ATTACHMENT A: ITEMS TO BE SEIZED

Pursuant to 18 U.S.C. § 2703 and 42 U.S.C. § 2000aa(a), it is hereby ordered as follows:

I. SERVICE OF WARRANT AND SEARCH PROCEDURE

a. Google, Incorporated, a provider of electronic communication and remote computing services, located at 1600 Amphitheatre Parkway, Mountain View, California, (the "PROVIDER") will isolate those accounts and files described in Section II below. Pursuant to 18 U.S.C. § 2703(g) the presence of an agent is not required for service or execution of this warrant.

b. The PROVIDER shall not notify any other person, including the subscriber(s) of [redacted]@gmail.com of the existence of the warrant.

c. In order to minimize any disruption of computer service to innocent third parties, the PROVIDER's employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the computer accounts and files described in Section II below, including an exact duplicate of all information stored in the computer accounts and files described therein.

d. As soon as practicable after service of this warrant, the PROVIDER shall provide the exact duplicate in electronic form of the account and files described in Section II below and all information stored in that account and files to the following FBI special agent:

Reginald B. Reyes
FBI-WFO
601 4th Street, NW
Washington, D.C. 20535
Fax: 202-278-2864
Desk: 202-278-4868

The PROVIDER shall send the information to the agent via facsimile and overnight mail, and where maintained in electronic form, on CD-ROM or an equivalent electronic medium.

e. The FBI will make an exact duplicate of the original production from the PROVIDER. The original production from the PROVIDER will be sealed by the FBI and preserved for authenticity and chain of custody purposes.

II. FILES AND ACCOUNTS TO BE COPIED BY THE PROVIDER'S EMPLOYEES

a. Any and all communications, on whatever date, between [redacted]@gmail.com ("SUBJECT ACCOUNT") and any of the following accounts:

(1) [redacted]@yahoo.com,

(2) [redacted]@yahoo.com, and

(3) [redacted]@gmail.com.

"Any and all communications" includes, without limitation, received messages (whether "to," "cc'd," or "bcc'd" to the SUBJECT ACCOUNT), forwarded messages, sent messages (whether "to," "cc'd," or "bcc'd" to the three above-listed accounts), deleted messages, and messages maintained in trash or other folders, and any attachments thereto, including videos, documents, photos, internet addresses, and computer files sent to and received from other websites. "Any and all communications" further includes all prior email messages in an email "chain" between the SUBJECT ACCOUNT and any of the three above-listed accounts, whether or not those prior emails were in fact sent between the SUBJECT ACCOUNT and the above-listed accounts;

b. Any and all communications "to" or "from" the SUBJECT ACCOUNT on June 10 and/or June 11, 2009. "Any and all communications" includes, without limitation, received messages (whether "to", "cc'd," or "bcc'd" to the SUBJECT ACCOUNT), forwarded messages, sent messages, deleted messages, messages maintained in trash or other folders, and any attachments thereto, including videos, documents, photos, internet addresses, and computer files

sent to and received from other websites. "Any and all communications" further includes all prior email messages in an email "chain" sent "to" or "from" the SUBJECT ACCOUNT on June 10 or June 11, 2009, whether or not those prior emails in the "chain" were in fact sent or received on June 10 or June 11, 2009;

c. All existing printouts from original storage of all of the electronic mail described above in Section II (a) and II(b);

d. All transactional information of all activity of the SUBJECT ACCOUNT described above in Section II(a) and II(b), including log files, dates, times, methods of connecting, ports, dial-ups, registration Internet Protocol (IP) address and/or locations;

e. All business records and subscriber information, in any form kept, pertaining to the SUBJECT ACCOUNT described above in Section II(a) and II(b), including applications, subscribers' full names, all screen names associated with the subscribers and/or accounts, all account names associated with the subscribers, account numbers, screen names, status of accounts, dates of service, methods of payment, telephone numbers, addresses, detailed billing records, and histories and profiles;

f. All records indicating the account preferences and services available to subscribers of the SUBJECT ACCOUNT described above in Section II(a) and II(b).

III. INFORMATION TO BE SEIZED BY LAW ENFORCEMENT PERSONNEL

Items to be seized, which are believed to be evidence and fruits of violations of 18 U.S.C. § 793 (Unauthorized Disclosure of National Defense Information) as follows:

a. The contents of electronic communications, including attachments and stored files, for the SUBJECT ACCOUNT as described and limited by Section II(a) and II(b) above,

including videos, computer files sent to and received from other websites, received messages, sent messages, deleted messages, messages maintained in trash or other folders, any attachments thereto, and all existing printouts from original storage of all of the electronic mail described above in Section II(a) and II(b), that pertain to:

1. records or information related to violations of 18 U.S.C. § 793;
2. any and all communications between Stephen Kim and the author of the article (the "Author") that is the subject matter of the FBI investigation that is the basis for this warrant (the "Article") and any record or information that reflects such communications;
3. records or information relating to Stephen Kim's communications and/or activities on the date of publication of the Article;
4. records or information relating to the Author's communication with any other source or potential source of the information disclosed in the Article;
5. records or information related to Stephen Kim's or the Author's knowledge of laws, regulations, rules and/or procedures prohibiting the unauthorized disclosure of national defense or classified information;
6. records or information related to Stephen Kim's or the Author's knowledge of government rules and/or procedures regarding communications with members of the media;
7. records or information related to any disclosure or prospective disclosure of classified and/or intelligence information;
8. any classified document, image, record or information, and any

communications concerning such documents, images, records, or information;

9. any document, image, record or information concerning the national defense, including but not limited to documents, maps, plans, diagrams, guides, manuals, and other Department of Defense, U.S. military, and/or weapons material, as well as sources and methods of intelligence gathering, and any communications concerning such documents, images, records, or information;

10. records or information related to the state of mind of any individuals seeking the disclosure or receipt of classified, intelligence and/or national defense information;

11. records or information related to the subject matter of the Article; and

12. records or information related to the user(s) of the SUBJECT ACCOUNT.

b. All of the records and information described above in Sections II(d), II(e), and II(f) including:

1. Account information for the SUBJECT ACCOUNT including:

(a) Names and associated email addresses;

(b) Physical address and location information;

(c) Records of session times and durations;

(d) Length of service (including start date) and types of service utilized;

(e) Telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address;

(f) The means and source of payment for such service (including any credit card or bank account number); and

(g) Internet Protocol addresses used by the subscriber to register the account or otherwise initiate service.

2. User connection logs for the SUBJECT ACCOUNT for any connections to or from the SUBJECT ACCOUNT. User connection logs should include the following:

(a) Connection time and date;

(b) Disconnect time and date;

(c) Method of connection to system (e.g., SLIP, PPP, Shell);

(d) Data transfer volume (e.g., bytes);

(e) The IP address that was used when the user connected to the service,

(f) Connection information for other systems to which user connected via the SUBJECT ACCOUNT, including:

(1) Connection destination;

(2) Connection time and date;

(3) Disconnect time and date;

(4) Method of connection to system (e.g., telnet, ftp, http);

(5) Data transfer volume (e.g., bytes);

(6) Any other relevant routing information.