Approved for public release. All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~SECRET//ORCON/NOFORN~~

U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT
2011 OCT 31 PM 5:10
LEEANN FLYNN HALL
CLERK OF COURT

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

IN RE DNI/AG 702(g) CERTIFICATION [redacted] ~~(S)~~	**UNDER SEAL** Docket No. [redacted]

GOVERNMENT'S EX PARTE SUBMISSION OF AMENDMENT TO DNI/AG 702(g) CERTIFICATION [redacted] AND EX PARTE SUBMISSION OF AMENDED MINIMIZATION PROCEDURES ~~(S)~~

In accordance with subsection 702(i)(1)(C) of the Foreign Intelligence Surveillance Act of 1978, as amended ("the Act"), the United States of America, by and through the undersigned Department of Justice attorney, hereby submits ex parte the attached Amendment to DNI/AG 702(g) Certification [redacted]. Attached as Exhibit B to this Amendment to DNI/AG 702(g) Certification [redacted] are the amended minimization procedures to be used under the certification. ~~(S//OC/NF)~~

DNI/AG 702(g) Certification [redacted] as amended, contains all of the elements required by the Act, and the minimization procedures to be used under the certification, as amended, are consistent with the requirements of the Act and the Fourth Amendment to the Constitution of the United States. Accordingly, the Government

~~SECRET//ORCON/NOFORN~~

Classified by: Lisa O. Monaco, Assistant Attorney General, NSD, DOJ
Reason: 1.4 (c)
Declassify on: 31 October 2036

respectfully requests that this Court enter an order pursuant to subsection 702(i)(3)(A) of the Act approving DNI/AG 702(g) Certification [redacted] as amended, and the use of the minimization procedures attached as Exhibit B to the Amendment to DNI/AG Certification [redacted] ~~(S//OC/NF)~~

Respectfully submitted,

[redacted]

National Security Division
United States Department of Justice

Approved for public release. All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~SECRET~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

IN RE DNI/AG 702(g) CERTIFICATION [redacted]	Docket No. [redacted]

ORDER

For the reasons stated in the Memorandum Opinion issued contemporaneously herewith, and in reliance on the entire record in this matter, the Court finds, in the language of 50 U.S.C. § 1881a(i)(3)(A), that the certification submitted in the above-captioned docket, as amended, "contains all the required elements" and that the revised minimization procedures submitted with the amendment "are consistent with the requirements of [Section 1881a(e)] and with the fourth amendment to Constitution of the United States."

Accordingly, it is hereby ORDERED, pursuant to 50 U.S.C. § 1881a(i)(3)(A), that such amendment and the use of such procedures are approved.

Entered this _____ day of November 2011, at _____ Eastern Time.

JOHN D. BATES
Judge, United States Foreign
Intelligence Surveillance Court

~~SECRET~~

Derived From: ~~Submission to the USFISC in Docket Number captioned above~~

Approved for public release. All withheld information exempt under b(1) and b(3) except as otherwise noted.

CERTIFICATION OF THE DIRECTOR OF NATIONAL INTELLIGENCE AND THE ATTORNEY GENERAL PURSUANT TO SUBSECTION 702(g) OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED

2011 OCT 31 PM 5:10

[redacted]

Amendment to DNI/AG 702(g) Certification [redacted]

On April 13, 2011, based on supporting affidavits, the Director of National Intelligence and the Attorney General executed in writing and under oath DNI/AG 702(g) Certification [redacted] pursuant to subsection 702(g) of the Foreign Intelligence Surveillance Act of 1978, as amended ("FISA" or "the Act"), thereby authorizing the targeting of non-United States persons reasonably believed to be outside the United States to acquire foreign intelligence information. Specifically, the Director of National Intelligence and the Attorney General certified that:

(1) there are procedures in place that had been approved or would be submitted with the certification for approval by the Foreign Intelligence Surveillance Court ("FISC")[1] that are reasonably designed to --

a. ensure that an acquisition authorized pursuant to subsection 702(a) of the Act is limited to targeting persons reasonably believed to be located outside the United States; and

b. prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States;

[1] Specifically, the targeting procedures to be used by the National Security Agency (NSA) and the Federal Bureau of Investigation (FBI) were submitted as Exhibits A and C, respectively, to the certification. ~~(S//OC/NF)~~

~~Classified by: The Attorney General~~
~~Reason: 1.4(c)~~
~~Declassify on: 31 October 2035~~

(2) the minimization procedures with respect to such acquisition --

a. meet the definition of minimization procedures under subsections 101(h) and 301(4) of the Act; and

b. had been approved or would be submitted with the certification for approval by the FISC;[2]

(3) guidelines have been adopted in accordance with subsection 702(f) of the Act to ensure compliance with the limitations in subsection 702(b) of the Act and to ensure that an application for a court order is filed as required by the Act;

(4) the procedures and guidelines referred to in sub-paragraphs (1), (2), and (3) above are consistent with the requirements of the Fourth Amendment to the Constitution of the United States;

(5) a significant purpose of the acquisition is to obtain foreign intelligence information;

(6) the acquisition involves obtaining foreign intelligence information from or with the assistance of an electronic communication service provider; and

(7) the acquisition complies with the limitations in subsection 702(b) of the Act.

DNI/AG 702(g) Certification [redacted] including supporting affidavits and targeting and minimization procedures, was submitted to the FISC for review on April 22, 2011. ~~(S//OC/NF)~~

In accordance with subsection 702(i)(1)(C) of the Act, DNI/AG 702(g) Certification [redacted] is hereby amended. Specifically, the use of the NSA minimization procedures attached

[2] Specifically, the minimization procedures to be used by the NSA, FBI, and Central Intelligence Agency (CIA) were submitted as Exhibits B, D, and E, respectively, to the certification. ~~(S//OC/NF)~~

hereto as Exhibit B under DNI/AG 702(g) Certification [redacted] is authorized. These minimization procedures --

a. meet the definition of minimization procedures under subsections 101(h) and 301(4) of the Act; and

b. will be submitted with this certification for approval by the FISC.

~~(S//OC/NF)~~

These minimization procedures are consistent with the requirements of the Fourth Amendment to the Constitution of the United States. ~~(S//OC/NF)~~

This authorization, as amended, shall be effective immediately. All other aspects of DNI/AG 702(g) Certification [redacted] remain unaltered and are incorporated herein. ~~(S//OC/NF)~~

---- *The remainder of this page intentionally left blank* ----

Approved for public release. All withheld information exempt under b(1) and b(3) except as otherwise noted.

VERIFICATION (U)

I declare under penalty of perjury that the facts set forth in the foregoing amendment [redacted] DNI/AG 702(g) Certification [redacted] are true and correct to the best of my knowledge and belief. Executed pursuant to 28 U.S.C. § 1746 on October 31, 2011. ~~(S)~~

Eric H. Holder, Jr.
Attorney General of the United States

NYT v DOJ, 16 CIV 7020_000516

Approved for public release. All withheld information exempt under b(1) and b(3) except as otherwise noted.

VERIFICATION (U)

I declare under penalty of perjury that the facts set forth in the foregoing amendment [redacted] DNI/AG 702(g) Certification [redacted] are true and correct to the best of my knowledge and belief. Executed pursuant to 28 U.S.C. § 1746 on October 31, 2011. ~~(S)~~

James R. Clapper
Director of National Intelligence

NYT v DOJ, 16 CIV 7020_000517

Approved for public release. All withheld information exempt under b(1) and b(3) except as otherwise noted.

U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT
2011 OCT 31 PM 5:10
LEEANN FLYNN HALL
CLERK OF COURT

EXHIBIT B

MINIMIZATION PROCEDURES USED BY THE NATIONAL SECURITY AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED

Section 1 - Applicability and Scope (U)

These National Security Agency (NSA) minimization procedures apply to the acquisition, retention, use, and dissemination of non-publicly available information concerning unconsenting United States persons that is acquired by targeting non-United States persons reasonably believed to be located outside the United States in accordance with section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended ("the Act"). (U)

If NSA determines that it must take action in apparent departure from these minimization procedures to protect against an immediate threat to human life (e.g., force protection or hostage situations) and that it is not feasible to obtain a timely modification of these procedures, NSA may take such action immediately. NSA will report the action taken to the Office of the Director of National Intelligence and to the National Security Division of the Department of Justice, which will promptly notify the Foreign Intelligence Surveillance Court of such activity. (U)

For the purposes of these procedures, the terms "National Security Agency" and "NSA personnel" refer to any employees of the National Security Agency/Central Security Service ("NSA/CSS" or "NSA") and any other personnel engaged in Signals Intelligence (SIGINT) operations authorized pursuant to section 702 of the Act if such operations are executed under the direction, authority, or control of the Director, NSA/Chief, CSS (DIRNSA). (U)

Section 2 - Definitions (U)

In addition to the definitions in sections 101 and 701 of the Act, the following definitions will apply to these procedures:

(a) Acquisition means the collection by NSA or the FBI through electronic means of a non-public communication to which it is not an intended party. (U)

(b) Communications concerning a United States person include all communications in which a United States person is discussed or mentioned, except where such communications reveal only publicly-available information about the person. (U)

(c) Communications of a United States person include all communications to which a United States person is a party. (U)

~~Derived From: NSA/CSSM 1-52~~
~~Dated: 20070108~~
~~Declassify On: 20320108~~

NYT v DOJ, 16 CIV 7020_000518

(d) Consent is the agreement by a person or organization to permit the NSA to take particular actions that affect the person or organization. To be effective, consent must be given by the affected person or organization with sufficient knowledge to understand the action that may be taken and the possible consequences of that action. Consent by an organization will be deemed valid if given on behalf of the organization by an official or governing body determined by the General Counsel, NSA, to have actual or apparent authority to make such an agreement. (U)

(e) Foreign communication means a communication that has at least one communicant outside of the United States. All other communications, including communications in which the sender and all intended recipients are reasonably believed to be located in the United States at the time of acquisition, are domestic communications. ~~(S//SI)~~

(f) Identification of a United States person means (1) the name, unique title, or address of a United States person; or (2) other personal identifiers of a United States person when appearing in the context of activities conducted by that person or activities conducted by others that are related to that person. A reference to a product by brand name, or manufacturer's name or the use of a name in a descriptive sense, e.g., "Monroe Doctrine," is not an identification of a United States person. ~~(S//SI)~~

(g) Internet transaction, for purposes of these procedures, means an Internet communication that is acquired through NSA's upstream collection techniques. An Internet transaction may contain information or data representing either a discrete communication [redacted] or multiple discrete communications [redacted] ~~(TS//SI)~~.

(h) Processed or processing means any step necessary to convert a communication into an intelligible form intended for human inspection. (U)

(i) Publicly available information means information that a member of the public could obtain on request, by research in public sources, or by casual observation. (U)

(j) Technical data base means information retained for cryptanalytic, traffic analytic, or signal exploitation purposes. ~~(S//SI)~~

(k) United States person means a United States person as defined in the Act. The following guidelines apply in determining whether a person whose status is unknown is a United States person: (U)

(1) A person known to be currently in the United States will be treated as a United States person unless positively identified as an alien who has not been admitted for permanent residence, or unless the nature or circumstances of the person's communications give rise to a reasonable belief that such person is not a United States person. (U)

(2) A person known to be currently outside the United States, or whose location is unknown, will not be treated as a United States person unless such person can be

positively identified as such, or the nature or circumstances of the person's communications give rise to a reasonable belief that such person is a United States person. (U)

(3) A person known to be an alien admitted for permanent residence loses status as a United States person if the person leaves the United States and is not in compliance with 8 U.S.C. § 1203 enabling re-entry into the United States. Failure to follow the statutory procedures provides a reasonable basis to conclude that the alien has abandoned any intention of maintaining his status as a permanent resident alien. (U)

(4) An unincorporated association whose headquarters or primary office is located outside the United States is presumed not to be a United States person unless there is information indicating that a substantial number of its members are citizens of the United States or aliens lawfully admitted for permanent residence. (U)

Section 3 - Acquisition and Processing - General (U)

(a) Acquisition (U)

The acquisition of information by targeting non-United States persons reasonably believed to be located outside the United States pursuant to section 702 of the Act will be effected in accordance with an authorization made by the Attorney General and Director of National Intelligence pursuant to subsection 702(a) of the Act and will be conducted in a manner designed, to the greatest extent reasonably feasible, to minimize the acquisition of information not relevant to the authorized purpose of the acquisition. ~~(S//SI)~~

(b) Monitoring, Recording, and Processing (U)

(1) Personnel will exercise reasonable judgment in determining whether information acquired must be minimized and will destroy inadvertently acquired communications of or concerning a United States person at the earliest practicable point in the processing cycle at which such communication can be identified either: as clearly not relevant to the authorized purpose of the acquisition (e.g., the communication does not contain foreign intelligence information); or, as not containing evidence of a crime which may be disseminated under these procedures. Except as provided for in subsection 3(c)(2) below, such inadvertently acquired communications of or concerning a United States person may be retained no longer than five years from the expiration date of the certification authorizing the collection in any event. ~~(S//SI)~~

(2) Communications of or concerning United States persons that may be related to the authorized purpose of the acquisition may be forwarded to analytic personnel responsible for producing intelligence information from the collected data. Such communications or information may be retained and disseminated only in accordance with Sections 4, 5, 6, and 8 of these procedures. (C)

(3) Magnetic tapes or other storage media that contain acquired communications may be processed. ~~(S)~~

(4) As a communication is reviewed, NSA analyst(s) will determine whether it is a domestic or foreign communication to, from, or about a target and is reasonably believed to contain foreign intelligence information or evidence of a crime. Only such communications may be processed. All other communications may be retained or disseminated only in accordance with Sections 5, 6, and 8 of these procedures. ~~(S//SI)~~

(5) Processing of Internet Transactions Acquired Through NSA Upstream Collection Techniques ~~(TS//SI)~~

a. Notwithstanding any processing [redacted] that may be required to render an Internet transaction intelligible to analysts, NSA will take reasonable steps post-acquisition to identify and segregate through technical means Internet transactions that cannot be reasonably identified as containing single, discrete communications where: the active user of the transaction (i.e., the electronic communications account/address/identifier used to send or receive the Internet transaction to or from a service provider) is reasonably believed to be located in the United States; or the location of the active user is unknown. ~~(TS//SI)~~

1. Internet transactions that are identified and segregated pursuant to subsection 3(b)(5)a. will be retained in an access-controlled repository that is accessible only to NSA analysts who have been trained to review such transactions for the purpose of identifying those that contain discrete communications as to which the sender and all intended recipients are reasonably believed to be located in the United States. ~~(TS//SI)~~

(a) Any information contained in a segregated Internet transaction (including metadata) may not be moved or copied from the segregated repository or otherwise used for foreign intelligence purposes unless it has been determined that the transaction does not contain any discrete communication as to which the sender and all intended recipients are reasonably believed to be located in the United States. Any Internet transaction that is identified and segregated pursuant to subsection 3(b)(5)a. and is subsequently determined to contain a discrete communication as to which the sender and all intended recipients are reasonably believed to be located in the United States will be destroyed upon recognition. ~~(TS//SI)~~

(b) Any information moved or copied from the segregated repository into repositories more generally accessible to NSA analysts will be processed in accordance with subsection 3(b)(5)b. below and handled in accordance the other applicable provisions of these procedures. ~~(TS//SI)~~

(c) Any information moved or copied from the segregated repository into repositories more generally accessible to NSA analysts will be marked, tagged, or otherwise identified as having been previously segregated pursuant to subsection 3(b)(5)a.

2. Internet transactions that are not identified and segregated pursuant to subsection 3(b)(5)a. will be processed in accordance with subsection 3(b)(5)b. below and handled in accordance with the other applicable provisions of these procedures.

b. NSA analysts seeking to use (for example, in a FISA application, intelligence report, or section 702 targeting) a discrete communication within an Internet transaction that contains multiple discrete communications will assess whether the discrete communication: 1) is a communication as to which the sender and all intended recipients are located in the United States; and 2) is to, from, or about a tasked selector, or otherwise contains foreign intelligence information. ~~(TS//SI)~~

1. If an NSA analyst seeks to use a discrete communication within an Internet transaction that contains multiple discrete communications, the analyst will first perform checks to determine the locations of the sender and intended recipients of that discrete communication to the extent reasonably necessary to determine whether the sender and all intended recipients of that communication are located in the United States. ~~(TS//SI)~~

2. If an NSA analyst seeks to use a discrete communication within an Internet transaction that contains multiple discrete communications, the analyst will assess whether the discrete communication is to, from, or about a tasked selector, or otherwise contains foreign intelligence information. ~~(TS//SI)~~

(a) If the discrete communication is to, from, or about a tasked selector, any U.S. person information in that communication will be handled in accordance with the applicable provisions of these procedures. ~~(TS//SI)~~

(b) If the discrete communication is not to, from, or about a tasked selector but otherwise contains foreign intelligence information, and the discrete communication is not to or from an identifiable U.S. person or a person reasonably believed to be located in the United States, that communication (including any U.S. person information therein) will be treated in accordance with the applicable provisions of these procedures. ~~(TS//SI)~~

(c) If the discrete communication is not to, from, or about a tasked selector but is to or from an identifiable U.S. person or a person reasonably believed to be located in the United States, the NSA analyst will document that determination in the relevant analytic repository or tool if technically possible or reasonably feasible. Such discrete communication cannot be used for any purpose other than to protect against an immediate threat to

human life (e.g., force protection or hostage situations). NSA will report any such use to the Office of the Director of National Intelligence and to the National Security Division of the Department of Justice, which will promptly notify the Foreign Intelligence Surveillance Court of such use. ~~(TS//SI)~~

3. An NSA analyst seeking to use a discrete communication within an Internet transaction that contains multiple discrete communications in a FISA application, intelligence report, or section 702 targeting must appropriately document the verifications required by subsections 3(b)(5)b.1. and 2. above. ~~(TS//SI)~~

4. Notwithstanding subsection 3(b)(5)b. above, NSA may use metadata extracted from Internet transactions that are not identified and segregated pursuant to subsection 3(b)(5)a. without first assessing whether the metadata was extracted from: a) a discrete communication as to which the sender and all intended recipients are located in the United States; or b) a discrete communication to, from, or about a tasked selector. Any metadata extracted from Internet transactions that are not identified and segregated pursuant to subsection 3(b)(5)a. will be handled in accordance with the applicable provisions of these procedures. Any metadata extracted from an Internet transaction subsequently determined to contain a discrete communication as to which the sender and all intended recipients are reasonably believed to be located inside the United States shall be destroyed upon recognition. ~~(TS//SI)~~

(6) Magnetic tapes or other storage media containing communications acquired pursuant to section 702 may be scanned by computer to identify and select communications for analysis. Computer selection terms used for scanning, such as telephone numbers, key words or phrases, or other discriminators, will be limited to those selection terms reasonably likely to return foreign intelligence information. Identifiers of an identifiable U.S. person may not be used as terms to identify and select for analysis any Internet communication acquired through NSA's upstream collection techniques. Any use of United States person identifiers as terms to identify and select communications must first be approved in accordance with NSA procedures. NSA will maintain records of all United States person identifiers approved for use as selection terms. The Department of Justice's National Security Division and the Office of the Director of National Intelligence will conduct oversight of NSA's activities with respect to United States persons that are conducted pursuant to this paragraph. ~~(S//SI)~~

(7) Further processing, retention and dissemination of foreign communications will be made in accordance with Sections 4, 6, 7, and 8 as applicable, below. Further processing, storage and dissemination of inadvertently acquired domestic communications will be made in accordance with Sections 4, 5, and 8 below. ~~(S//SI)~~

(c) Destruction of Raw Data ~~(C)~~

(1) Telephony communications, Internet communications acquired [redacted] from Internet Service Providers, and other discrete forms of information (including that reduced to graphic or "hard copy" form such as [redacted] that do not meet the retention standards set forth in these procedures and that are known to contain communications of or concerning United States persons will be destroyed upon recognition, and may be retained no longer than five years from the expiration date of the certification authorizing the collection in any event. ~~(S//SI)~~

(2) Internet transactions acquired through NSA's upstream collection techniques that do not contain any information that meets the retention standards set forth in these procedures and that are known to contain communications of or concerning United States persons will be destroyed upon recognition. All Internet transactions may be retained no longer than two years from the expiration date of the certification authorizing the collection in any event. The Internet transactions that may be retained include those that were acquired because of limitations on NSA's ability to filter communications. Any Internet communications acquired through NSA's upstream collection techniques that are retained in accordance with this subsection may be reviewed and processed only in accordance with the standards set forth in subsection 3(b)(5) of these procedures. ~~(TS//SI)~~

(d) Change in Target's Location or Status ~~(S//SI)~~

(1) In the event that NSA determines that a person is reasonably believed to be located outside the United States and after targeting this person learns that the person is inside the United States, or if NSA concludes that a person who at the time of targeting was believed to be a non-United States person is in fact a United States person, the acquisition from that person will be terminated without delay. ~~(S//SI)~~

(2) Any communications acquired through the targeting of a person who at the time of targeting was reasonably believed to be located outside the United States but is in fact located inside the United States at the time such communications were acquired, and any communications acquired by targeting a person who at the time of targeting was believed to be a non-United States person but was in fact a United States person, will be treated as domestic communications under these procedures. ~~(S//SI)~~

Section 4 - Acquisition and Processing - Attorney-Client Communications ~~(C)~~

As soon as it becomes apparent that a communication is between a person who is known to be under criminal indictment in the United States and an attorney who represents that individual in the matter under indictment (or someone acting on behalf of the attorney), monitoring of that communication will cease and the communication will be identified as an attorney-client communication in a log maintained for that purpose. The relevant portion of the communication containing that conversation will be segregated and the National Security

Division of the Department of Justice will be notified so that appropriate procedures may be established to protect such communications from review or use in any criminal prosecution, while preserving foreign intelligence information contained therein. Additionally, all proposed disseminations of information constituting United States person attorney-client privileged communications must be reviewed by the NSA Office of General Counsel prior to dissemination. ~~(S//SI)~~

Section 5 - Domestic Communications (U)

A communication identified as a domestic communication will be promptly destroyed upon recognition unless the Director (or Acting Director) of NSA specifically determines, in writing, that: ~~(S)~~

(1) the communication is reasonably believed to contain significant foreign intelligence information. Such communication may be provided to the FBI (including United States person identities) for possible dissemination by the FBI in accordance with its minimization procedures; ~~(S)~~

(2) the communication does not contain foreign intelligence information but is reasonably believed to contain evidence of a crime that has been, is being, or is about to be committed. Such communication may be disseminated (including United States person identities) to appropriate Federal law enforcement authorities, in accordance with 50 U.S.C. §§ 1806(b) and 1825(c), Executive Order No. 12333, and, where applicable, the crimes reporting procedures set out in the August 1995 "Memorandum of Understanding: Reporting of Information Concerning Federal Crimes," or any successor document. Such communications may be retained by NSA for a reasonable period of time, not to exceed six months unless extended in writing by the Attorney General, to permit law enforcement agencies to determine whether access to original recordings of such communications is required for law enforcement purposes; ~~(S)~~

(3) the communication is reasonably believed to contain technical data base information, as defined in Section 2(i), or information necessary to understand or assess a communications security vulnerability. Such communication may be provided to the FBI and/or disseminated to other elements of the United States Government. Such communications may be retained for a period sufficient to allow a thorough exploitation and to permit access to data that are, or are reasonably believed likely to become, relevant to a current or future foreign intelligence requirement. Sufficient duration may vary with the nature of the exploitation. ~~(S//SI)~~

a. In the context of a cryptanalytic effort, maintenance of technical data bases requires retention of all communications that are enciphered or reasonably believed to contain secret meaning, and sufficient duration may consist of any period of time during which encrypted material is subject to, or of use in, cryptanalysis. ~~(S//SI)~~

b. In the case of communications that are not enciphered or otherwise thought to contain secret meaning, sufficient duration is five years from the expiration date of the certification authorizing the collection unless the Signal Intelligence Director, NSA, determines in writing that retention for a longer period is required to respond to authorized foreign intelligence or counterintelligence requirements; or ~~(S//SI)~~

(4) the communication contains information pertaining to a threat of serious harm to life or property. ~~(S)~~

Notwithstanding the above, if a domestic communication indicates that a target has entered the United States, NSA may advise the FBI of that fact. Moreover, technical data regarding domestic communications may be retained and provided to the FBI and CIA for collection avoidance purposes. ~~(S//SI)~~

Section 6 - Foreign Communications of or Concerning United States Persons (U)

(a) Retention (U)

Foreign communications of or concerning United States persons collected in the course of an acquisition authorized under section 702 of the Act may be retained only:

(1) if necessary for the maintenance of technical data bases. Retention for this purpose is permitted for a period sufficient to allow a thorough exploitation and to permit access to data that are, or are reasonably believed likely to become, relevant to a current or future foreign intelligence requirement. Sufficient duration may vary with the nature of the exploitation.

a. In the context of a cryptanalytic effort, maintenance of technical data bases requires retention of all communications that are enciphered or reasonably believed to contain secret meaning, and sufficient duration may consist of any period of time during which encrypted material is subject to, or of use in, cryptanalysis.

b. In the case of communications that are not enciphered or otherwise thought to contain secret meaning, sufficient duration is five years from the expiration date of the certification authorizing the collection unless the Signals Intelligence Director, NSA, determines in writing that retention for a longer period is required to respond to authorized foreign intelligence or counterintelligence requirements;

(2) if dissemination of such communications with reference to such United States persons would be permitted under subsection (b) below; or

(3) if the information is evidence of a crime that has been, is being, or is about to be committed and is provided to appropriate federal law enforcement authorities. ~~(S//SI)~~

(b) Dissemination (U)

A report based on communications of or concerning a United States person may be disseminated in accordance with Section 7 or 8 if the identity of the United States person is deleted and a generic term or symbol is substituted so that the information cannot reasonably be connected with an identifiable United States person. Otherwise, dissemination of intelligence reports based on communications of or concerning a United States person may only be made to a recipient requiring the identity of such person for the performance of official duties but only if at least one of the following criteria is also met:

(1) the United States person has consented to dissemination or the information of or concerning the United States person is available publicly;

(2) the identity of the United States person is necessary to understand foreign intelligence information or assess its importance, e.g., the identity of a senior official in the Executive Branch;

(3) the communication or information indicates that the United States person may be:

a. an agent of a foreign power;

b. a foreign power as defined in Section 101(a) of the Act;

c. residing outside the United States and holding an official position in the government or military forces of a foreign power;

d. a corporation or other entity that is owned or controlled directly or indirectly by a foreign power; or

e. acting in collaboration with an intelligence or security service of a foreign power and the United States person has, or has had, access to classified national security information or material;

(4) the communication or information indicates that the United States person may be the target of intelligence activities of a foreign power;

(5) the communication or information indicates that the United States person is engaged in the unauthorized disclosure of classified national security information or the United States person's identity is necessary to understand or assess a communications security vulnerability, but only after the agency that originated the information certifies that it is properly classified;

(6) the communication or information indicates that the United States person may be engaging in international terrorist activities;

(7) the acquisition of the United States person's communication was authorized by a court order issued pursuant to the Act and the communication may relate to the foreign intelligence purpose of the surveillance; or

(8) the communication or information is reasonably believed to contain evidence that a crime has been, is being, or is about to be committed, provided that dissemination is for law enforcement purposes and is made in accordance with 50 U.S.C. §§ 1806(b) and 1825(c), Executive Order No. 12333, and, where applicable, the crimes reporting procedures set out in the August 1995 "Memorandum of Understanding: Reporting of Information Concerning Federal Crimes," or any successor document. (U)

(c) Provision of Unminimized Communications to CIA and FBI ~~(S//NF)~~

(1) NSA may provide to the Central Intelligence Agency (CIA) unminimized communications acquired pursuant to section 702 of the Act. CIA will identify to NSA targets for which NSA may provide unminimized communications to CIA. CIA will process any such unminimized communications received from NSA in accordance with CIA minimization procedures adopted by the Attorney General, in consultation with the Director of National Intelligence, pursuant to subsection 702(e) of the Act. ~~(S//SI//NF)~~

(2) NSA may provide to the FBI unminimized communications acquired pursuant to section 702 of the Act. The FBI will identify to NSA targets for which NSA may provide unminimized communications to the FBI. The FBI will process any such unminimized communications received from NSA in accordance with FBI minimization procedures adopted by the Attorney General, in consultation with the Director of National Intelligence, pursuant to subsection 702(e) of the Act. ~~(S//SI)~~

Section 7 - Other Foreign Communications (U)

Foreign communications of or concerning a non-United States person may be retained, used, and disseminated in any form in accordance with other applicable law, regulation, and policy. (U)

Section 8 - Collaboration with Foreign Governments ~~(S//SI)~~

(a) Procedures for the dissemination of evaluated and minimized information. Pursuant to Section 1.7(c)(8) of Executive Order No. 12333, as amended, NSA conducts foreign cryptologic liaison relationships with certain foreign governments. Information acquired pursuant to section 702 of the Act may be disseminated to a foreign government. Except as provided in subsection 8(b) of these procedures, any dissemination to a foreign government of information of or concerning a United States person that is acquired pursuant to section 702 may only be done in a manner consistent with subsections 6(b) and 7 of these NSA minimization procedures. ~~(S)~~

(b) Procedures for technical or linguistic assistance. It is anticipated that NSA may obtain information or communications that, because of their technical or linguistic content, may require further analysis by foreign governments to assist NSA in determining their meaning or significance. Notwithstanding other provisions of these minimization procedures, NSA may disseminate computer disks, tape recordings, transcripts, or other information or items containing unminimized information or communications acquired pursuant to section 702 to foreign governments for further processing and analysis, under the following restrictions with respect to any materials so disseminated: ~~(S)~~

(1) Dissemination to foreign governments will be solely for translation or analysis of such information or communications, and assisting foreign governments will make no use of any information or any communication of or concerning any person except to provide technical and linguistic assistance to NSA. ~~(S)~~

(2) Dissemination will be only to those personnel within foreign governments involved in the translation or analysis of such information or communications. The number of such personnel will be restricted to the extent feasible. There will be no dissemination within foreign governments of this unminimized data. ~~(S)~~

(3) Foreign governments will make no permanent agency record of information or communications of or concerning any person referred to or recorded on computer disks, tape recordings, transcripts, or other items disseminated by NSA to foreign governments, provided that foreign governments may maintain such temporary records as are necessary to enable them to assist NSA with the translation or analysis of such information. Records maintained by foreign governments for this purpose may not be disseminated within the foreign governments, except to personnel involved in providing technical or linguistic assistance to NSA. ~~(S)~~

(4) Upon the conclusion of such technical or linguistic assistance to NSA, computer disks, tape recordings, transcripts, or other items or information disseminated to foreign governments will either be returned to NSA or be destroyed with an accounting of such destruction made to NSA. ~~(S)~~

Approved for public release. All withheld information exempt under b(1) and b(3) except as otherwise noted.

(5) Any information that foreign governments provide to NSA as a result of such technical or linguistic assistance may be disseminated by NSA in accordance with these minimization procedures. ~~(S)~~

10-31-11
Date

Eric H. Holder, Jr.
Attorney General of the United States

NYT v DOJ, 16 CIV 7020_000530