~~SECRET//X1~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

IN RE APPLICATION OF THE
FEDERAL BUREAU OF INVESTIGATION
FOR AN ORDER REQUIRING THE
PRODUCTION OF TANGIBLE THINGS
[redacted]

Docket Number: [redacted]

ORDER

An Application having been made by the Director of the Federal Bureau of Investigation (FBI) for an Order pursuant to the Foreign Intelligence Surveillance Act of 1978 (the Act), Title 50, United States Code (U.S.C.), § 1861, as amended, requiring the production to [redacted] of the tangible things described below, and full consideration having been given to the matters set forth therein, the Court finds that:

1. The Director of the FBI is authorized to make an application for an order requiring the production of any tangible things for an investigation to obtain foreign intelligence information not concerning a United States person

~~SECRET//X1~~

Derived from: Pleadings in the Above-Captioned Docket
Declassify on: X1

or to protect against international terrorism, provided that such investigation of a United States person is not conducted solely on the basis of activities protected by the First Amendment to the Constitution of the United States. [50 U.S.C. § 1861(c)(1)]

2. The tangible things to be produced are records of [redacted] for the periods specified herein [redacted] [50 U.S.C. § 1861(c)(2)(A)]

3. There are reasonable grounds to believe that the tangible things sought are relevant to authorized investigations (other than threat assessments) being conducted by the FBI under guidelines approved by the Attorney General under Executive Order 12333 to protect against international terrorism, and that any such investigations of U.S. persons are not being conducted solely upon the basis of activities protected by the First Amendment to the Constitution of the United States. [50 U.S.C. § 1861(c)(1)]

4. The tangible things sought could be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things. [50 U.S.C. § 1861(c)(2)(D)]

WHEREFORE, the Court finds that the Application of the United States to obtain the tangible things, as described in the Application, satisfies the requirements of the Act and, therefore,

IT IS HEREBY ORDERED, pursuant to the authority conferred on this Court by the Act, that the Application is GRANTED, and it is

FURTHER ORDERED, as follows:

(1) To the extent practicable, the Custodian of Records [redacted] shall produce to [redacted] appropriate secondary order, and continue production on an ongoing approximately daily basis thereafter for the duration of this Order, unless otherwise ordered by the Court, an electronic copy of the following tangible things: [redacted]

[redacted]

(2) The Custodian of Records also shall produce to [redacted] appropriate secondary order, an electronic copy of the [redacted] records dated from [redacted] to the date of this Order;

(3) The Court understands that on or about [redacted] non compulsory National Security Letter to [redacted] pursuant to that request. The Court understands that [redacted] ill delete from its computer system and destroy all data received pursuant to [redacted] National Security Letter;

(4) This Order does not require the production of [redacted]

(5) The Court understands that once an analyst completes his or her research, all disseminations of the positive results of queries of [redacted] records obtained pursuant to this Order will be made available to appropriately-

[redacted]

~~SECRET//X1~~

cleared employees [redacted] shall handle and disseminate such information, including U.S. person information, in accordance with the procedures set forth in The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (October 31, 2003). [redacted] shall also maintain records of all of [redacted] written and oral disseminations.[1]

[1] [redacted]

~~SECRET//X1~~

~~SECRET//X1~~

(6) In addition, with respect to the information that the [redacted] shall adhere to the following procedures:

A. [redacted] establish mandatory procedures strictly to control access to and use of [redacted] records obtained pursuant to this Order. Any search or analysis of [redacted] records obtained pursuant to this Order shall occur only when, based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion that a particular known identifier[2] is associated with [redacted]

[redacted]

2 [redacted]

[redacted] terrorist organization,[3] [redacted] provided, however, that [redacted] Office of General Counsel (OGC) shall review proposed queries involving a particular known identifier when such identifier is reasonably believed to be used by a U.S. person and shall approve a query only if [redacted] determines that such suspicion is not founded solely on the basis of activities that are protected by the First Amendment to the U.S. Constitution. Moreover, consistent with its current practice as described in paragraph 25 of [redacted] Declaration, [redacted] is authorized

[redacted]

3 [redacted]

to review only the first and second "hops" from the original search term(s) when using the link analysis tool for a single query. Additional information may be reviewed only by means of a query using a new identifier(s) in accordance with this subparagraph.

B. [redacted] records shall be stored on a restricted, stand-alone network in a secure [redacted] No merger or commingling of [redacted] records received pursuant to this Order with any other dataset shall occur without the prior authorization of this Court.

C. [redacted] records obtained pursuant to this Order shall be "tagged" or identified as FISA business records data. Any search that includes a search of [redacted] records obtained pursuant to this Order shall be done only in accordance with the procedures set forth herein.

D. Access to [redacted] records obtained pursuant to this Order shall be made by logging onto one of approximately [redacted] stand-alone workstations that are part of a compartmented computer system,

all of which are housed in access-controlled rooms.[4] [redacted] shall only be provided to authorized users after a full briefing on the security and usage protocols and only to those analysts who require access to the data in the normal course of their duties. Before accessing the computer system, all new analysts who are briefed into the compartmented program [redacted] shall be provided with written guidance regarding the requirements for unmasking or receiving access to any U.S. person information (described below) and shall be given basic search application training. Such guidance and training shall detail the policies and restrictions on accessing and using the data, shall describe the masking and unmasking process, [redacted] Before they are authorized to use the system, analysts shall be required to sign an acknowledgement that they are aware of and understand the restrictions on accessing the data and the use of U.S. person information and understand how to handle U.S. person data.

[4] [redacted]

SECRET//X1

E. The Court understands that there will be approximately [redacted] that will have access to [redacted] records.

[redacted]

5 [redacted]

6 [redacted]

SECRET//X1

~~SECRET//X1~~

[redacted]

F. Authorized users shall only make targeted searches in accordance with subparagraph A above and shall be prohibited from browsing the whole collection of data.

G. All user activity, including search queries, shall be recorded and maintained. The computer application shall also require analysts to enter a justification prior to conducting a query, and the system shall record all such justifications.[7] If any [redacted] records obtained pursuant to this Order are returned as a result of a query, the computer system shall clearly indicate to the authorized user that FISA information was returned. All displayed and printed [redacted] records obtained pursuant this Order shall contain an appropriate FISA warning label.

H. Before new [redacted] records received pursuant to this Order are made searchable, system administrators shall mask all presumed U.S. person

[7] The Court understands that prior to searching any records received pursuant to this Order, a pop-up screen will appear any time a user attempts to search [redacted] records obtained pursuant to this Order alerting the user that the search includes such records and requires appropriate search justification.

~~SECRET//X1~~

information.[8] The search application shall substitute the text "[US PERSON DATA]" for all [redacted] text, rather than the actual U.S. person information, shall be displayed to the analyst as a search result.

I. If an analyst wants U.S. person information unmasked, the analyst shall submit a request to his/her supervisor to unmask the U.S. person information. Before U.S. person information is unmasked, the analyst shall: (1) confirm for his/her supervisor that the query meets the standard set forth in subparagraph A above; and (2) articulate to his/her supervisor that the U.S. person information is necessary to understand the foreign intelligence information or to assess its importance. Upon approval by the supervisor, a system administrator may print out the masked data and provide it to the analyst. [redacted] shall maintain a record of all "unmaskings" associated with U.S. person information [redacted]

[8] [redacted]

~~SECRET//X1~~

[redacted]

J. At least twice every ninety days, [redacted] specialist (who may be an appropriately-cleared [redacted] who is trained on and works with this collection shall conduct random spot checks of [redacted] records obtained to ensure [redacted] receiving only data as authorized by the Court. Such spot checks shall include an [redacted]

K. At least every ninety days, the Department of Justice, [redacted] shall review this program. In addition, the Department of Justice shall prepare a report within forty-five days after the initiation of the collection assessing the adequacy of the management controls for the processing and dissemination of U.S. person information. The Department of Justice shall provide the findings of that report to the Attorney General.

L. At least every ninety days, the Department of Justice [redacted] shall review a sample of [redacted] justifications for querying [redacted] records obtained pursuant to this Order.

~~SECRET//X1~~

M. [redacted]

records collected under this Court's Order online (that is, accessible for queries by cleared analysts) for five years from the date of acquisition [redacted] at which time they shall be destroyed.[9]

/

/

/

/

/

/

/

/

/

/

/

/

[9] In the event of an operational need, the Court understands that the Government may seek authority from the Court to retain the records for an additional time period.

~~SECRET//X1~~

N. Any application to renew or reinstate the authority requested herein shall include a report describing: (i) the queries that have been made since this Application was granted; (ii) [redacted] application of the standard set forth in subparagraph A above; (iii) the number of records unmasked since this Application was granted; (iv) the number of times a query produced known U.S. person information that was not masked since this Application was granted; and (v) any proposed changes in the way [redacted] records would be received [redacted] and/or used [redacted] in the future.

Signed [redacted] Eastern Time
Date Time

This authorization regarding **the production of tangible things** [redacted] expires on the [redacted] Eastern Time.

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

~~SECRET//X1~~