; and
4. All records of any agency communications with financial services companies including, but not limited to Visa, MasterCard, and PayPal, regarding lists of individuals who have demonstrated, through monetary donations or other means, support or interest in WikiLeaks.

Request for Expedited Processing

This request warrants expedited processing because it is made by “a person primarily engaged in disseminating information . . .” and it pertains to a matter about

¹⁶ Glenn Greenwald, *Government Harrassing and Intimidating Bradley Manning Supporters*, Salon, Nov. 9, 2010, http://www.salon.com/news/opinion/glenn_greenwald/2010/11/09/manning.

¹⁷ *Id.*

¹⁸ Nakashima, *supra* note 15.

¹⁹ Peter Beaumont, *WikiLeaks Demands Google and Facebook Unseal US Subpoenas*, The Guardian, Jan. 8, 2011, <http://www.guardian.co.uk/media/2011/jan/08/wikileaks-calls-google-facebook-us-subpoenas>.

which there is an "urgency to inform the public about an actual or alleged federal government activity." 5 U.S.C. § 552(a)(6)(E)(v)(II).

EPIC is "primarily engaged in disseminating information." *Am. Civil Liberties Union v. U.S. Dep't of Justice*, 321 F. Supp. 2d 24, 29 n.5 (D.D.C. 2004). This request is part of EPIC's open government program and its ongoing efforts to investigate the U.S. government's domestic surveillance programs.²⁰ On December 22, 2010, EPIC submitted FOIA requests to the DOJ, the Secret Service, ICE, and the FinCEN, seeking documents related to the government's attempts to compel Internet and financial services companies to disclose private records regarding WikiLeaks supporters. In January 2011, Steven Aftergood, who directs the Project on Government Secrecy at the American Federation of Scientists, and Glenn Greenwald, a noted constitutional lawyer and writer at Salon.com, spoke at an EPIC board meeting regarding WikiLeaks.

There is particular urgency for the public to obtain information about the extent of the government's domestic surveillance programs. Disclosure of information related to the surveillance of WikiLeaks supporters will enhance the public's understanding of the extent of the government's surveillance of individuals exercising the rights to freedom of speech and association guaranteed by the First Amendment of the U.S. Constitution.

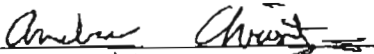
Request for "News Media" Fee Status


EPIC is a "representative of the news media" for fee waiver purposes. *EPIC v. Department of Defense*, 241 F. Supp. 2d 6 (D.D.C. 2003). Based on our status as a "news media" requester, we are entitled to receive the requested record with only duplication fees asserted. Further, because disclosure of this information will "contribute greatly public understanding of the operation or activities of the government," and duplication fees should be waived.

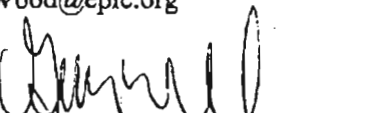
Thank you for your consideration of this request. As 5 U.S.C. § 552(a)(6)(E)(ii)(I) provides, I will anticipate your determination on our request within ten (10) calendar days.

²⁰ See, e.g., EPIC, Domestic Surveillance, <http://www.epic.org/features/surveillance.html> (last visited June 9, 2011).

Respectfully submitted,


Andrew Christy
Law Clerk, EPIC
Christy@epic.org


Alexandra Wood
Law Clerk, EPIC
Wood@epic.org


Ginger McCall
Staff Counsel, EPIC
Mccall@epic.org

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION
CENTER,

Plaintiff,

v.

U.S. DEPARTMENT OF JUSTICE CRIMINAL
DIVISION, *et al.*,

Defendants.

Civil Action No. 12-cv-0127 (RWR)

EXHIBIT B



U.S. Department of Justice

Federal Bureau of Investigation

Washington, D.C. 20535

July 11, 2011

MR. ANDREW CHRISTY
ELECTRONIC PRIVACY INFORMATION CENTER
SUITE 200
1718 CONNECTICUT AVENUE NORTHWEST
WASHINGTON, DC 20009

Request No.: 1169306- 000
Subject: WIKILEAKS (SUPPORT FOR OR
INTEREST IN)

Dear Mr. Christy:

This responds to your Freedom of Information/Privacy Acts (FOIPA) request.

Based on the information you provided, we conducted a search of the indices to our Central Records System for "Wikileaks." We were unable to identify responsive main file records. If you have additional information pertaining to the subject and you believe it was of investigative interest to the Bureau, please provide us the details and we will conduct an additional search.

You may file an appeal by writing to the Director, Office of Information Policy (OIP), U.S. Department of Justice, 1425 New York Ave., NW, Suite 11050, Washington, D.C. 20530-0001. Your appeal must be received by OIP within sixty (60) days from the date of this letter in order to be considered timely. The envelope and the letter should be clearly marked "Freedom of Information Appeal." Please cite the FOIPA Request Number assigned to your request so that it may be identified easily.

Since we did not locate any files to process, there was no need to adjudicate your request for expedited processing.

Enclosed for your information is a copy of the FBI File Fact Sheet.

Sincerely yours,

A handwritten signature in black ink, appearing to read "D. Hardy", is written over a horizontal line.

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

Enclosure

FBI FILE FACT SHEET

- The primary function of the FBI is law enforcement.
The FBI does not keep a file on every citizen of the United States.
- The FBI was not established until 1908 and we have very few records prior to the 1920's.
- **FBI files generally contain reports** of FBI investigations of a wide range of matters, including counterterrorism, foreign counter-intelligence, organized crime/drugs, violent crime, white-collar crime, applicants, and civil rights.
- **The FBI does not issue clearances or nonclearances for anyone other than its own personnel or persons having access to FBI facilities.** Background investigations for security clearances are conducted by many different Government agencies. Persons who received a clearance while in the military or employed with some other government agency should write directly to that entity.
- **An FBI identification record or "rap sheet" is NOT the same as an FBI "file"** - it is simply a listing of information taken from fingerprint cards submitted to the FBI in connection with arrests, federal employment, naturalization, or military service. The subject of a "rap sheet" may obtain a copy by submitting a written request to FBI, CJIS Division, Attn: SCU, Mod. D-2, 1000 Custer Hollow Road, Clarksburg, West Virginia 26306. Each request must have proof of identity which shall consist of **name, date and place of birth and a set of rolled-ink fingerprint impressions** placed upon fingerprint cards or forms commonly utilized for applicant or law enforcement purposes by law enforcement agencies, plus **payment of \$18.00** in the form of a certified check or money order, payable to the Treasury of the United States.
- **The National Name Check Program (NNCP)** conducts a search of the FBI's Universal Index to identify any information contained in FBI records that may be associated with an individual and provides the results of that search to the requesting Federal, State or local agency. For the NNCP, a name is searched in a multitude of combinations and phonetic spellings to ensure all records are located. The NNCP also searches for both "main" and "cross reference" files. A main file is an entry that carries the name corresponding to the subject of a file while a cross reference is merely a mention of an individual contained in a file. The results from a search of this magnitude can result in several "hits" and "idents" on an individual. In each instance where UNI has identified a name variation or reference, information must be reviewed to determine whether it is applicable to the individual in question.
- **The Record/Information Dissemination Section/Freedom of Information-Privacy Acts (FOIPA)** search for records provides copies of FBI files relevant to a FOIPA request for information. FOIPA provides responsive documents to requesters seeking "reasonably described information." For a FOIPA search, the subject name, event, activity, business, or event is searched to determine whether there is an investigative file associated with the subject. This is called a "main file search" and differs from The NNCP search.

FOR GENERAL INFORMATION ABOUT THE FBI,
CHECK OUT OUR WEBSITE AT
<http://www.fbi.gov>

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION
CENTER,

Plaintiff,

v.

U.S. DEPARTMENT OF JUSTICE CRIMINAL
DIVISION, *et al.*,

Defendants.

Civil Action No. 12-cv-0127 (RWR)

EXHIBIT C

ELECTRONIC PRIVACY INFORMATION CENTER

1718 CONNECTICUT AVENUE NW, SUITE 200
WASHINGTON, D.C. 20009
202-483-1140
FAX 202-483-1248

CONFIDENTIAL -- SUBJECT TO ATTORNEY-CLIENT PRIVILEGE

ANY DISSEMINATION, DISTRIBUTION, OR COPYING OF THIS COMMUNICATION BY OTHER THAN
ITS ADDRESSEE IS STRICTLY PROHIBITED. IF THIS FACSIMILE HAS BEEN RECEIVED IN ERROR,
PLEASE IMMEDIATELY NOTIFY THE SENDER

TO: DIRECTOR, OIP

FROM: GINGER MCCALL

COMPANY:

DATE:

Office of Information Policy

9/9/11

RECIPIENT'S FAX NUMBER:

SENDER'S EMAIL:

202-514-1009

mccall@epic.org

RECIPIENT'S TELEPHONE NUMBER:

SENDER'S TELEPHONE NUMBER:

(202) 483-1140

TOTAL NO. OF PAGES INCLUDING COVER:

7

COMMENTS:

 **RECEIVED**

SEP 09 2011

Office of Information Policy



September 8, 2011

VIA FAX (202-514-1009)

Freedom of Information Appeal
Office of Information Policy
U.S. Department of Justice
Suite 11050
1425 New York Avenue, N.W.
Washington, D.C. 20530-0001

1718 Connecticut Ave NW

Suite 200

Washington DC 20009

USA

+1 202 483 1140 [tel]

+1 202 483 1248 [fax]

www.epic.org

RE: Freedom of Information Act Appeal

Dear FOIA Appeals Officer:

This letter constitutes an appeal under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, and is submitted to the Federal Bureau of Investigation ("FBI") on behalf of the Electronic Privacy Information Center ("EPIC").

On June 23, 2011, EPIC submitted to the FBI via facsimile a FOIA request regarding the government's identification and surveillance of individuals who have demonstrated support for or interest in WikiLeaks, as well as any documents relating to records obtained from Internet and financial services companies regarding these individuals. Specifically, EPIC requested:

1. All records regarding any individuals targeted for surveillance for support for or interest in WikiLeaks;
2. All records regarding lists of names of individuals who have demonstrated support for or interest in WikiLeaks;
3. All records of any agency communications with Internet and social media companies including, but not limited to Facebook and Google, regarding lists of individuals who have demonstrated, through advocacy or other means, support for or interest in WikiLeaks; and
4. All records of any agency communications with financial services companies including, but not limited to Visa, MasterCard, and PayPal, regarding lists of

individuals who have demonstrated, through monetary donations or other means, support or interest in WikiLeaks.

See Appendix 1 ("EPIC's FOIA Request").

Factual Background

On December 22, 2010, EPIC submitted FOIA requests to the Department of Justice ("DOJ"), the Secret Service, Immigration and Customs Enforcement ("ICE"), and the Financial Crimes Enforcement Network ("FinCEN"). These requests sought communications or agreements between the government and certain corporations regarding donations to WikiLeaks and personally identifiable information for individuals who accessed or attempted to access the WikiLeaks website. The request to the DOJ was referred to the Antitrust Division. As of June 9, 2011, none of the agencies have found or disclosed the records EPIC requested.

On November 28, 2010, WikiLeaks and cooperating news agencies published State Department cables allegedly provided by Pvt. Bradley Manning.¹ On November 29, Attorney General Eric Holder stated that DOJ was conducting a criminal investigation regarding WikiLeaks.² The government filed a sealed request pursuant to 18 U.S.C. § 2703(d) with federal magistrate judge Theresa C. Buchanan in the Eastern District of Virginia in Alexandria.³ On December 14, 2010, Judge Buchanan issued an order ("Twitter Order") pursuant to § 2703(d) compelling Twitter to disclose customer account information, including Internet Protocol addresses and addressing information associated with communications, for Julian Assange, Bradley Manning, Rop Gonggrijp, and Birgitta Jónsdóttir.⁴

The Twitter Order prohibited Twitter from disclosing the existence of the application or order to anyone.⁵ After contesting the seal, Twitter convinced the federal district court to unseal the order and allow Twitter to notify its users of the government's request for their information.⁶ On January 26, 2011, the Electronic Frontier Foundation and the American Civil Liberties Union filed a motion in the Eastern District of Virginia to overturn the Twitter Order, on behalf of Rop Gonggrijp, Birgitta Jónsdóttir, and Jacob Appelbaum (the only U.S. citizen among the plaintiffs).⁷ This litigation remains pending.⁸

¹ Robert Booth, *WikiLeaks Cables: Bradley Manning Faces 52 Years in Jail*, The Guardian, November 30, 2010, <http://www.guardian.co.uk/world/2010/nov/30/wikileaks-cables-bradley-manning>.

² Mark Memmott, *WikiLeaks Update: Justice Investigating*, National Public Radio, Nov. 29, 2010, <http://www.npr.org/blogs/thetwo-way/2010/11/29/131669228/wikileaks-update-justice-investigating>.

³ *See In re Application of the United States for an Order Pursuant to 18 U.S.C. § 2703(d)*, Misc. No. 10GJ3793 (E.D. Va. Dec. 14, 2010).

⁴ *Id.*

⁵ *See id.*

⁶ Order to Unseal the Order Pursuant to 18 U.S.C. § 2703(D), Misc. No. 10GJ3793 (E.D. Va. Jan. 5, 2011).

⁷ Motion to Vacate Dec. 14, 2010 Order, Misc. No. GJ3793 (E.D. Va. Jan. 26, 2011).

⁸ *See Government Demands for Twitter Records of Birgitta Jonsdottir*, Electronic Frontier Foundation, June 2, 2011, <https://www.eff.org/cases/government-demands-twitter-records>.

As evidence of surveillance of WikiLeaks supporters, Jacob Appelbaum, U.S. WikiLeaks spokesperson, and David House, close friend of Bradley Manning, have been stopped at the border by Customs and Border Patrol ("CBP") agents when entering the United States and specifically questioned about their involvement with WikiLeaks.⁹ Appelbaum has been questioned at least twice at the border, and his electronic devices have been confiscated. The first time was on July 29, 2010 upon reentering the United States from the Netherlands.¹⁰ When he was questioned a second time on January 10, 2011 upon return from Iceland, he traveled with no electronic equipment, causing the customs agents to be "visibly unhappy."¹¹ The CBP agents also indicated they had viewed his Twitter feed ahead of his flight to obtain his flight details.¹² On July 31, 2010, plainclothes FBI agents questioned Appelbaum after he gave a speech at Defcon.¹³ All of the questioning by FBI and DHS focused on his personal views on and work with WikiLeaks.¹⁴

The Washington Post reported that DHS agents at Chicago O'Hare International Airport detained David House and seized his laptop on November 3, 2010.¹⁵ David House created the Bradley Manning Support Network, a defense fund for Bradley Manning.¹⁶ An agent from the FBI Joint Terrorism Task Force questioned David House about his relationship with Manning and WikiLeaks.¹⁷ In an interview with *The Washington Post*, David House claimed he had been stopped and questioned at the border seven times since September and he believes his name is on a government watchlist.¹⁸

There has been widespread suspicion that other online services such as Facebook and Google were served with similar court orders requesting information on WikiLeaks supporters, though neither company has confirmed the existence of such an order.¹⁹ The broad nature of the Twitter Order and the silence of other companies that were likely served with a similar sealed order suggest that DOJ, FBI, DHS, and CBP may be conducting surveillance of WikiLeaks supporters.

⁹ Glenn Greenwald, *Government Harrassing and Intimidating Bradley Manning Supporters*, Salon, Nov. 9, 2010, http://www.salon.com/news/opinion/glenn_greenwald/2010/11/09/manning.

¹⁰ Elinor Mills, *Researcher Detained at U.S. Border, Questioned about WikiLeaks*, CNET, July 31, 2010, http://news.cnet.com/8301-27080_3-20012253-245.html

¹¹ Xenia Jardin, *Wikileaks Volunteer Detained and Searched (again) by US Agents*, Boing Boing, Jan. 12, 2011, <http://www.boingboing.net/2011/01/12/wikileaks-volunteer-1.html>.

¹² *Id.*

¹³ Elinor Mills, *Researcher Detained at U.S. Border, Questioned about WikiLeaks*, CNET, July 31, 2010, http://news.cnet.com/8301-27080_3-20012253-245.html

¹⁴ *Id.*

¹⁵ Ellen Nakashima, *Activist Who Supports Soldier in WikiLeaks Case Sues U.S. over Seizure of Laptop*, *The Washington Post*, May 13, 2011, http://www.washingtonpost.com/national/activist-who-supports-soldier-in-wikileaks-case-sues-us-over-seizure-of-laptop/2011/05/11/AFxxzflG_story.html.

¹⁶ Glenn Greenwald, *Government Harrassing and Intimidating Bradley Manning Supporters*, Salon, Nov. 9, 2010, http://www.salon.com/news/opinion/glenn_greenwald/2010/11/09/manning.

¹⁷ *Id.*

¹⁸ Nakashima, *supra* note 15.

¹⁹ Peter Beaumont, *WikiLeaks Demands Google and Facebook Unseal US Subpoenas*, *The Guardian*, Jan. 8, 2011, <http://www.guardian.co.uk/media/2011/jan/08/wikileaks-calls-google-facebook-us-subpoenas>.

Procedural Background

On June 23, 2011, EPIC sent EPIC's FOIA Request to the Federal Bureau of Investigation. *See* Appendix 1. The FOIA Request was sent via facsimile to (240) 868-4997. *See* Appendix 2 ("Fax Receipt"). The FBI received EPIC's FOIA Request on June 23, 2011. *See* Appendix 2.

On July 11, 2011, the FBI mailed a letter to EPIC in response to EPIC's FOIA Request. *See* Appendix 3 ("FBI Letter"). The FBI Letter assigned the request the Request Number 1169306-000 and stated that the agency's search of the indices of its Central Records System for "Wikileaks" did not return responsive main file records. *See* Appendix 3.

EPIC Appeals the FBI's Failure to Disclose Records

EPIC is appealing the FBI's failure to disclose relevant records in its possession. The FBI Letter states that the agency conducted a search of the indices of its Central Records Systems for the term "Wikileaks" but did not "identify responsive main file records." *See* Appendix 3. Because the FBI possesses records relevant to EPIC's FOIA Request, the agency's failure to disclose any relevant records is evidence of an insufficient search.

As described in detail above, the FBI possesses records relevant to EPIC's FOIA Request. On November 29, 2010, Attorney General Eric Holder publicly announced that the Department of Justice had initiated a criminal investigation regarding WikiLeaks.²⁰ On December 14, 2010, Judge Buchanan of the U.S. District Court for the Eastern District of Virginia issued an order pursuant to 18 U.S.C. § 2703(d) compelling Twitter to disclose customer account information associated with WikiLeaks supporters Rop Gonggrijp, Birgitta Jónsdóttir, and Jacob Appelbaum.²¹ On June 15, 2011, David House appeared before a grand jury convened in the U.S. District Court for the Eastern District of Virginia and a U.S. Attorney questioned him about his alleged support for WikiLeaks. Because the FBI is the "principle investigative arm of the United States Department of Justice," there is a substantial likelihood that the FBI possesses records related to the Department of Justice's criminal investigation of individuals associated with WikiLeaks.²²

Contact between the FBI and WikiLeaks supporters is further evidence that the FBI possesses records relevant to EPIC's FOIA Request. The *New York Times* reported in December 2010 that FBI agents seized a hard drive from Adrian Lamo, an individual

²⁰ Mark Memmott, *WikiLeaks Update: Justice Investigating*, National Public Radio, Nov. 29, 2010, <http://www.npr.org/blogs/thertwo-way/2010/11/29/131669228/wikileaks-update-justice-investigating>.

²¹ *See In re Application of the United States for an Order Pursuant to 18 U.S.C. § 2703(d)*, Misc. No. 10GJ3793 (E.D. Va. Dec. 14, 2010).

²² Federal Bureau of Investigation, About Us: Frequently Asked Questions, <http://www2.fbi.gov/aboutus/faqs/faqsone.htm> (last visited Aug. 1, 2011).

who had communicated with Bradley Manning online, as part of the Department of Justice's WikiLeaks investigation.²³ David House, who is associated with the Bradley Manning Support Network, claims that on November 3, 2010, an FBI Joint Terrorism Task Force agent stopped him at Chicago O'Hare International Airport, seized his laptop, and asked him questions about WikiLeaks.²⁴ In addition, Jacob Appelbaum has alleged that FBI agents questioned him about WikiLeaks on July 31, 2010, after he spoke at Defcon.²⁵ The FBI possesses records related to the contact its agents have had with WikiLeaks supporters, and these records are responsive to EPIC's FOIA Request.

EPIC has attached copies of press releases made available on the FBI web site on January 27, 2011, and July 19, 2011. See Appendix 4 ("January 27 Press Release"); Appendix 5 ("July 19 Press Release"). The January 27 Press Release and July 19 Press Release are evidence of an ongoing FBI investigation of WikiLeaks supporters that commenced prior to January 27, 2011. The January 27 Press Release stated that the FBI executed more than forty search warrants in the investigation regarding cyber attacks "in protest" of actions of U.S. companies, referring to the activities of WikiLeaks supporters.²⁶ The July 19 Press Release, issued by the U.S. Attorney's Office for the Northern District of California states that FBI agents arrested sixteen individuals for alleged involvement in a cyber attack against PayPal "in retribution for PayPal's termination of WikiLeaks' donation account." See Appendix 5. Furthermore, MSNBC reported that, on December 15, 2010, PayPal provided to the FBI a list of approximately 1,000 Internet protocol addresses associated with cyber attacks against PayPal.²⁷ This "collaboration" between PayPal and the FBI led to the FBI's arrests of sixteen WikiLeaks supporters on July 19, 2011.²⁸

The examples provided above are sufficient to establish that the FBI has failed to fulfill its statutory obligation under FOIA to provide records in its possession responsive to the request. See 5 U.S.C. § 552(a)(3)(A). Because the FBI is conducting an investigation of WikiLeaks supporters and information about this investigation—including explicit references to WikiLeaks—appears on the FBI web site, the failure of the FBI to find and disclose records related to this investigation demonstrates that the search the agency conducted was insufficient. The FBI is required to comply with FOIA and disclose responsive documents.

²³ Charlie Savage, *U.S. Tries to Build Case for Conspiracy by WikiLeaks*, N.Y. Times, Dec. 15, 2010, <http://www.nytimes.com/2010/12/16/world/16wiki.html>.

²⁴ Ellen Nakashima, *Activist Who Supports Soldier in WikiLeaks Case Sues U.S. over Seizure of Laptop*, The Washington Post, May 13, 2011, http://www.washingtonpost.com/national/activist-who-supports-soldier-in-wikileaks-case-sues-us-over-seizure-of-laptop/2011/05/11/AFxxzflG_story.html.

²⁵ Elinor Mills, *Researcher Detained at U.S. Border, Questioned about WikiLeaks*, CNET, July 31, 2010, http://news.cnet.com/8301-27080_3-20012253-245.html.

²⁶ Charlie Savage, *F.B.I. Warrants Into Service Attacks by WikiLeaks Supporters*, N.Y. Times, Jan. 27, 2011, <http://www.nytimes.com/2011/01/28/us/28wiki.html>.

²⁷ Athima Chansanchai, *PayPal Sent FBI List That Led to Anonymous Raids*, MSNBC.com, Aug. 1, 2011, http://technolog.msnbc.msn.com/_news/2011/08/01/7180192-paypal-sent-fbi-list-that-led-to-anonymous-raids.

²⁸ *Id.*

It is the burden of the FBI to conduct a sufficient search. A single search for the term "Wikileaks" within the main file records of the FBI's Central Records System is insufficient to comply with the requirements of the Freedom of Information Act, 5 U.S.C. § 552. Although the FBI Letter directs EPIC to provide "additional information" and the agency will conduct an "additional search," it is not EPIC's responsibility to determine the specific search terms and databases that must be used to find the records relevant to EPIC's FOIA Request. See Appendix 3. However, as described in EPIC's FOIA Request, relevant records may include terms such as "Julian Assange," "Rop Gonggrijp," "Birgitta Jónsdóttir," "Jacob Appelbaum," "David House," "PayPal," "Visa," "MasterCard," "Twitter," "Google," and "Facebook." It should be noted that these search terms are provided as examples and are not presented as an all-inclusive list of search terms that the FBI must employ in order to comply with EPIC's FOIA Request.

EPIC Renews Its Request for "News Media" Fee Status

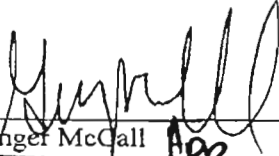
EPIC is a non-profit, educational organization that routinely and systematically disseminates information to the public. EPIC is a representative of the news media. *Elec. Privacy Info. Ctr. v. U.S. Dep't of Def.*, 241, F.Supp. 2d 5 (D.D.C. 2003).

Based on our status as a "news media" requester, we are entitled to receive the requested records with only duplication fees assessed. Further, because disclosure of this information will "contribute significantly to public understanding of the operations or activities of the government," as described above, any duplication fees should be waived.

Conclusion

Thank you for your prompt response to this appeal. As provided in 5 U.S.C. § 552(a)(6)(A)(ii), I anticipate that you will produce responsive documents within twenty (20) working days of receipt of this appeal. If you have any questions, please feel free to contact Ginger McCall at (202) 483-1140 or mccall@epic.org.

Respectfully submitted,


Ginger McCall
Open Government Counsel, EPIC

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION
CENTER,

Plaintiff,

v.

U.S. DEPARTMENT OF JUSTICE CRIMINAL
DIVISION, *et al.*,

Defendants.

Civil Action No. 12-cv-0127 (RWR)

EXHIBIT D



U.S. Department of Justice

Office of Information Policy

Telephone: (202) 514-3642

Washington, D.C. 20530

SEP 20 2011

Ginger P. McCall, Esq.
Electronic Privacy Information Center
Suite 200
1718 Connecticut Avenue, NW
Washington, DC 20009

Re: Request No. 1169306

Dear Ms. McCall:

This is to advise you that your administrative appeal from the action of the Federal Bureau of Investigation was received by this Office on September 9, 2011.

The Office of Information Policy has the responsibility of adjudicating such appeals. In an attempt to afford each appellant equal and impartial treatment, we have adopted a general practice of assigning appeals in the approximate order of receipt. Your appeal has been assigned number **AP-2011-03084**. Please mention this number in any future correspondence to this Office regarding this matter.

We will notify you of the decision on your appeal as soon as we can. If you have any questions about the status of your appeal you may contact me at the number above.

Sincerely,

A handwritten signature in black ink, appearing to read "Priscilla Jones", with a large, stylized flourish at the end.

Priscilla Jones
Supervisory Administrative Specialist