UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

APPLICATION FOR SEARCH WARRANT	)	
FOR EMAIL ACCOUNT	)	
Redacted	)	**Mag. No. 09-616-M-01**
MAINTAINED ON COMPUTER SERVERS	)	
OPERATED BY YAHOO!, INC.	)	
HEADQUARTERED AT	)	
701 FIRST AVENUE,	)	
SUNNYVALE, CA	)	

ORDER

After reviewing the United States' May 21, 2013 Motion to Unseal Entire Docket, it is hereby

ORDERED that the United States' motion is **GRANTED**; it is

FURTHER ORDERED that the Clerk of Court **UNSEAL** and place on the public docket redacted versions of the documents attached as Exhibits A through G to the United States' Motion to Unseal; it is

FURTHER ORDERED that the Clerk of Court shall place on the public docket a redacted version of the motion to Unseal Entire Docket and this Order, removing from the caption the name of the email account at issue (proposed versions of which were attached to the United States' Motion to Unseal Entire Docket as Exhibit H and I); and

FURTHER ORDERED that the United States may produce unredacted versions of all the unsealed materials to the defense in United States v. Stephen Jin-Woo Kim, Cr. No. 10-255 (CKK), pursuant to the Rule 16 Protective Order in that matter.

SO ORDERED this 22nd day of May 2013.

Reggie C. Lamberth
United States District Court

EXHIBIT A

UNITED STATES MAGISTRATE JUDGE
U.S. DISTRICT COURT BUILDING
WASHINGTON, D.C.

PLEASE ISSUE: [ ] Arrest [X] Search [X] Seizure

warrant for: E-mail Account [redacted]**@yahoo.com** Maintained on Computer Servers Operated by YAHOO!, Inc , Headquartered at 701 First Avenue, Sunnyvale, California

Violation: [ ] D C C [X] U.S.C. Title: 18

Section(s): 793

G Michael
Assistant United States Attorney
(202) 305-4155

November 9, 2009
Date

Bond. _____

COMPLETE FOR ALL ARREST WARRANTS:

The following information must be provided for ALL arrest warrants and an ***original*** *and* ***duplicate*** *of this form must be submitted to the Clerk's Office with the warrant papers*

Officer / Agent Name: Casey P. Farrell

Badge Number.

Agency / Unit: Federal Bureau of Investigation
24 Hour Telephone Number: (202) 278-4875
(For officer/agent)

Beeper Number:
(For officer/agent) 202-497-9000

EXHIBIT B

FILED
NOV 09 2009
Clerk, U.S. District and Bankruptcy Courts

THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF COLUMBIA

APPLICATION FOR SEARCH WARRANT FOR E-MAIL ACCOUNT [redacted]@YAHOO.COM MAINTAINED ON COMPUTER SERVERS OPERATED BY YAHOO!, INC., HEADQUARTERED AT 701 FIRST AVENUE, SUNNYVALE, CA	)	09-616 M-01
	)	UNDER SEAL

MOTION TO SEAL SEARCH WARRANT AND RELATED MATERIALS AND FOR NON-DISCLOSURE

The United States, by and through its attorney, the United States Attorney for the District of Columbia respectfully **requests** that the Court issue an Order to Seal the **search warrant** and related materials, including the **application for the search warrant,** the **affidavit** in support of the search warrant, the **memorandum** in support thereof, and the subsequent **return on the search warrant**, together with this Motion to Seal and proposed Order, until the United States makes a motion to unseal the materials.

The Court has the inherent power to seal search warrants and their related materials to protect an ongoing investigation. United States v. Hubbard, 650 F.2d 293 (D.C. Cir. 1980). Moreover, under Post v. Robinson, 935 F.2d 282, 289 n.10 (D.C. Cir. 1991), the court may seal filings where there exists an extraordinary situation and a compelling governmental interest which justify such sealing.

FACTS

In June 2009 TOP SECRET United States national defense information was published in an article on a national news organization's website (hereinafter the "June 2009 article"). Following that unauthorized disclosure, an FBI investigation was initiated to determine the source(s) of the disclosure. The investigation has revealed that one individual who both accessed the classified information at issue, and communicated with the author of the June 2009 article, was Stephen Jin-

Woo Kim. Mr. Kim is a user of the email account that is the subject of the present search warrant. The FBI is currently engaged in an ongoing investigation of Mr. Kim that will be substantially and adversely affected if he or any other potential subjects were to prematurely become aware of the specific details known to the FBI about their activities or the legal process which is being used during the investigation. The government submits that this constitutes a legitimate governmental interest to be protected by the requested sealing.

Moreover, ongoing investigative steps that will be taken in the wake of execution of this search warrant, such as interviews and the pursuit of other warrants, would be adversely affected if the details set forth in the Affidavit were to become known at this time. This, too, constitutes a legitimate governmental interest to be protected by the requested sealing.

The United States has considered alternatives less drastic than sealing and has found none that would suffice to protect the government's legitimate interest in attempting to locate and prosecute those responsible for the bombings.

The government submits that under Post v. Robinson, 935 F.2d 282, 289 n.10 (D.C. Cir. 1991), these facts present an extraordinary situation and a compelling governmental interest which justify the sealing of the search warrant, the application, the affidavit, the memorandum in support thereof, and the return of the warrant as well as the instant Motion to Seal, and the Order to Seal, until such time as the Court orders otherwise.

CONCLUSION

WHEREFORE, the United States respectfully requests that the search warrant, the application for the search warrant, the affidavit in support of the search warrant, the memorandum in support thereof, the return of the search warrant and this Motion to Seal and proposed Order be sealed until the United States moves to unseal. A proposed Order is submitted herewith.

Respectfully submitted,

CHANNING D. PHILLIPS
ACTING UNITED STATES ATTORNEY
D.C. Bar Number 415-793

By: _____
G. MICHAEL HARVEY
Assistant United States Attorney
D.C. Bar Number 447-465
National Security Section
United States Attorney's Office
555 4th Street, N.W., Room 11-439
Washington, D.C. 20530
(202) 305-4155 (phone)
michael.harvey2@usdoj.gov

EXHIBIT C

IN THE UNITED STATES DISTRICT COURT FOR THE
DISTRICT OF COLUMBIA

APPLICATION FOR SEARCH WARRANT FOR E-MAIL ACCOUNT [redacted]@YAHOO.COM MAINTAINED ON COMPUTER SERVERS OPERATED BY YAHOO!, INC., HEADQUARTERED AT 701 FIRST AVENUE, SUNNYVALE, CA	)	09-516-M-01
		UNDER SEAL

FILED
NOV 09 2009
Clerk, U.S. District and Bankruptcy Courts

ORDER TO SEAL

Having considered the Government's Motion for an Order to Seal Search Warrant and Related Materials and for Non-disclosure ("Government's Motion"), in connection with the above-captioned matter, and having found that sealing the search warrant and all attachments thereto, the application for the search warrant, the affidavit in support of the search warrant, the memorandum in support thereof, the subsequent return of the search warrant, and the government's motion and proposed order will further the legitimate prosecutorial interest in preserving the integrity of an ongoing criminal investigation, and having therefore concluded that there is a compelling governmental interest in sealing said documents, and having further concluded that notification of the government's access to the e-mail account in question would seriously jeopardize an ongoing criminal investigation,

the Government's Motion is **HEREBY GRANTED;** it is further

ORDERED that the Search Warrant and attachments thereto, the Application for the Search Warrant, Affidavit in Support of the Search Warrant in this matter, the Memorandum in Support Thereof, the subsequent Return of the Search Warrant, the Government's Motion and this Order be sealed until further order of this Court; it is further

ORDERED that, pursuant to Title 18, United States Code, Section 2705(b), Yahoo!, Inc., and its employees and agents are prohibited from notifying the subscriber(s) of the above-listed

3

e-mail address, or any other unauthorized person, in any manner, of the existence of the search warrant or application and any work or request for work conducted in response to the search warrant; and it is further

ORDERED that the Clerk's Office shall provide to the U.S. Attorney's Office three (3) certified copies of the Search Warrant and related pleadings in this case.

Nothing in this Order shall prohibit the government from providing this Order or the Search Warrant and its attachment, to Yahoo!, Inc., or Yahoo!, Inc., from providing the same to its authorized employees, so that the warrant can be executed.

Dated: November 9, 2009

U.S. DISTRICT COURT MAGISTRATE JUDGE

ALAN KAY
U.S. MAGISTRATE JUDGE

NOV 0 9 2009

Serve: G. Michael Harvey
Assistant United States Attorney
National Security Section
555 4th Street, N.W., Room 11-439
Washington, D.C. 20530
(202) 305-4155
michael.harvey2@usdoj.gov

EXHIBIT D

SEALED

FILED

NOV 09 2009

Clerk, U.S. District and Bankruptcy Courts

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

APPLICATION FOR SEARCH WARRANT FOR E-MAIL ACCOUNT [redacted]@YAHOO.COM MAINTAINED ON COMPUTER SERVERS OPERATED BY YAHOO!, INC., 701 FIRST AVENUE, SUNNYVALE, CALIFORNIA	)	**Magistrate No.: 09 616 M (DAR)**
		UNDER SEAL

GOVERNMENT'S MEMORANDUM IN SUPPORT OF ITS REQUEST FOR ISSUANCE OF A SEARCH WARRANT FOR ELECTRONIC EVIDENCE[1]

The United States of America, by and through the United States Attorney for the District of Columbia, hereby submits this memorandum in support of its request that the Court issue the accompanying search warrant for the electronic mail ("e-mail") account identified as, [redacted]@yahoo.com, provided service by Yahoo! Incorporated, (hereinafter "Yahoo"), located at 701 First Avenue, Sunnyvale, California. The accompanying warrant includes language authorizing the search and seizure of, among other things, electronically stored information. Such warrants are the topic of a recently issued Ninth Circuit en banc decision in United States v. Comprehensive Drug Testing, Inc., Nos. 05-10067, 05-15006, 05-55354, 2009WL2605378 (9th Cir. Aug. 26, 2009) (en banc) (hereinafter "CDT"), which appears to

---

[1] A similar memorandum, accompanying search warrant applications for electronic evidence, was submitted to Chief Judge Royce C Lamberth in Misc. Nos. 09-515, 09-516, and 09-517, on September 16, 2009. The memorandum and warrant applications were filed with the Chief Judge because in light of the CDT opinion, the matter presented an emerging legal issue with broad implications for new warrant applications in this district. On September 16, 2009, Chief Judge Lambert signed the warrants authorizing the search for electronic evidence consistent with the approach outlined in this instant application. A similar memorandum was also filed accompanying search warrant applications for electronic evidence in two cases before Magistrate Judge John M Facciola in Mag Nos. 09-536 and 09-547. On September 28, 2009 and October 6, 2009, respectively, Judge Facciola signed the warrants in those two cases authorizing the search for electronic evidence consistent with the approach outlined in this instant application. Last month, a similar memorandum accompanied a search warrant application for electronic evidence in a case before Magistrate Judge Deborah A. Robinson in Mag. No. 09-584. On October 23, 2009, Judge Robinson signed the warrant in that case authorizing the search for electronic evidence consistent with the approach outlined in this instant application It is the undersigned's understanding that, earlier this month, Magistrate Judge Alan Kay also signed search warrants in cases authorizing the search for electronic evidence consistent with the approach outlined herein as well.

prescribe a code of conduct that the government must follow for such searches.[2] The government subsequently moved to stay the mandate in CDT to consider whether to file a petition for a writ of certiorari to the United States Supreme Court, arguing that such a petition would "present a substantial question" and provide "good cause for a stay." See Fed. R. App. P. 41(d)(2). On September 2, 2009, the Ninth Circuit granted the government's motion to stay the mandate pending the filing of a timely petition for certiorari.

In addition to being currently stayed, the CDT opinion is not precedential in the District of Columbia Circuit and thus not binding on this Court. Notwithstanding these deficiencies in the CDT case, because the CDT opinion appears to set out a broad code of conduct relating to the execution of all searches of electronically stored information, the United States is submitting this brief to further explain why CDT is distinguishable from the instant matter and to outline why several of the procedural requirements and restrictions mandated by the Ninth Circuit in CDT appear to be unworkable and in conflict with both the Federal Rules of Criminal Procedure and existing Fourth Amendment case law.

THE CDT OPINION

A. Facts

CDT affirms three district court orders, one of them quashing subpoenas and the other two ordering the return of property seized pursuant to a search warrant. Although the facts involved a criminal investigation, CDT did not involve criminal defendants. The litigation was a dispute between the United States and parties not charged with any violations of criminal law.

---

[2] The en banc court was divided in the case, with three judges filing partial dissenting opinions.

As part of its investigation into the illegal distribution of steroids, the United States subpoenaed two companies, Comprehensive Drug Testing, Inc., and Quest Diagnostics, Inc., for the testing results for all baseball players. CDT, 2009WL2605378, at *1. After negotiations over the subpoenas broke down, Comprehensive Drug Testing, Inc. and the baseball players' union moved to quash the subpoena. Id. The United States then applied for and received two search warrants that would allow it to search Comprehensive Drug Testing's facilities in Long Beach, California and Quest's laboratory in Las Vegas, Nevada, for the test results of ten named baseball players. Id.

In executing the Long Beach warrant, the agents copied a file directory off a network server. Id. at *5. The file directory included, among hundreds of other documents, an Excel spreadsheet that contained the names of baseball players who had tested positive for steroids. Id. The agents took an electronic copy of the entire directory off-site for later review. They did not take a computer, or image a hard drive.

Both the District of Nevada and the Central District of California ordered the return of the property seized pursuant to the warrants. Id. at *2. Additionally, the Northern District of California ordered that the subpoenas be quashed. Id. Sitting en banc, the Ninth Circuit held that the order in the Central District of California had not been appealed on time, and dismissed that appeal. Id. The court affirmed the other two orders. Id. at *16.

The en banc court went further, however, and addressed the question of how a search of computer records should proceed. It stated that an "inherent part of the electronic search process" is "over-seizing" — that is, seizing an entire set of electronically stored data, even though probable cause exists to believe that only some of the data it contains is responsive to the warrant. Id. at *15. After that over-seizure, it is necessary to "segregate" the data that is called

for by the warrant. The bulk of the opinion concerns how the Court believes this process should occur in future searches.

The Court looked to United States v. Tamura, 694 F.2d 591 (9th Cir. 1982), for guidance. Tamura involved paper records rather than computers; as the Court noted, it was decided prior to "the dawn of the information age." Id. at *4. Tamura allowed the government, in a warrant application, to "apply for specific authorization for large-scale removal of material" when "on-site sorting is infeasible." Id. at *5 (quoting Tamura, 694 F.2d at 596). The court characterized the Tamura procedures as requiring an on-site review to determine whether over-seizure was necessary, and spoke favorably of warrant procedures that required off-site sorting be done "by computer personnel." Id.

The court considered the government's argument that "[o]fficers may lawfully seize evidence of a crime that is in plain view... and thus it had no obligation under *Tamura* to return that property." Id. at *6. Although the court did not specifically reject this argument, it criticized it severely. It called the argument "too clever by half," because the "point" of the Tamura procedures "is to maintain the privacy of materials that are intermingled with seizable materials, and to avoid turning a limited search for particular information into a general search of office file systems and computer databases." Id. While expressing "no cavil with this general proposition" that "the government can't be sure whether data may be concealed, compressed, erased or booby-trapped without carefully examining the contents of every file," the court said that "under this theory" everything the government seizes from the premises will come into plain view. Id. That, the court said, would "make a mockery of Tamura." Id. at 7.

B. CDT's Description of New Search Procedures

The court's opinion includes several descriptions of how judicial officers and the government "should" act in the future. The CDT procedures appear to govern every aspect of the process of obtaining, executing, and returning warrants involving electronic evidence. The following is a summary of CDT's new procedures:

Forced waiver of plain view doctrine. In "future" applications, the government "should ... forswear reliance on the plain view doctrine or any similar doctrine that would allow it to retain data to which it has gained access only because it was required to segregate seizable from non-seizable data." Id. at *7. The court also characterized this as saying that judicial officers should "insist that the government waive reliance upon the plain view doctrine in digital evidence cases." Id. at *15. If the government refuses to do this, then the judicial officer should order that the task of segregating the data be done by "an independent third party under the supervision of the court," or "deny the warrant altogether." Id. at *7. Here, the court was motivated by a concern that the government's ability to rely upon the plain view exception converted every warrant into a general warrant. Id. at *13.

The court did *not* hold that the plain view doctrine does not apply in searches of electronically stored information. To the contrary, it appears to acknowledge that the plain view doctrine does apply; that is why it instructed judicial officers to demand a "waiver" or "forswear[ing]" of the doctrine. The court described plain view as a "doctrine that would allow [the government] to retain data to which it has gained access only because it was required to segregate seizable from non-seizable data." Id. at *7. While harshly criticizing the government for misconduct in "counting on the search to bring constitutionally protected data into the plain view of the investigating agents," it did not dispute that, once in plain view, the data would be seizable. Id. at *8.

1. Contents of the affidavit supporting probable cause

Disclosure of risk. Although a warrant application may mention theoretical risks of data destruction or tampering, the government must also disclose "the actual degree of such risks in the case presented to the judicial officer." Id. at *7 (emphasis in original). The court particularly faulted the government in that case for describing theoretical risks that data could be destroyed, but not mentioning that it had accepted Comprehensive Drug Testing's representation that it would preserve the data pending resolution of its motion to quash the subpoena. Such a pledge, whether believed or not, is "highly relevant information," both to the need for off-site review and to "whether a warrant is needed at all." Id. at *7.

Disclosure of prior efforts. An affidavit must disclose "prior efforts in other judicial fora to obtain the same or related information, and what those efforts have achieved." Id. at *12. In particular, the court criticized what it saw as the failure of the search warrant affidavits to inform the reviewing judicial officer of the prior use of subpoenas for similar information, and of other warrants in other districts. Id.

2. Seizure of co-mingled data

Justifying site seizure of co-mingled data. The court agreed with the government that "over-seizing is an inherent part of the electronic search process," and one that "will be far more common" than were *en masse* seizures of paper records before the advent of computer storage. Id. at *15. This "over-seizure" must be justified in the affidavit. Here, the government made "a strong case" for it by explaining the possibility that files can be disguised through misleading names or file name extensions, the possibility that data could be erased or hidden, that "booby traps" might erase data, that certain files might not be accessible without the proper software,

that there may be too much information to be examined on site, that data might be encrypted or compressed, and that forensics requires "precise, scientific procedures." Id. at *3.

3. The procedure for executing the warrant

Independent third-party review. The CDT court held that in some cases a judicial officer may order that the off-site review of "over-seized" data be performed by independent third parties not affiliated with the government, rather than by government agents. Id. at *7, 9, 15. The choice appears to be that of the judicial officer, and not of the government; in fact, in cases where (1) the party being searched is not suspected of any crime, and (2) the privacy interests of "numerous" other parties "who are not under suspicion of criminal wrongdoing" are implicated, the CDT court stated that courts should presume that the segregation should be conducted by or closely supervised by "an independent third party selected by the court." Id. at *9.

In cases where the government is permitted to conduct the off-site review itself, the court imposes three requirements:

Narrow search protocol. First, the process of segregating the data must be "designed to achieve" one purpose only: separating data called for by the warrant from data not called for by the warrant. Id. at *7. The court also described this requirement as saying that the "search protocol must be designed to uncover only the information for which it has probable cause." Id. at *16. If the government (as was the case in CDT) was allowed to discover data pertaining to only ten names, then it must employ a search protocol "designed to discover data pertaining to those names only, not to others, and not those pertaining to other illegality." Id. at *7. The court particularly criticized the use of "hashing tools" to identify child pornography on a hard drive, and said that such a tool may not be used "without specific authorization in the warrant" supported by probable cause to believe such files will be found. Id.

Wall between investigators and reviewers. Second, the warrant must include a written protocol preventing "agents involved in the investigation" from examining or retaining "any data other than that for which probable cause is shown." Id. at *9. The court also phrased this by saying that only "information for which [the government] has probable cause" may be "examined by the case agents." Id. at *16.

Redaction. The court refers to the process of not only "segregating," but also "redacting" data. Id. at *9, 15. The court does not explain when data must be "redacted," or through what technique. Its repeated use of the words "data" and "information," rather than "file," suggest that the decision about whether material is responsive to the warrant must be made at the smallest quantum possible, possibly including byte-by-byte determinations.

Time limitation.

The court requires that future warrants must specify a time, "which should be as soon as practicable," by which the government must make a return of the warrant. Id. at *9. This appears to require judges to place an upfront time limitation in the execution of the forensic analysis.

4. Return and inventory

Destruction and return requirements. After the process of off-site review for data called for by the warrant is complete, the government is not free to "retain" the information. Id. at *9. With "specific judicial authorization," the government may keep it. Id. Barring that, the government must return "the actual physical medium that may have been seized" to the owner, unless the media contains contraband. Id. Remaining copies in the government's possession must be destroyed. Id. However, the court also allowed that if the "government believes it is entitled to retain data as to which no probable cause was shown in the original warrant," then it

may either "seek a new warrant" or "justify the warrantless seizure by some means other than plain view." Id.

Inventory requirements. The warrant must require the government to file a return that discloses "precisely what data it has obtained as a consequence of the search, and what data it has returned to the party from whom it was seized" and includes a "sworn certificate" stating that the government has returned or destroyed all "copies" of data that it is not entitled to keep. Id.

5. Suppression

CDT did not involve a criminal defendant. Nevertheless, the Ninth Circuit discussed suppression of evidence in several contexts.

Lack of candor. First, CDT suggested that a "lack of candor" in any aspect of the warrant application—but, in particular, in identifying other search warrants or subpoenas—will "bear heavily against the government in the calculus of any subsequent motion to return or suppress the seized data." Id. at *7.

Use of Rule 41(g). The opinion also suggested that a Rule 41(g) motion for return of property provides an alternative means to require the government not to use electronic evidence obtained with a warrant. A motion for return of property, when brought by a party against whom no criminal charges have been brought, is "a petition that the district court invoke its civil equitable jurisdiction." Id. at *9.

According to the CDT opinion, while a motion to suppress is "limited by the exclusionary rule," a motion for return of property "is not." Id. at *10. To the contrary, "Rule 41(g) is broader than the exclusionary rule" and permits motions for the return of lawfully seized property. Id. "[J]udicially-imposed restrictions" that are present in the exclusionary rule do not apply. Id. Further, Rule 41(g) can be used to require the government to return all copies. Id. at

*11. The court also introduced a new ground for Rule 41(g) orders: where the government comes into possession of evidence by "circumventing or willfully disregarding limitations in a search warrant," it can be ordered to give up the evidence and "any fruits thereof." Id. at *12. When the wrongdoing is "intentional," not "technical or [a] good faith mistake," a court should order the return of the property "without the need for balancing that is applicable in the more ordinary case." Id.

II. THE STANDARDS SET FORTH IN CDT DO NOT APPLY TO THE INSTANT CASE

A. CDT is limited to its facts and is readily distinguishable from the instant matter

The CDT opinion involved the search of electronically stored data held by third parties that were not themselves subjects or targets of a criminal investigation. These particular third parties were engaged in businesses that required them to hold highly confidential and sensitive information relating to large numbers of people, yet the governmental interest was limited to information regarding a tiny percentage of the persons on whom they kept data. The warrant sought a specific set of facts about ten named individuals, so it would have been easy to target a limited computer search just for information pertaining to just those individuals. By contrast, the government seized a file which "contained a huge number of drug testing records, not only of the ten players for whom the government had probable cause but hundreds of other professional baseball players, thirteen other sports organizations, three unrelated sporting competitions, and a non-sports business entity...." Id. at *14. The court explained that most of the individuals, about whom drug testing information was seized, had "no relationship to professional baseball except that they had the bad luck of having their test results stored on the same computer as the baseball

players." Id. Moreover, the baseball players had been assured by Major League Baseball that their testing results would remain anonymous and confidential.

The search warrant application in this case also involves the search of electronically stored data held by a third party, specifically Yahoo! Inc. However, in contrast to CDT, the scope of the search is limited to the email accounts of a subject of a government's criminal investigation. The search warrant affidavit sets out the probable cause to believe that the accounts contain evidence of the subject's offenses. Because the search here is limited to the subject's particular email accounts, there will be no "over-seizing" as there was in CDT and the risk that data beyond the scope of the warrant will fall into the hands of the government is *de minimis*. Furthermore, there is no reason to believe that this particular email accounts contains highly sensitive or confidential records of other people unrelated to, and independent of, the criminal activity, as was the case in CDT.

B. Federal Rule of Criminal Procedure 41 and the Fourth Amendment, rather than the new CDT rules, control the procedure for the execution of the warrants

CDT does not make clear whether its guidelines are based on the Fourth Amendment or the court's supervisory powers. The decision is designed to protect privacy, which suggests that it may be Fourth Amendment based, but at the same time the court makes no attempt to root its decision in existing case law or traditional Fourth Amendment analysis. To the extent CDT is based on the Fourth Amendment, it flatly contradicts a significant amount of existing Fourth Amendment case law. See id. at *25 (Bea, J., concurring in part and dissenting in part) (noting that requiring the government to forswear reliance on the plain view doctrine "departs from existing Supreme Court precedent regarding the 'plain view' exception to the Fourth Amendment's warrant requirement, and do so without a single citation to the Supreme Court's

extensive precedent on the subject or an explanation why that precedent no longer applies"). To the extent it is based on the court's supervisory powers, it is impermissible because the guidance contradicts Rule 41.

Rule 41(d)(1) states that "[a]fter receiving an affidavit or other information, a magistrate judge — or if authorized by Rule 41(b), a judge of a state court of record — must issue the warrant if there is probable cause to search for and seize a person or property." Fed. R. Crim. P. 41(d)(1) (emphasis added). This rule creates a single condition — probable cause — that the government must satisfy for a search warrant. The CDT opinion, however, encourages judges to condition the issuance of warrants on the government's agreement to "forswear reliance on the plain view doctrine," and in some circumstances to "deny the warrant altogether." CDT, 2009WL2605378, at *7. The notion of prior judicial approval for the manner in which the government executes a warrant is simply inconsistent with the Supreme Court's rule that "[n]othing in the language of the Constitution or in [the Supreme Court's] decisions interpreting that language suggests that, in addition to the requirements set forth in the text [of the Fourth Amendment], search warrants also must include a specification of the precise manner in which they are to be executed." United States v. Grubbs, 547 U.S. 90, 98 (2006) (quoting Dalia v. United States, 441 U.S. 238, 255 (1979)).

The Federal Rules of Criminal Procedure are enacted by the Supreme Court, subject to Congressional approval; consequently, when they contradict a rule propounded by a Circuit Court, they control. See 28 U.S.C. § 2072(b) ("[a]ll laws in conflict with such rules shall be of no further force or effect after such rules have taken effect."); Clinton v. City of New York, 524

U.S. 417, 446 n.40 (1998) ("Congress itself made the decision to repeal prior rules upon the occurrence of a particular event — here, the promulgation of procedural rules by this Court."). [3]

Furthermore, if the new CDT procedures are viewed as an announcement of new court rules about "the proper administration of search warrants," CDT, 2009WL2605378, at *2, then there is a question as to whether such procedures violate the separation of powers doctrine. "Congress has undoubted power to regulate the practice and procedure of federal courts," Sibbach v. Wilson & Co., 312 U.S. 1, 9 (1941), and while it has, through the Rules Enabling Act, partially "delegate[d] rulemaking authority to the Judicial Branch," Mistretta v. United States, 488 U.S. 361, 388 (1989), judicial rulemaking must occur within the scope of that delegation to be binding.

C. Caselaw in Other Circuits and District Courts is Contrary to CDT

1. Search protocols

The Ninth Circuit is alone in requiring search protocols. In general, "[n]othing in the language of the Constitution or in [the Supreme Court's] decisions interpreting that language suggests that, in addition to the requirements set forth in the text [of the Fourth Amendment], search warrants also must include a specification of the precise manner in which they are to be

---

[3] It is also worth noting that proposed amendments to Rule 41 that will take effect on December 1, 2009, barring contrary congressional action, would directly contradict other portions of the CDT opinion. The Supreme Court has already approved these rule amendments.

The new rule 41(f)(1)(B) will state that "[i]n a case involving the seizure of electronic storage media or the seizure or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied." The CDT opinion, however, has extensive rules for what the inventory must describe, requiring "precisely what data it has obtained as a consequence of the search, and what data it has returned to the party from whom it was seized." CDT, 2009WL2605378, at *9. Similarly, the new rule will allow agents to retain copies of the data, in contrast to CDT which requires return or destruction of seized information except when the government obtains specific judicial authorization.

executed." Grubbs, 547 U.S. at 98 (quoting Dalia, 441 U.S. at 255). Search protocols are, at their core, directions to the officer about how he or she may execute the warrant, and then subsequently analyze the seized evidence. Grubbs and Dalia make clear, however, that the Fourth Amendment's particularity clause does not require a warrant to say anything about how a warrant can be executed — even if there is the potential to affect Fourth Amendment rights in unexpected ways. "It would extend the Warrant Clause to the extreme to require that, whenever it is reasonably likely that Fourth Amendment rights may be affected in more than one way, the court must set forth precisely the procedures to be followed by the executing officers." Dalia, 441 U.S. at 258.

The Tenth Circuit emphasized in United States v. Brooks, 427 F.3d 1246, 1251 (10th Cir. 2005), that while warrants must describe "with particularity the objects of their search," the methodology used to find those objects need not be described: "This court has never required warrants to contain a particularized computer search strategy." The Tenth Circuit recently elaborated in United States v. Burgess, No. 08-8053, 2009 WL 2436674, at *11 (10th Cir. Aug. 11, 2009), in which it noted that "[i]t is unrealistic to expect a warrant to prospectively restrict the scope of a search by directory, filename or extension or to attempt to structure search methods—that process must remain dynamic." Other courts have recognized that "[c]omputer searches . . . are technical and complex and cannot be limited to precise, specific steps or only one permissible method." United States v. Triumph Capital Group, Inc., 211 F.R.D. 31, 47 (D. Conn. 2002). "To require such a pinpointed computer search, restricting the search to a [particular] program or to specific search terms, would likely . . . fail[] to cast a sufficiently wide net to capture the evidence sought," United States v. Adjani, 452 F.3d 1140, 1149-50 (9th Cir. 2006), and "would give criminals the ability to evade law enforcement scrutiny," United States

v. Graziano, 558 F. Supp. 2d. 304, 315 (E.D.N.Y. 2008). See also United States v. Vilar, 2007WL1075041, at *38 (S.D.N.Y. Apr. 4, 2007) ("[I]t seems manifestly obvious that any requirement that a computer search be confined by a key-word search protocol would inevitably immunize criminals.").

In United States v. Khanani, 502 F.3d 1281, 1290-91 (11th Cir. 2007), the Eleventh Circuit rejected the argument that a warrant should have included a search protocol, pointing in part to the careful steps agents took to ensure compliance with the warrant. See also United States v. Cartier, 543 F.3d 442, 447-48 (8th Cir. 2008) ("While we acknowledge that there may be times that a search methodology or strategy may be useful or necessary, we decline to make a blanket finding that the absence of a search methodology or strategy renders a search warrant invalid per se."); United States v. Upham, 168 F.3d 532, 537 (1st Cir. 1999) ("The warrant process is primarily concerned with identifying what may be searched or seized — not how."); cf. Vernonia School Dist. 47J v. Acton, 515 U.S. 646, 663 (1995) (noting that the Supreme Court has "repeatedly refused to declare that only the 'least intrusive' search practicable can be reasonable under the Fourth Amendment").

Additionally, many district court opinions reject the need for search protocols. See United States v. Aguirre, No. CR 108-053, 2008WL4790659, at *14 (S.D. Ga. Nov. 3, 2008); United States v. Jack, No. CR.S-07-0266 FCD, 2009WL453051, at *4-5 (E.D. Cal. Feb. 23, 2009); United States v. Hanna, No. 07-CR-20355, 2008WL2478330, at *7 (E.D. Mich. Jun. 17, 2008); United States v. Kaechele, 466 F.Supp.2d 868, 888 (E.D. Mich. 2006). See also United States v. Cioffi, No. 08-CR-415, 2009WL3416241, at *5 (E.D.N.Y. Oct. 26, 2009) (noting that the Second Circuit has not taken a position on search protocols, but suppressing electronic

evidence on particularity grounds, where the application did not limit the search to a particular crime).

2. Plain view and the "wall"

As noted above, CDT did not hold that the plain view doctrine does not apply to searches of electronically stored information; to the contrary, it implicitly acknowledged that it applied, and for that reason instructed judges to exact a promise from prosecutors to waive plain view. However, the opinion did seek to make the plain view doctrine less useful to the government by requiring that a separate group of investigators examine the whole set of data and communicate only files specifically called for by the warrant to the case agent. Such filter team procedures have previously been used only in privilege situations, not searches pursuant to a warrant for private information. Even Title III orders do not require such a procedure.

Courts considering this issue have found constitutional a procedure in which investigators seize an entire hard drive and then later search through it for material called for by the warrant, without imposing upon investigators any wall of separation between a review team and an investigation team. See Khanani, 502 F.3d at 1290 (endorsing a search in which "a computer examiner eliminated files that were unlikely to contain material within the warrants' scope"); Brooks, 427 F.3d at 1251-53 (approving "a warrant that authorized officers to search through computer files for particular items specifically related to child pornography"); Guest v. Leis, 255 F.3d 325, 335 (6th Cir. 2001) ("[Law enforcement officers] may legitimately have checked to see that the contents of the directories corresponded to the labels placed on the directories. Suspects would otherwise be able to shield evidence from a search simply by 'misfiling' it in a directory labeled 'e-mail.' "); Jack, 2009WL453051, at *4 ("[I]t is reasonable for the executing officers to open the various types of files located in the computer's hard drive in order to

determine whether they contain such evidence."); United States v. Fumo, 565 F.Supp.2d 638, 649 (E.D. Pa. 2008) ("[B]ecause of the nature of computer files, the government may legally open and briefly examine each file when searching a computer pursuant to a valid warrant"); Manno v. Christie, 2008WL4058016 (D. N.J. Aug. 22, 2008) (finding it "reasonable for [agent] to briefly review each electronic document to determine if it is among the materials authorized by the warrant, just as he could if the search was only of paper files"); United States v. Potts, 2008WL2051090, at *11 (D. Kan. May 13, 2008) (holding that warrant did not authorize an overbroad search when it allowed the investigator "to search the computer by ... opening or cursorily reviewing the first few 'pages' of such files in order to determine the precise content" (internal quotation marks omitted)); United States v. Triumph Capital Group, Inc., 211 F.R.D. 31, 47 (D.Conn.2002); United States v. Gray, 78 F.Supp.2d 524, 529 (E.D.Va.1999); United States v. Hunter, 13 F.Supp.2d 574, 584 (D. Vt. 1998).

3. Time limitations

The CDT opinion's brief suggestion that a warrant specify a date by which all seized data is returned or destroyed implies a requirement that all forensic review occur within a specified time. Several other courts have held, however, that "the Federal Rules of Criminal Procedure do not require that the forensic analysis of computers and other electronic equipment take place within a specific time limit. Any subsequent search only needs to be conducted within a reasonable time." United States v. Mutschelknaus, 564 F.Supp.2d 1072, 1077 (D. N.D. 2008); see also United States v. Murinko, 2009WL2487042, at *5 (E.D. Wash. Aug. 12, 2009) ("The forensic review of the material obtained from the hard drive took several months, but the actual search of the computer was completed within the time dictates of the search warrant"); In the Matter of the Search of Scranton Housing Authority, 436 F. Supp. 2d 714 (E.D. Pa. 2006);

United States v. Hernandez, 183 F. Supp.2d 468, 480 (D.P.R. 2002); Triumph Capital Group, Inc., 211 F.R.D. at 66; United States v. Habershaw, 2001WL1867803, at *8 (D. Mass. May 13, 2001).

4. Independent third party review

The CDT opinion's suggestion that in some cases judges supervise a search, or even order an "independent" review by non-governmental third parties, is novel, and no cases directly reject it. However, the notion poses several problems.

The Fourth Amendment requires that a warrant be issued by a detached and neutral judicial officer. "Whatever else neutrality and detachment might entail, it is clear that they require severance and disengagement from activities of law enforcement." Shadwick v. Tampa, 407 U.S. 345, 350 (1972). The indirect involvement of a judicial officer in determining what data falls within a warrant threatens that detachment. Indeed, if a defendant later wishes to challenge that determination, he might persuasively argue that he would be denied due process if the same judicial officer who oversaw the decision to seize a particular piece of evidence also sat in judgment of whether that seizure was proper.

In Lo-Ji Sales, Inc. v. New York, 442 U.S. 319 (1979), a magistrate judge authorized the seizure of obscene items and then went to the search site and made determinations of obscenity. The Supreme Court condemned this practice, stating that in so doing the magistrate judge "was not acting as a judicial officer but as an adjunct law enforcement officer." Id. at 327. The magistrate judge "here undertook to telescope the processes of the application for a warrant, the issuance of the warrant, and its execution," and, as a result, "[i]t is difficult to discern when he was acting as a 'neutral and detached' judicial officer and when he was one with the police and prosecutors in the executive seizure." Id. at 328. Under Lo-Ji, it is improper for a judicial

officer to become "a member, if not the leader, of the search party which [is] essentially a police operation." Id. at 327.

The legal authority of a court to "appoint" such an independent third-party examiner is also unclear. Although the Federal Rules of Civil Procedure allow the appointment of a special master in some cases, see Fed. R. Civ. P. R. 53, no equivalent authority exists in the criminal rules. The third-party examiner might be justified because "district courts retain inherent authority to appoint technical advisors in appropriate cases," Ass'n of Mexican-American Educators v. California, 231 F.3d 572, 591 (9th Cir. 2000) (en banc), but the role of technical advisor has never been held to encompass traditional police operations such as analyzing evidence for use in criminal prosecution.

D. The CDT Rules are Simply Unworkable

The CDT court announced its set of procedures without the benefit of briefing and with a minimal record concerning how searches of electronically stored information are performed. This is particularly unfortunate because the facts before the court concerned an atypical search that bears little resemblance to the searches of electronic stored information that are preformed, thousands of times a year, in investigations of terrorism, computer hacking, identity theft, drug distribution, child pornography, and many other crimes in which relevant issues include who used a computer, what purpose they used it for, how they put the computer to that purpose, and when they did so. Such "a search can be as much an art as a science," Brooks, 427 F.3d at 1252, and is necessarily integrated into an investigator's detective work. See also Vilar, 2007WL1075041, at *38. Just as a forensic pathologist can study the body of a deceased to find physical evidence of many aspects of the person's life, so too can a forensic examiner study the bits and bytes written into electronic evidence to find information about the user. Forensic

examination requires not just mechanical searches for easily-identifiable documents, but intuition and on-the-spot judgment in deciding, based on what one has just seen, the best step to take next. While the complex nature of searches of electronically stored information forces judges to confront difficult legal issues, such as the practical necessity to "over-seize" data, combined with the ability of investigators sifting through that data to rely upon "plain view," the answer is not to issue sweeping rules requiring one-size-fits-all search protocols, but to consider, after the fact, the reasonableness of the government's conduct in each case. The following paragraphs describe some of the unworkable aspects of CDT's rules.

1. Plain view waiver

In particular, forced "plain view" waivers are simply unworkable. If plain view is "waived," for example, a search in a terrorism case that uncovers evidence of money laundering, or ongoing child abuse or human trafficking would require the United States Government to essentially ignore its existence, even though that evidence was obtained consistent with the Constitution.

2. Rules governing who may search, how, and when

CDT's prescription of the use of "independent" third parties, time limitations, requirements of a detailed inventory accompanying the return, instructions about the need for a wall between investigators and probable cause reviewers, the requirement of a written search protocol, and the requirements of redaction all either misapprehend the nature of a forensic computer examination or incorrectly assume that all searches are as simple as identifying a single spreadsheet containing ten drug test results. For example, if a forensic examiner is assigned the task of confirming that an illegal act was committed by a particular individual at a computer's keyboard, and not by someone remotely controlling the computer through malware, it may be

necessary to search every single file and boot sector to rule out the possibility. Evidence that a computer has not been tampered with in this way is not "data" that can be merely reviewed by a review team and passed along to investigators; it is, if anything, an expert conclusion, based on a review of available facts and the application of accepted principles.

The requirement of a separate forensic review team, isolated from the investigative team, presents a significant challenge to government resources. A limited number of forensic examiners are available, and the volume of work required of them is already pushing them to capacity and beyond. Doubling the need for forensic examiners will significantly hurt government's ability to investigate any crime that involves a computer.

3. Non-government "independent" third party forensic reviewers

The use of third-party reviewers — independent of the government — is particularly unworkable. A hard drive may, whether investigators know it or not, contain contraband that cannot legally be possessed by non-governmental parties. Such contraband could include child pornography. However, the Adam Walsh Act requires that "[i]n any criminal proceeding, any property or material that constitutes child pornography... shall remain in the care, custody, and control of either the Government or the court." 18 U.S.C. § 3509(m). Giving child pornography to an "independent" third party, by definition "not affiliated with the government," would certainly violate this federal statute in a child pornography investigation, and may inadvertently violate the provision in other cases.

Other sorts of information should also not be disclosed to a non-government reviewer. In order to determine whether or not a piece of information is within the scope of the warrant, the third-party reviewer might need to have a complete understanding of the investigation to date. It may well be inappropriate, and perhaps illegal, to disclose case information such as grand jury

material, tax information, and the results of court-ordered wiretaps outside of law enforcement to a third-party independent of the government. See Fed. R. Crim. P. R. 6(e) (grand jury information); 26 U.S.C. § 6103(h)(2) (tax returns); 18 U.S.C. § 2517 (wiretaps). Even apart from these privacy statutes, it may be necessary that an examiner be familiar with highly sensitive information, such as the identity of a confidential informant, or the nature of classified information. Indeed, as the facts in CDT show, an examination might turn up highly private information about innocent third parties, such as drug testing records or medical patient records.

These problems are related to another: evidence security. To protect the privacy of victims, the privacy of witnesses, and public safety, law enforcement takes care in how it stores forensic images of electronic media. Without appropriate care, an examiner might accidentally run malware, leak information over the Internet, or disseminate copies of child pornography. Although every law enforcement agency takes the necessary precautions to avoid such a problem, the independent third-party reviewer chosen by the court might not.

CDT contemplates a central role for the independent third-party examiner: for at least part of the time, this examiner will be the only person with access to the forensic copy of the electronically stored information. Therefore, proving chain of custody and authentication might require testimony from the independent examiner. It is crucial, therefore, that the independent examiner employ procedures that can give confidence in the integrity of the electronic evidence, and be able to testify about those procedures. Because law enforcement will have no role in selecting the examiner, there is a danger that, through no fault of the government, the electronic evidence will not be admitted at trial.

Indeed, it is unclear how, if at all, the conduct of an independent third-party examiner will be regulated. If the independent third-party examiner exceeds the scope of the warrant with

reckless disregard, for example, it is unclear whether suppression would follow (as it normally would if a law enforcement officer did the same). Moreover, employing judicially appointed examiners will be extremely expensive and inefficient. In order for the third-party examiner to complete the task, he or she must have a high degree of computer forensic skill. Although there is a burgeoning field of consultants who advertise expertise in "e-discovery," they tend to specialize in skills that are most useful in civil litigation (such as indexing Outlook PST files or organizing large document productions) and may be unfamiliar with the cutting-edge forensic techniques developed and used by law enforcement agencies. Even when qualified forensic examiners are available in the private sector, they will be expensive to hire. In certain cases where non-technically-trained special masters have been employed to separate legally privileged materials, bills have reached tens or even hundreds of thousands of dollars, and such reviews create substantial delays. The CDT opinion leaves unclear who will choose the examiners to assure that they have appropriate skills, and whether the government can object to the skill level of the examiner chosen by the court.

III. CONCLUSION

For the foregoing reasons, the government respectfully requests that the Court reject the procedures set forth in CDT relating to searches of electronically stored information and that it rely on the Fourth Amendment, Rule 41 and existing caselaw to issue the accompanying search warrant that contains search protocols similar to those routinely used in this district.

Respectfully Submitted

CHANNING D. PHILLIPS
ACTING UNITED STATES ATTORNEY
D.C. Bar No. 415-793

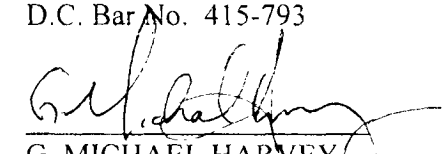
By: 
G. MICHAEL HARVEY
Assistant United States Attorney
D.C. Bar No. 447-465
National Security Section
555 4th Street, N.W.
Washington, D.C. 20530
(202) 305-4155 (phone)
michael.harvey2@usdoj.gov

EXHIBIT E

SEALED

AO93(Rev 5/85)Search Warrant

UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF COLUMBIA

In the Matter of the Search of
(Name, address or brief description of person or property to be searched)

E-mail Account [redacted]@yahoo.com
Maintained on Computer Servers Operated
by YAHOO! Inc., Headquartered at
701 First Avenue,
Sunnyvale, California

SEARCH WARRANT

CASE NUMBER: 09-316 M-01

TO: Casey P. Farrell and any Authorized Officer of the United States

Affidavit(s) having been made before me by FBI Special Agent Casey P. Farrell who has reason to believe that ☐ on the person or ☒ on the premises known as (name, description and or location)
e-mail account identified by user account [redacted]@yahoo.com maintained on computer servers operated by YAHOO!, Inc., Headquartered at 701 First Avenue, Sunnyvale, California, and more fully described in ATTACHMENT A to this application

in the Northern District of California, there is now concealed certain property the disclosure of which is governed by 18 U.S.C. §§ 2701-2711, namely (describe the person or property)

contents of electronic e-mails and other electronic data more fully described in the Application and ATTACHMENT A to this Application (which are both incorporated into this Warrant as if set forth fully herein).

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

YOU ARE HEREBY COMMANDED to search on or before NOV 13 2009
(Date)
(not to exceed 10 days) the person or place named above for the person or property specified, serving this warrant and making the search ☑ (in the daytime - 6:00 A.M. to 10:00 P.M.) ☐ (at any time in the day or night as I find reasonable cause has been established) and if the person or property be found there to seize same, leaving a copy of this warrant and receipt for the person or property taken, and prepare a written inventory of the person or property seized and promptly return this warrant to the undersigned U.S. Judge/U.S. Magistrate Judge, as required by law.

4:45 pm
Date and Time Issued

at Washington, D.C.

ALAN KAY
US MAGISTRATE JUDGE
Name and Title of Judicial Officer

Signature of Judicial Officer

AO 109 (2/90) Seizure Warrant

RETURN

DATE WARRANT RECEIVED	DATE AND TIME WARRANT EXECUTED	COPY OF WARRANT AND RECEIPT FOR ITEMS LEFT WITH
11/9/2009	11/9/2009 1125	[illegible]

INVENTORY MADE IN THE PRESENCE OF

[illegible]

INVENTORY OF PROPERTY SEIZED PURSUANT TO THE WARRANT

ONE DVD-R CONTAINING: [redacted]. [illegible] (1) [illegible]

(2) [illegible]

(3) [illegible]

(4) [illegible]

(5) [illegible]

FILED

DEC - 7 2009

Clerk, U.S. District and Bankruptcy Courts

CERTIFICATION

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

[illegible]

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

[illegible]
U.S Judge or U S. Magistrate Judge

12/07/09
Date

EXHIBIT F

THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

APPLICATION FOR SEARCH WARRANT FOR E-MAIL ACCOUNT [redacted]@YAHOO.COM MAINTAINED ON COMPUTER SERVERS OPERATED BY YAHOO!, INC., HEADQUARTERED AT 701 FIRST AVENUE, SUNNYVALE, CA	)	Mag. No.: 09-616-M-01
	)	UNDER SEAL

FILED

GOVERNMENT'S MOTION FOR UNSEALING OF SEARCH WARRANT AND RELATED MATERIALS

The United States, by and through its attorney, the United States Attorney for the District of Columbia, respectfully requests the Court to unseal in the above-captioned matter: (1) the application for search warrant, (2) the affidavit in support of the application for search warrant, (3) the search and seizure warrant, and (4) the Attachment A thereto (hereinafter "search warrant material"). The Government seeks the unsealing of the search warrant material to fulfill its discovery obligations in a pending criminal case, United States v. Stephen Jin-Woo Kim, Cr. No. 10-225 (CKK), to which the search warrant relates. See F.R.Cr.P. 12(b)(4). To protect the privacy of those involved, the Government requests that dates of birth and email addresses appearing in the search warrant material be redacted before it is placed on the public record. Cf. F.R.Cr. P. 49. To assist the Court, and consistent with F.R.Cr.P. 49.1(d), the Government attaches hereto redacted versions of the search warrant material for entry on the public docket. Further, the Government requests that it be permitted to produce to the defense in United States v. Stephen Jin-Woo Kim unredacted versions of the search warrant material pursuant to the Rule 16 Protective Order entered in that matter on October 13, 2010. See United States v. Stephen Jin-Woo Kim, Cr. No. 10-225 (CKK), Docket #11.

A proposed Order is submitted herewith this motion.

WHEREFORE, the Government respectfully requests (1) that the application for search

warrant in this matter, the affidavit in support of the application for search warrant, the search and seizure warrant, and the Attachment A thereto, be unsealed; (2) that the attached redacted versions of the search warrant material be placed on the public record; and (3) that the Government be permitted to produce unredacted versions of the search warrant material to the defense in United States v. Stephen Jin-Woo Kim pursuant to the Rule 16 Protective Order in that matter.

Respectfully submitted,

RONALD C. MACHEN JR.
UNITED STATES ATTORNEY
D.C. Bar Number 447-889

By: _____
G. MICHAEL HARVEY
Assistant United States Attorney
D.C. Bar Number 447-465
National Security Section
United States Attorney's Office
555 4th Street, N.W., Room 11-848
Washington, D.C. 20530
Phone: (202) 252-7810
Michael.Harvey@usdoj.gov

_____
JONATHAN M. MALIS
Assistant United States Attorney
D.C. Bar Number 454-548
National Security Section
United States Attorney's Office
555 4th Street, N.W., Room 11-447
Washington, D.C. 20530
Phone: (202) 252-7806
Jonathan.M.Malis@usdoj.gov

DEBORAH CURTIS
Trial Attorney
CA Bar Number 172208
Counterespionage Section
U.S. Department of Justice
600 E Street, N.W.
Washington, D.C. 20530
Phone: (202) 233-2133
Deborah.Curtis@usdoj.gov

Attachment A

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

In the Matter of the Search of
(Name, address or brief description of person, property, or premises to be searched)

E-mail Account [redacted]@yahoo.com
Maintained on Computer Servers Operated
by YAHOO!, INC., Headquartered at
701 First Avenue,
Sunnyvale, California

(Further described below)

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

CASE NUMBER: 09-616-M-01

I Casey P. Farrell being duly sworn depose and say:

I am a(n) Special Agent with the Federal Bureau of Investigation and have reason to believe
(Official Title)
that ☐ on the person of or ☒ on the property or premises known as (name, description and or location)
e-mail accounts identified by user account [redacted]@yahoo.com maintained on computer servers operated by YAHOO, Inc, Headquartered at 701 First Avenue, Sunnyvale, California, and more fully described in ATTACHMENT A to this application

(describe the person or property to be searched)
in the Northern District of California, there is now concealed certain property, the disclosure of which is governed by Title 18, United States Code, Sections 2701 through 2711, namely contents of electronic e-mails and other electronic data more fully described in ATTACHMENT A to this application

which is (state one or more bases for search and seizure set forth under Rule 41(c) of the Federal Rules of Criminal Procedure)
evidence, fruits, and instrumentalities of the crimes of Unauthorized Disclosure of National Defense Information, in violation of Title 18 United States Code, Section(s) 793. The facts to support a finding of Probable Cause are as follows:

SEE ATTACHED AFFIDAVIT HEREIN INCORPORATED BY REFERENCE AS IF FULLY RESTATED HEREIN

Continued on the attached sheet and made a part hereof. ☒ YES ☐ NO

G. Michael Harvey
National Security Section
(202) 305-4155

Signature of Affiant
Casey P. Farrell, Special Agent
Federal Bureau of Investigation

Sworn to before me, and subscribed in my presence

NOV 09 2009
Date

at Washington, D.C.

ALAN KAY
U.S. MAGISTRATE JUDGE
Name and Title of Judicial Officer

Signature of Judicial Officer

AO93(Rev.5/85)Search Warrant

SEALED

UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF COLUMBIA

In the Matter of the Search of
(Name, address or brief description of person or property to be searched)

E-mail Account [redacted]@yahoo.com
Maintained on Computer Servers Operated
by YAHOO! Inc., Headquartered at
701 First Avenue,
Sunnyvale, California

SEARCH WARRANT

CASE NUMBER: 09-616-M-01

TO: Casey P. Farrell and any Authorized Officer of the United States

Affidavit(s) having been made before me by FBI Special Agent Casey P. Farrell who has reason to believe that ☐ on the person or ☒ on the premises known as (name, description and or location)
e-mail account identified by user account [redacted]@yahoo.com maintained on computer servers operated by YAHOO!, Inc., Headquartered at 701 First Avenue, Sunnyvale, California, and more fully described in ATTACHMENT A to this application

in the Northern District of California, there is now concealed certain property the disclosure of which is governed by 18 U.S.C. §§ 2701-2711, namely (describe the person or property)

contents of electronic e-mails and other electronic data more fully described in the Application and ATTACHMENT A to this Application (which are both incorporated into this Warrant as if set forth fully herein).

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

YOU ARE HEREBY COMMANDED to search on or before NOV 19 2009
(Date)

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

NOV 05 2009 4:43 pm
Date and Time Issued

at Washington, D.C.

ALAN KAY
U.S. MAGISTRATE JUDGE
Name and Title of Judicial Officer

Signature of Judicial Officer

SEALED

09-616-M-01

ATTACHMENT A: ITEMS TO BE SEIZED

Pursuant to 18 U.S.C. § 2703, it is hereby ordered as follows:

I. SERVICE OF WARRANT AND SEARCH PROCEDURE

a. Yahoo! Incorporated, a provider of electronic communication and remote computing services, located at 701 First Avenue, Sunnyvale, California 94089, (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. 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.

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

Jeffrey B. Williams
FBI-WFO
601 4th Street, NW
Washington, DC 20535
Fax: 202-278-4726
Desk: 202-278-4181

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

d. The original production from the PROVIDER will be sealed -- and preserved for authenticity and chain of custody purposes -- until further order of the Court.

e. Cleared agents of the FBI who are not, and will not be, involved in the criminal investigation will first examine the a copy of the production from the PROVIDER for privilege, in consultation with an Assistant United States Attorney designated for that purpose (and who likewise is not, and will not be, involved in the criminal investigation). Said agents will only release any materials to the FBI case agents in this matter after it has been ascertained that they contain no privileged information or that such information has been removed from the materials. Any materials that do contain privileged information will be sealed and not examined by any agent or government attorney participating in the criminal investigation unless and until the privilege is waived or otherwise determined to be inapplicable. Following that review for privilege, all non-privilege materials will be reviewed by agents responsible for this investigation to ascertain the information to be seized by law enforcement personnel specified in Section III below.

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

g. The U.S. Department of Justice and the Federal Bureau of Investigation shall not be prohibited from sharing information obtained from this warrant with other law enforcement and intelligence agencies, including foreign law enforcement and intelligence agencies, for use in investigation and prosecution.

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

a. All material stored and presently contained in, or on behalf of, [redacted]@yahoo.com ("SUBJECT ACCOUNT"), including videos, computer files sent to and received from other websites, received messages, sent messages, deleted messages, and

messages maintained in trash or other folders, and any attachments thereto;

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

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

d. All business records and subscriber information, in any form kept, pertaining to the SUBJECT ACCOUNT described above in Section II(a), 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;

e. Any and all Yahoo address books and/or Yahoo instant messenger list maintained by the accounts; and

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

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 wire and electronic communications, including attachments and stored files, for the SUBJECT ACCOUNT, 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), that pertain to:

1. records or information related to violations of the aforementioned statute;
2. records or information concerning Stephen Kim's communications and activities on the date of publication of the June 2009 article;
3. records or information related to Stephen Kim's knowledge of rules and/or procedures prohibiting the unauthorized disclosure of classified information;
4. records or information related to Stephen Kim's knowledge of rules and/or procedures regarding communications with the press;
5. records or information related to any disclosure or prospective disclosure of classified information;
6. any classified document, image, record or information, and any communications concerning such documents, images, records, or information
7. 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
8. records or information related to Reporter A or Reporter A's news

organization or any entity or individual affiliated in any way with that organization;

9. records or information related to communications with members of the press or any entity or individual affiliated in any way with a press organization;

10. records or information related to the state of mind of any individuals seeking the disclosure or receipt of classified information;

11. records or information related to the subject matter of the June 2009 article or the foreign country that was the subject matter of the disclosure in the June 2009 article;

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

13. records or information related to the associates of Stephen Kim or any other user identified with the SUBJECT ACCOUNT;

14. records or information related to Stephen Kim or his associates' schedule of travel or travel documents;

15. records or information related to communications to any foreign person or any person residing in a foreign country; and

16. records and information related to any bank records, checks, credit card bills, account information, and other financial records.

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

(g) Source or destination of any wire or electronic mail messages sent from or received by the SUBJECT ACCOUNT, and the date, time, and length of the message; and

(h) Any address to which the wire or electronic mail was or is to be forwarded from the SUBJECT ACCOUNT or email address.

THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

APPLICATION FOR SEARCH WARRANT FOR E-MAIL ACCOUNT [redacted]@YAHOO.COM MAINTAINED ON COMPUTER SERVERS OPERATED BY YAHOO!, INC., HEADQUARTERED AT 701 FIRST AVENUE, SUNNYVALE, CA	)	09-616-M-01
	)	UNDER SEAL

AFFIDAVIT IN SUPPORT OF
APPLICATION FOR SEARCH WARRANT

I, Casey P. Farrell, being first duly sworn, hereby depose and state as follows:

I. INTRODUCTION

1. I am a Special Agent of the Federal Bureau of Investigation ("FBI") assigned to the Washington Field Office, and have been employed by the FBI for over four years. I am assigned to a squad responsible for counterespionage matters and matters involving the unauthorized disclosure of classified information, and have worked in this field since October 2007. As a result of my involvement in espionage investigations and investigations involving the unauthorized disclosure of classified information, I am familiar with the tactics, methods, and techniques of particular United States persons who possess, or have possessed a United States government security clearance and may choose to harm the United States by misusing their access to classified information. Before working for the FBI, I was an active duty officer in the United States Marine Corps for four years.

2. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

The statements in this affidavit are based in part on information provided by the investigation to date and on my experience and background as a Special Agent of the FBI. The information set forth in this affidavit concerning the investigation at issue is known to me as a result of my own involvement in that investigation or has been provided to me by other law enforcement professionals. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation.

3. This affidavit is made in support of an application for a warrant pursuant to 18 U.S.C. § 2703 to compel Yahoo! Incorporated, which functions as an electronic communication service and remote computing service, and is a provider of electronic communication and remote computing services (hereinafter "Yahoo!" or the "PROVIDER"), located at 701 First Avenue, Sunnyvale, California 94089, to provide subscriber information, records, and the contents of wire and electronic communications pertaining to the accounts identified as [redacted]**@yahoo.com** and [redacted]**@yahoo.com**, herein referred to as the SUBJECT ACCOUNTS.[1]

4. For the reasons set forth below, I believe there is probable cause to conclude that the contents of the wire and electronic communications pertaining to the SUBJECT ACCOUNTS, are evidence, fruits and instrumentalities of criminal violations of 18 U.S.C. § 793

[1] Because this Court has jurisdiction over the offense under investigation, it may issue the warrant to compel the PROVIDER pursuant to 18 U.S.C. § 2703(a). See 18 U.S.C. § 2703(a) ("A governmental entity may require the disclosure by a provider . . . pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation . . . .").

(Unauthorized Disclosure of National Defense Information).

5. Based on my training and experience, and discussions with the United States Attorney's Office, I have learned that Title 18, United States Code, Section 793(d) makes punishable, by up to ten years imprisonment, the willful communication, delivery or transmission of documents and information related to the national defense to someone not entitled to receive them by one with lawful access or possession of the same.

6. The SUBJECT ACCOUNTS are e-mail accounts. As discussed below, investigation into the SUBJECT ACCOUNTS indicates they were and are used by Stephen J. Kim, believed to have been associated with the unauthorized disclosure of national defense information in June 2009.

II. FACTS SUPPORTING PROBABLE CAUSE

7. In June 2009, classified United States national defense information was published in an article on a United States news organization's website (hereinafter the "June 2009 article"). The June 2009 article was written by a national news reporter, herein referred to as "Reporter A," who was assigned to cover, and who physically worked at, the main Department of State (DoS) building located at 2201 C Street, N.W., Washington, D.C.

8. Based on my training and experience, and discussion with the United States Attorney's Office, I have learned that "classified" information is defined by Executive Order 12958, as amended by Executive Order 13292, and their predecessor orders, Executive Orders 12356 and 12065, as information in any form that: (1) is owned by, produced by or for, or under control of the United States government; (2) falls within one or more of the categories set forth

in the Order; and (3) is classified by an original classification authority who determines that its unauthorized disclosure reasonably could be expected to result in damage to the national security. Where such damage could reasonably result in "exceptionally grave" damage to the national security, the information may be classified as "TOP SECRET." Access to classified information at any level may be further restricted through compartmentalization "SENSITIVE COMPARTMENTED INFORMATION" (SCI) categories, which further restricts the dissemination and handling of the information.

9. The Intelligence Community owners of the classified information at issue have informed the FBI that the June 2009 article disclosed national defense information that was classified TOP SECRET/SPECIAL COMPARTMENTED INFORMATION (TS/SCI). Further, they have informed the FBI that the information was not declassified prior to its disclosure in the June 2009 article, it remains classified at the TS/SCI level to this day, and its public disclosure has never been lawfully authorized.

10. Based on my training and experience, I have learned that classified information, of any designation, may be shared only with persons determined by an appropriate United States government official to be eligible for access to classified information, that is, the individual has received a security clearance, has signed an approved non-disclosure agreement and possesses a "need to know" the information in question. If a person is not eligible to receive classified information, classified information may not be disclosed to that person. Reporter A did not possess a security clearance.

11. Following the disclosure of the classified national defense information in the June 2009 article, an FBI investigation was initiated to determine the source(s) of the unauthorized

disclosure. That investigation has revealed that the TS/SCI information disclosed in the June 2009 article was first made available to a limited number of Intelligence Community members in an intelligence report (the "Intelligence Report") that was first electronically disseminated to the Intelligence Community on the morning that the June 2009 article was published. The Intelligence Report was accessible on a classified information database that warned all Intelligence Community users seeking access to information in the database, through a "click through" banner, of the following:

> Due to recent unauthorized disclosures of sensitive intelligence, you are reminded of your responsibility to protect the extremely sensitive, compartmented intelligence contained in this system. Use of this computer system constitutes consent to monitoring of your actions. None of the intelligence contained in this system may be discussed or shared with individuals who are not authorized to receive it. Unauthorized use . . . is prohibited and violations may result in disciplinary action or criminal prosecution.

12. The Intelligence Report was clearly marked TS/SCI. The security markings further instructed the reader that every portion of the information contained in the Intelligence Report was classified TS/SCI and was not authorized for disclosure.

13. The investigation has revealed that one individual who accessed the Intelligence Report through the classified database was Stephen Jin-Woo Kim.[1] Review of government records has revealed that Mr. Kim was born on [redacted] and was naturalized as a United States citizen in 1999. Mr. Kim is a Lawrence Livermore National Laboratory employee who was on detail to the DoS's Bureau of Verification, Compliance, and Implementation (VCI) at the

[1] The FBI's investigation has revealed that individuals other than Mr. Kim had authorized access to the Intelligence Report. To date, the FBI's investigation has not revealed any other individual who accessed the Intelligence Report who also had contact with Reporter A on the day that the June 2009 article was published.

time of the publication of the June 2009 article. VCI is responsible for ensuring that appropriate verification requirements are fully considered and properly integrated into arms control, nonproliferation, and disarmament agreements and to ensure that other countries' compliance with such agreements is carefully monitored, assessed, and enforced. On his detail to VCI, Mr. Kim worked as a Senior Advisor for Intelligence to the Assistant Secretary of State for VCI.

14. Like Reporter A's office on the date of the June 2009 article's publication, Mr. Kim's VCI office was located at the DoS headquarters building at 2201 C Street, N.W., Washington, D.C.

15. Government records demonstrate that Mr. Kim possesses a TS/SCI security clearance. As a government employee with a security clearance, and prior to the disclosures at issue, Mr. Kim executed multiple SF 312 Classified Information Non-Disclosure Agreements (NDAs) with the Government. NDAs are legally binding agreements between an individual being granted, or already in possession of, a security clearance, and the United States Government wherein the parties agree that the individual never disclose classified information without the authorization of the Government. The NDAs further notified Mr. Kim that the unauthorized disclosure of classified information can lead to criminal prosecution, including for violations of 18 U.S.C. § 793.

16. The Intelligence Community owners of the classified information disclosed in the June 2009 article have informed the FBI that Mr. Kim was not authorized, directly or indirectly, by the United States Government to deliver, communicate, or transmit that TS/SCI information to Reporter A or any other member of the press, and Reporter A was not authorized to receive it.

17. Government electronic records revealed that approximately four hours before the

June 2009 article was published, the unique electronic user profile and password associated with Mr. Kim ***accessed three times*** Intelligence Report that contained the TS/SCI information which later that day was disclosed in the June 2009 article.[2] Specifically, the Intelligence Report was accessed by Mr. Kim's user profile at 11:27 a.m., 11:37 a.m., and 11:48 a.m. on the date the article was published. DoS security badge access records confirm that, at those times, Mr. Kim was in his VCI office space where his DoS TS/SCI computer was located on which he would

---

[2] Mr. Kim accessed the classified database in question through his DoS work computer provided to him to process and access TOP SECRET/SCI information. That classified DoS computer requires the user to "click through" the following security banner every time it is used:

NOTICE AND CONSENT LOG-ON BANNER

THIS IS A DEPARTMENT OF STATE (DoS) COMPUTER SYSTEM. THIS COMPUTER SYSTEM, INCLUDING ALL RELATED EQUIPMENT, NETWORKS, AND NETWORK DEVICES (SPECIFICALLY INCLUDING INTERNET ACCESS), ARE PROVIDED ONLY FOR AUTHORIZED U.S. GOVERNMENT USE. DoS COMPUTER SYSTEMS MAY BE MONITORED FOR ALL LAWFUL PURPOSES, INCLUDING TO ENSURE THAT THEIR USE IS AUTHORIZED, FOR MANAGEMENT OF THE SYSTEM, TO FACILITATE PROTECTION AGAINST UNAUTHORIZED ACCESS, AND TO VERIFY SECURITY PROCEDURES, SURVIVABILITY, AND OPERATIONAL SECURITY. MONITORING INCLUDES ACTIVE ATTACKS BY AUTHORIZED DoS ENTITIES TO TEST OR VERIFY THE SECURITY OF THIS SYSTEM. DURING MONITORING, INFORMATION MAY BE EXAMINED, RECORDED, COPIED, AND USED FOR AUTHORIZED PURPOSES. ALL INFORMATION, INCLUDING PERSONAL INFORMATION, PLACED ON OR SENT OVER THIS SYSTEM MAY BE MONITORED. USE OF THIS DoS COMPUTER SYSTEM, AUTHORIZED OR UNAUTHORIZED CONSTITUTES CONSENT TO MONITORING OF THIS SYSTEM. UNAUTHORIZED USE MAY SUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE OF UNAUTHORIZED USE COLLECTED DURING MONITORING MAY BE USED FOR ADMINISTRATIVE, CRIMINAL OR OTHER ADVERSE ACTION. USE OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR THESE PURPOSES.

In addition, the DoS's Foreign Affairs Manual states that security personnel are responsible for conducting security inspections of DoS buildings to insure that classified information is properly protected. Indeed, Mr. Kim's office was located in a secured facility within the main DoS building that was subject to daily inspections by rotating duty officers (sometimes including Mr. Kim himself) who were responsible for making sure that classified information in each of the offices within the facility was properly secured.

have accessed the Intelligence Report.

18. Telephone call records demonstrate that earlier on the same day that Mr. Kim viewed the Intelligence Report and that it was published, multiple telephone communications occurred between phone numbers associated with Mr. Kim and with Reporter A. Specifically:

- at 10:15 a.m., a 34-second call was made from Reporter A's DoS desk telephone to Mr. Kim's DoS desk telephone;
- two minutes later, at 10:17 a.m., an 11 minute 35 second call was made from Mr. Kim's DoS desk telephone to Reporter A's DoS desk telephone;
- one hour later, at 11:18 a.m., a 3 minute 58 second call was made from Mr. Kim's DoS desk telephone to Reporter A's DoS desk telephone; and
- at 11:24 a.m., an 18 second call was made from Mr. Kim's DoS desk telephone to Reporter A's DoS desk telephone.

19. Thereafter, telephone call records for Mr. Kim's office phone reveal that ***at the same time that Mr. Kim's user profile was viewing the TS/SCI Intelligence Report two telephone calls were placed from his desk phone to Reporter A.*** Specifically, a call was made at 11:37 a.m (the same time that Mr. Kim's user profile was viewing the Intelligence Report) from Mr. Kim's desk phone to Reporter A's desk phone located within the DoS. That call lasted 20 seconds. Immediately thereafter, a call was placed by Mr. Kim's desk phone to Reporter A's cell phone. This second call lasted 1 minute and 8 seconds.

20. In the hour following that call at 11:37 a.m., the FBI's investigation has revealed evidence suggesting that Mr. Kim met face-to-face with Reporter A outside of the DoS. Specifically, DoS security badge access records demonstrate that Mr. Kim and Reporter A departed the DoS building at 2201 C Street, N.W., at nearly the same time, they were absent from the building for nearly 25 minutes, and then they returned to the DoS building at nearly the

same time. Specifically, the security badge access records indicate:

- Mr. Kim departed DoS at 12:02 p.m. followed shortly thereafter by Reporter A at 12:03 p.m.; and
- Mr. Kim returned to DoS at 12:26 p.m. followed shortly thereafter by Reporter A at 12:30 p.m.

21. Within three hours after those nearly simultaneous exits and entries at DoS, the June 2009 article was published on the Internet. Immediately following the publishing of the article, yet another call was placed from Mr. Kim's DoS desk telephone to Reporter A's DoS desk telephone number. This call, believed by the FBI to be a voice mail from Mr. Kim to Reporter A, lasted 22 seconds.

22. In the evening of August 31, 2009, DoS Diplomatic Security entered Mr. Kim's DoS office space pursuant to DoS internal regulations, procedures, and computer banner authority for purposes of imaging his computer hard drives. Sitting in plain view on Mr. Kim's desk next to his DoS computer were photocopies of the June 2009 article as well as two other articles published in June 2009. The first of the latter two articles also disclosed classified information and is the subject of an FBI investigation. The FBI is still determining whether the third article disclosed classified information. All three articles were stapled together. These three articles were also observed on Mr. Kim's desk during entries made in his DoS office space on September 21 and 22, 2009.

23. On September 24, 2009, the FBI conducted a non-custodial interview of Mr. Kim concerning the leak of classified information in the June 2009 article, among other leaks of classified information. During that interview, Mr. Kim denied being a source of the classified

information in the June 2009 article. Mr. Kim also claimed to have no recollection of one of the other two articles which were seen in plain view on his desk on August 31, 2009. Mr. Kim admitted to meeting Reporter A in approximately March 2009 but denied having any contact with Reporter A since that time. Mr. Kim stated that DoS protocol required that he would have to go through the DoS press office before he could speak with the press. Mr. Kim added, "I wouldn't pick-up a phone and call [Reporter A] or [the news organization that Reporter A works for]."

24. An analysis of call records for Mr. Kim's DoS ***desk phone*** reveals that between May 26, 2009 and July 14, 2009, ***36 calls*** were placed to or received from telephone numbers associated with Reporter A, including the 7 aforementioned calls on the day that the June 2009 article was published. Further, there were ***3 calls*** during this timeframe between his desk phone and a number associated with Reporter A's news organization.

25. During the September 24, 2009 non-custodial interview, when asked by the FBI for a cell phone number to reach him in the future, Mr. Kim stated that his cell phone was "no longer active" as of the day of the interview. Mr. Kim indicated to the FBI that he would be purchasing a new cell phone with a different number.

26. An analysis of call records for Mr. Kim's ***cellular phone*** (which he apparently intended to disconnect after his interview with the FBI) reveals that between May 26, 2009 and June 30, 2009, ***16 calls*** were placed to or received from telephone numbers associated with Reporter A and ***11 calls*** were placed to or received from telephone numbers associated with Reporter A's news organization.

27. It is apparent from the foregoing both that Mr. Kim has been in contact with

Reporter A on multiple occasions in the recent past and that Mr. Kim does not want the FBI, who he knows is investigating the leak of classified information in the June 2009 article, to know about those contacts. The FBI has also learned that Mr. Kim has provided Department of Energy (DoE) – for which Mr. Kim's permanent employer, LLNL, is a sub-contractor – with a telephone number for a "pre-paid" cell phone (sometimes referred to as a "throw away" phone) that he instructed DoE representatives to use in the future to contact him about future employment opportunities.

28. Similarly, during the same September 24, 2009 non-custodial interview, Mr. Kim also provided the FBI with e-mail account [redacted]**@yahoo.com** as a means of contacting him in the future. One day later, Mr. Kim e-mailed the FBI and stated that (like his soon to be disconnected cell phone) "[m]y yahoo account that I gave you is full and am going to get rid of it. I can be reached at [redacted]@gmail.com." Again, it is apparent from the foregoing that Mr. Kim is concerned about the FBI focusing on his [redacted]**@yahoo.com** email account.

29. Following the FBI's interview of Mr. Kim on September 24, 2009, FBI and DoS/DS agents entered Mr. Kim's office on the evening of September 26, 2009. The stapled photocopies of the three articles containing classified information (including the June 2009 article) seen next to Mr. Kim's computer on August 31, 2009, September 21 and 22, 2009, were no longer present in Mr. Kim's office on September 26th – two days after his interview with the FBI wherein he was questioned about the unauthorized disclosures of classified information in each of those articles.

30. A forensic analysis of the hard drive imaged from Mr. Kim's DoS unclassified

computer on August 31, 2009,[3] has revealed an email communication, dated July 11, 2009, from Reporter A's email account to an email account entitled [redacted]@yahoo.com. The email from Reporter A forwarded another email from other news reporters which included in its body a news article (not written by Reporter A) that would appear in the Washington Times (not Reporter A's news organization) the following day, July 12, 2009. This email was found in the unallocated space located on Mr. Kim's DoS unclassified hard drive. When a computer file is deleted, the deleted file is flagged by the operating system as no longer needed, but remains on the hard disk drive in unallocated space unless the date is later overwritten.

31. Electronic evidence retrieved by DoS/DS from Mr. Kim's DoS unclassified

---

[3] The "click through" banner on DoS's unclassified computers reads as follows:

> You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to the network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only.
>
> Unauthorized or improper use of this system may result in disciplinary actions, as well as civil and criminal penalties.
>
> By using this information system, you understand and consent to the following:
>
> * You have no reasonable expectation of privacy regarding any communications or data transiting or stored on this information system. At any time, and for any lawful government purpose, the government may monitor, intercept, and search and seize any communication or data transiting or stored on this information system.
>
> * Any communications or data transiting or stored on this information system may be disclosed or used for any lawful government purpose.
>
> Nothing herein consents to the search and seizure of a privately-owned computer or other privately owned communications device, or the contents therefor, that is in the system user's home.

workstation also revealed that on September 24, 2009, following his interview with the FBI, Mr. Kim's user profile logged into the [redacted]@yahoo.com account through an Internet connection accessed through his DoS unclassified workstation. DoS security badge access records confirm that Mr. Kim was in his VCI office space where his DoS unclassified workstation was located when the [redacted]@yahoo.com account was accessed on September 24, 2009. While accessing that account on his DoS computer, Mr. Kim's user profile observed emails in that account from Reporter A. Mr. Kim's profile also observed emails between Reporter A and [redacted]@yahoo.com, the email account identified by Mr. Kim as his own during his September 24, 2009 interview with the FBI, but which, one day later, he told the FBI was "full" and that he was "going to get rid of it." Specifically, Mr. Kim's user profile observed on September 24, 2009 on his DoS computer:

- an email sent on May 11, 2009 at 8:20 a.m. from [redacted]@yahoo.com to what the FBI believes is an email account entitled [redacted]@gmail.com. The body of the email reads:

  > I am back from my trip. Here is my personal information.
  >
  > Please send me your personal cell number. I believe you have mine. It was great meeting you.
  >
  > Thanks,
  >
  > Stephen

- an email sent on May 20, 2009 at 5:52 p.m. from [redacted]@gmail.com to [redacted]@yahoo.com responded to the above May 11, 2009 email, the body of which states:

  > Your credentials have never been doubted – but I am nonetheless grateful to have the benefit of a chronological listing of your postings and accomplishments. I only have one cell phone number, on my Blackberry, which I gave you 202-[phone number for Reporter A]. Unfortunately, when I am seated in my booth at

the State Department, which is much of every day, it does not get reception. thus [sic] I instruct individuals who wish to contact me simply to send me an e-mail to this address [[redacted]@gmail.com[4]]. one asterisk means to contact them, or that previously suggested plans for communication are to proceed as agreed; two asterisks means the opposite. With all this established, and presuming you have read/seen enough about me to know that I am trustworthy . . . let's get about our work! What do you want to accomplish together? As I told you when we met, I can always go on television and say: "Sources tell [name of Reporter A's national news organization]" But I am in a much better position to advance the interests of all concerned if I can say: "[Name of Reporter A's national news organization] has obtained . . ."
Warmest regards, [first name of Reporter A].

- an email sent on May 20, 2009 at 6:12 p.m. from [redacted]@gmail.com to [redacted]**@yahoo.com,** the body of which states:

  Please forgive my delay in replying to you. I was on vacation out of town with my wife and son last week.

  Yours faithfully, [first name of Reporter A]

- an email sent on August 15, 2009 from [redacted]**@yahoo.com** to Reporter A's work email account, the body of which has not yet been retrieved from forensic analysis.

- an email sent on August 15, 2009 at 9:25 a.m. from Reporter A's work email account to [redacted]**@yahoo.com**, the body of which states:

  Leo,

  You are most perceptive and I appreciate your inquiry. Call me at work on Monday [at Reporter A's work phone number] and I will tell you about my reassignment.[5] In the meantime, enjoy your weekend!

---

[4] "[redacted]" is not the name of Reporter A. Rather, this e-mail account appears to be a clandestine account used by Reporter A to communicate with Mr. Kim. I would note that [redacted] was a Deputy Assistant to President Richard Nixon who is best known as the individual who was responsible for the secret taping system that President Nixon had installed in the White House. [redacted] was also the individual who publicly exposed the existence of that taping system when he testified before Congress during the Watergate hearings.

[5] The FBI has determined that Reporter A was reassigned from the DoS in August 2009 to cover another government entity.

Alex

32. Immediately following the foregoing text of the August 15, 2009 e-mail sent at 9:25 a.m. from "Alex" is an electronic signature that identifies Reporter A by Reporter A's full name and the media organization for which Reporter A works. The electronic signature also provides Reporter A's phone number and e-mail address associated with Reporter A's media organization.

33. After viewing the emails listed above on September 24, 2009, Mr. Kim attempted to clear his "Temporary Internet Files." Deletion of Temporary Internet Files created by a web browser software application moves the cached content of internet sites visited to unallocated space, which, again, is space on the hard drive flagged by the operating system as being available for overwriting.

34. I conclude from the foregoing that Mr. Kim and Reporter A have communicated as recently as August 15, 2009 by e-mail through both the [redacted]**@yahoo.com** and [redacted]**@yahoo.com** accounts, as well as through what appears to be a clandestine e-mail account set up by Reporter A, [redacted]@gmail.com, to communicate with Mr. Kim and perhaps other sources of information.[6] Further, in their most recent e-mail communication about which the FBI is aware, Mr. Kim and Reporter A appear to be employing aliases (i.e., Mr. Kim is "Leo" and Reporter A is "Alex").

35. On September 24, 2009, Mr. Kim's user profile also observed on his DoS

[6] The FBI is not at this time seeking a search warrant for [redacted]@gmail.com. Rather, it is restricting its request for e-mail search warrants to accounts associated with Mr. Kim.

workstation a list of e-mails stored in the "inbox" of the [redacted]**@yahoo.com** account. The list indicates that there are at least five e-mail communications between that account and Reporter A since June 18, 2009, the full content of which the FBI does not have in its possession. Those communications occurred this past summer on June 18 and 30, July 11 and 12, and August 15, 2009. Further, there is one e-mail communication in the account from "Leo Grace" on the date of the publication of the June 2009 article. The subject line of that e-mail reads "Fw: Re: here." It is reasonable to believe the content of the e-mail could reflect an attempt by Mr. Kim and Reporter A to coordinate a meeting face-to-face outside of the DoS.

36. Results received from an October 6, 2009 order pursuant to 18 U.S.C. § 2703(d) for the [redacted]**@yahoo.com** confirms that that account has received at least four communications from the [redacted]@gmail.com account, and at least 3 communications from the [redacted]**@yahoo.com** account.

37. On September 28, 2009, the FBI submitted a preservation letter to Yahoo!, pursuant to 18 U.S.C. § 2703(f), requesting that the contents of [redacted]**@yahoo.com** and [redacted]**@yahoo.com** be preserved.

III. COMPUTERS, THE INTERNET, AND E-MAIL

38. I have received training from the FBI related to computer systems and the use of computers during criminal investigations. Based on my education, training and experience, and information provided to me by other law enforcement agents, I know the following:

a. The Internet is a worldwide computer network that connects computers and allows communications and the transfer of data and information across state and national boundaries. The term "computer", as used herein, is defined in 18 U.S.C. § 1030(e)(1) and includes an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage

functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. A computer user accesses the Internet through a computer network or an Internet Service Provider (ISP).

b. E-mail, or electronic mail, is a popular method of sending messages and files between computer users. When a computer user sends an e-mail, it is created on the sender's computer, transmitted to the mail server of the sender's e-mail service providers, then transmitted to the mail server of the recipient's e-mail service provider, and eventually transmitted to the recipient's computer. A server is a computer attached to a dedicated network that serves many users. Copies of e-mails are usually maintained on the recipient's e-mail server, and in some cases are maintained on the sender's e-mail server.

39. Based on my training and experience, and information provided to me by other law enforcement agents, I know the following: First, searches of e-mail accounts usually provide information that helps identify the user(s) of the e-mail accounts. Second, individuals who use e-mail in connection with criminal activity, or activity of questionable legality, often set up an e-mail account to be used solely for that purpose. This is often part of an effort to maintain anonymity and to separate personal communication from communication and information that is related to the criminal activity. Third, when the criminal violation involves a conspiracy, a search of an e-mail account often allows the identification of co-conspirators.

IV. BACKGROUND REGARDING YAHOO!

40. Yahoo! is an e-mail service provider located at 701 First Avenue, Sunnyvale, California 94089. Yahoo! offers free and paid e-mail services. Yahoo! maintains records pertaining to the subscribers of its e-mail services. These records include account access information, transaction information, and account application information.

41. Yahoo! subscribers can access their accounts on servers maintained and/or owned by Yahoo! from any computer connected to the Internet located anywhere in the world. E-mail

messages and files sent to a Yahoo! account are stored in the account's "inbox" as long as they are not identified as "junk mail" and the account has not exceeded the maximum storage limit, and the account is not set up to forward messages to another e-mail account. If the message/file is not deleted by the subscriber, the account is below the maximum storage limit, and the account has not been inactivated, then the message/file will remain on the server indefinitely. E-mail messages and files sent from a Yahoo account will remain on the server unless the account user changes the default account setup by deselecting the option "Save your sent messages in the Sent Items folder" under "General Preferences."

42. Yahoo! provides POP3 access only for paid e-mail accounts. POP3 is a protocol by which e-mail client software such as Microsoft Outlook or Netscape Mail can access the servers of an e-mail service provider and download the messages to a local computer. If POP3 access is enabled, the account user can select to keep a copy of the downloaded messages on the server or have the messages deleted from the server.

43. Computers located at Yahoo! contain information and other stored electronic communications belonging to unrelated third parties. Accordingly, this affidavit and application for search warrant seek authorization solely to search the accounts and/or files following the procedures described in the Attachment A.

V. STORED WIRE AND ELECTRONIC COMMUNICATIONS

44. 18 U.S.C. §§ 2701–2711 is called the "Electronic Communications Privacy Act."

a. 18 U.S.C. § 2703(a) provides, in part:

> A governmental entity may require the disclosure by a provider of electronic communication service of the contents of an electronic communication that is in electronic storage in an electronic

communications system for one hundred and eighty days or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

b. 18 U.S.C. § 2703(b) provides, in part:

(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection –

(A) Without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant; or . . . .

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service –

(A) On behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) Solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

c. The Government may also obtain records and other information pertaining to a subscriber or customer of an electronic communication service or remote computing service by way of a search warrant. 18 U.S.C. § 2703(c)(1)(A). No notice to the subscriber or customer is required. 18 U.S.C. § 2703(c)(2).

d. 18 U.S.C. § 2711 provides, in part:

As used in this chapter – (1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section; and (2) the term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system.

e. 18 U.S.C. § 2510 provides, in part:

(8) "contents," when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication;...(14) "electronic communications system" means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications; (15) "electronic...communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications;... (17) "electronic storage" means - (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.

f. 18 U.S.C. § 2703(g) provides, in part:

Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service.

VI. ITEMS TO BE SEIZED

45. Based on my training and experience, and the training and experience of other counterespionage agents, I believe that the information requested in Attachment A for the SUBJECT ACCOUNTS will provide valuable information regarding the investigation of the June 2009 unauthorized disclosures of national defense information. The content of the e-mails

may help to establish further links between Mr. Kim and Reporter A, as well as other members of the media to whom disclosure of national defense information is illegal. Further, the content of those communications from Mr. Kim may well assist the FBI in establishing the fact of the disclosures and his intent in making them.

46. Based on the foregoing, I request that the Court issue a search warrant with respect to the PROVIDER in accordance with 18 U.S.C. § 2703 using the procedures set forth in Attachment A to this search warrant. The PROVIDER will copy all of the files, records, and other documents for the SUBJECT ACCOUNTS. Government agents will then review the copied material to search for evidence, fruits and instrumentalities of criminal violations of 18 U.S.C. §793. The original production from the PROVIDER will then be sealed.

VII. MINIMIZATION PROCEDURES FOR MATERIAL POTENTIALLY SUBJECT TO ATTORNEY-CLIENT OR OTHER PRIVILEGE

47. I believe that e-mails containing information that may be subject to attorney-client or other privilege could be found in the SUBJECT ACCOUNTS. These accounts may also contain classified information, however. Further, review of the SUBJECT ACCOUNTS will reveal the name of Reporter A, the identity of the Reporter A's news organization, and possibly the precise date of the classified disclosure in question. I believe that this information, when combined with the information disclosed in this affidavit, would be sufficient for a reviewer of the SUBJECT ACCOUNTS to determine the information that was disclosed in the June 2009 article which, again, continues to be classified TOP SECRET/SCI. Accordingly, any reviewer of these accounts will need to possess the necessary security clearances, as well as the permission of the Intelligence Community owners of the information, to review the material.

The number of emails in the [redacted]@yahoo.com account is also believed to be voluminous. It is my understanding that there are nearly 1500 emails in that account. For these reasons, and because of the exigency presented by the possible further unauthorized disclosures of classified information by Mr. Kim, the FBI submits that the materials produced in response to this Search Warrant should be reviewed for privilege by a cleared law enforcement agent.

48. The FBI proposes that it designate cleared agents who are not, and will not be, involved in the criminal investigation to first examine the materials for privilege, in consultation with an Assistant United States Attorney designated for that purpose (and who likewise is not, and will not be, involved in the criminal investigation). Said agents will only release the materials to the FBI case agents in this matter after it has been ascertained that they contain no privileged information or that such information has been removed from the materials. Any materials that do contain privileged information will be sealed and not examined by me or any other agent or government attorney participating in the criminal investigation unless and until the privilege is waived or otherwise determined to be inapplicable.

VIII. REQUEST FOR NON-DISCLOSURE BY PROVIDER

49. Pursuant to 18 U.S.C. § 2705(b), I request that the Court enter an order commanding the PROVIDER not to notify any other person, including the subscriber of the SUBJECT ACCOUNTS, of the existence of the warrant because there is reason to believe that notification of the existence of the warrant will result in: (1) endangering the life or physical safety of an individual; (2) flight from prosecution; (3) destruction of or tampering of evidence; (4) intimidation of potential witnesses; or (5) otherwise seriously jeopardize the investigation.

The involvement of the SUBJECT ACCOUNTS as set forth above is not public and I know, based on my training and experience, that subjects of criminal investigations will often destroy digital evidence if the subject learns of an investigation. Additionally, if the PROVIDER or other persons notify anyone that a warrant has been issued on the SUBJECT ACCOUNTS, the targets of this investigation and other persons may further mask their identity and activity and seriously jeopardize the investigation.

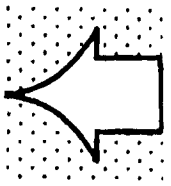
IX. REQUEST FOR SEALING

50. Because this investigation is continuing and disclosure of some of the details of this affidavit may compromise subsequent investigative measures to be taken in this case may cause the subject to flee, may cause the suspect to destroy evidence and/or may otherwise jeopardize this investigation, I respectfully request that this affidavit, and associated materials seeking this search warrant, be sealed until further order of this Court. Finally, I specifically request that the sealing order not prohibit information obtained from this warrant from being shared with other law enforcement and intelligence agencies.

X. CONCLUSION

51. Based on the foregoing, there is probable cause to believe on the computer systems owned, maintained, and/or operated by Yahoo!, Inc., there exists in, and related to, the SUBJECT ACCOUNTS, evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 793 (Unauthorized Disclosure of National Defense Information). By this affidavit and application, I request that the Court issue a search warrant directed to Yahoo!, Inc., allowing agents to seize the content of the SUBJECT ACCOUNTS and other related information stored on the Yahoo! servers following the search procedure described in Attachment A.

Casey P. Farrell
Special Agent
Federal Bureau of Investigation



Sworn to and subscribed before me
on this 9th day of NOV, NOV 0 9 2009

United States Magistrate Judge

ALAN KAY
U.S. MAGISTRATE JUDGE

EXHIBIT G

THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

APPLICATION FOR SEARCH WARRANT FOR E-MAIL ACCOUNT [redacted]@YAHOO.COM MAINTAINED ON COMPUTER SERVERS OPERATED BY YAHOO!, INC., HEADQUARTERED AT 701 FIRST AVENUE, SUNNYVALE, CA	)	Mag. No.: 09-616-M-01
	)	UNDER SEAL

FILED
NOV 0 7 2011
Clerk, U.S. District & Bankruptcy
Courts for the District of Columbia

ORDER

After reviewing the Government's Motion for Unsealing Search Warrant and Related Materials, it is hereby

ORDERED that the Government's motion is **GRANTED**; it is

FURTHER ORDERED that, to protect the privacy of the individuals involved, the attached redacted versions of the application for search warrant in this matter, the affidavit in support of the application for search warrant, the search and seizure warrant, and the Attachment A thereto, be **UNSEALED** and placed on the public record; and it is

FURTHER ORDERED that the Government may produce unredacted versions of this same material to the defense in United States v. Stephen Jin-Woo Kim, Cr. No. 10-225 (CKK), pursuant to the Rule 16 Protective Order in that matter.

SO ORDERED this 7th day of November 2011.

United States District Court
US MAGISTRATE JUDGE

(N)