

EMN:SDD
F.#2012R01737

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

12M1083

----- X

IN THE MATTER OF THE APPLICATION OF
THE UNITED STATES OF AMERICA FOR A
SEARCH WARRANT FOR THE PREMISES
KNOWN AND DESCRIBED AS:
ONE SMALL BROWN NOTEBOOK WITH THE
WORD "NORINCO" ON THE FRONT COVER;
ONE APPLE IPAD 2, 16GB, BLACK IN
COLOR, SERIAL NUMBER DN6HNU22ZDFHW;
ONE NIKON COOLPIX S6100 DIGITAL
CAMERA, SERIAL NUMBER 30113801; ONE
HTC CELLULAR TELEPHONE, SERIAL
NUMBER HC27NMG05191; ONE COOLPAD
CELLULAR TELEPHONE, SERIAL NUMBER
2010CP2894; ONE KINGSUN CELLULAR
TELEPHONE, SERIAL NUMBER
B8T1003313; AND ONE KINGSTON 16GB
DATATRAVELER G3 THUMBDRIVE, AS
FURTHER DESCRIBED HEREIN AND IN
ATTACHMENT A.

TO BE FILED UNDER SEAL
AFFIDAVIT IN SUPPORT OF
APPLICATION FOR SEARCH
WARRANT

(Fed. R. Crim. P. 41)

----- X

EASTERN DISTRICT OF NEW YORK, SS:

STEVEN GOODMAN, being duly sworn, deposes and says that
he is a Special Agent with the United States Department of
Homeland Security, Homeland Security Investigations ("HSI"), duly
appointed according to law and acting as such.

Upon information and belief there is probable cause to
believe that there is kept and concealed within the premises
known and described as a small, brown notebook with the word
"NORINCO" on the front cover; One Apple iPad 2, 16GB, black in
color on the front, serial number DN6HNU22ZDFHW; one Nikon

Coolpix S6100 digital camera, serial number 30113801; one HTC cellular telephone, serial number HC27NMG05191; one Coolpad cellular telephone, serial number 2010CP2894; one Kingsun cellular telephone, serial number B8T1003313; and one Kingston 16GB DataTraveler G3 thumbdrive ("SUBJECT PREMISES"), as further described herein and in Attachment A, within the Eastern District of New York, certain property, as set forth in Attachment B, all of which constitute evidence, fruits and instrumentalities of violations of Title 50, United States Code, Sections 1702 and 1705, and Title 15, Code of Federal Regulations, § 764.2 (attempted unlicensed export of controlled commodities).

The source of your deponent's information and the grounds for his belief are as follows:¹

I. INTRODUCTION

1. I have been a Special Agent with HSI since 2010. I am currently assigned to the Counter-Proliferation Investigations section of the Office of the Special-Agent-in-Charge, New York. My duties include the investigation and prosecution of violations

¹ The information contained in this affidavit is based upon my conversations with various law enforcement agents, and others, as well as my review of, among other things, reports, personal observations and recordings. Where statements of others are related herein, they are related in sum and substance and in part. Where foreign language materials are set forth, they are set forth based on summary and/or draft translations. Because the purpose of this affidavit is merely to establish probable cause to search the SUBJECT PREMISES, I have not set forth all of the facts and circumstances related to this matter of which I am aware.

pertaining to the export of licensable commodities, munitions and high-technology commodities such as carbon fiber. As a Special Agent with HSI, I have participated in numerous investigations into violations of the United States export control laws, during the course of which I have conducted or participated in surveillance, execution of search warrants, debriefings of informants, and review of documents and taped conversations.

2. As a Special Agent of HSI, I also have received specialized training at the Federal Law Enforcement Training Center. I have conducted and participated in several investigations of the above listed laws and regulations.

3. Through my training, education, and experience, I have become familiar with the manner in which commodities are exported from the United States directly or indirectly to certain countries, such as China, to avoid reporting requirements and detection by law enforcement.

II. APPLICABLE EXPORT REGULATIONS

4. The export of so-called "commerce controlled" items is regulated by the United States Department of Commerce ("DOC"). Under the International Emergency Economic Powers Act ("IEEPA"), 50 U.S.C. §§ 1701 et seq., the President of the United States was granted the authority to deal with unusual and extraordinary threats to the national security, foreign policy, and economy of the United States. Under IEEPA, the President could declare a

national emergency through Executive Orders that had the full force and effect of law.

5. On August 17, 2001, under the authority of IEEPA, the President issued Executive Order 13222, which declared a national emergency with respect to the unrestricted access of foreign parties to United States goods and technologies and extended the Export Administration Regulations (the "EAR"), 15 C.F.R. §§ 730-774. Through the EAR, the DOC imposed license or other requirements before an item subject to the EAR could be lawfully exported from the United States or lawfully re-exported from another country. These items are listed on the commerce control list, or "CCL," published at 15 C.F.R. § 774. The President issued annual Executive Notices extending the national emergency declared in Executive Order 13222 from the time period covered by that Executive Order through the time of this affidavit. See 77 Fed. Reg. 49,699 (Aug. 16, 2012).

6. Pursuant to its authority derived from IEEPA, the DOC reviews and controls the export of certain goods and technology from the United States to foreign countries. In particular, the DOC has placed restrictions on the export of goods and technology that it has determined could make a significant contribution to the military potential or nuclear proliferation of other nations or that could be detrimental to the foreign policy or national security of the United States. Under IEEPA and the EAR, it is a

crime to, among other things, willfully export, conspire to export, attempt to export or aid and abet the export from the United States any item subject to the EAR for which a license is required without first obtaining the license from the DOC. 50 U.S.C. §§ 1705(a) and 1705(c); 15 C.F.R. § 764.2.

III. TECHNICAL TERMS

7. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Computer: A computer includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

IV. FACTUAL BASIS FOR PROBABLE CAUSE

8. Since approximately April 2012, HSI, along with the DOC, has been conducting an investigation into the activities of Ming Suan Zhang ("the defendant") and others for attempting to export commerce controlled items from the United States to China, among other countries, without possessing the requisite export licenses.

9. During the course of the investigation, I have reviewed email communications and transcripts of recorded telephone calls between the defendant and others, including undercover HSI agents (referred to individually and collectively as "UC" or "UCs"). During certain of these communications, the defendant discussed his efforts to obtain large quantities of carbon fiber, purportedly for use in a Chinese military aircraft development program.

10. In addition, I have reviewed an email sent by the defendant from the email address MXMS-7666@189.CN to an accomplice on July 17, 2012, in which the defendant indicated that he had found a buyer for M60-type carbon fiber. The defendant further indicated that the carbon fiber was going to be purchased by a principal associated with the "Northern China Industrial Company." I am aware that NORINCO is a Chinese-based company that develops and manufactures defense products, weapons

systems, and other commodities.² The defendant further indicated that a sample of the M60 carbon fiber was needed to test before a larger order would be placed, and that the carbon fiber was needed by July 20, 2012, for the test flight of the new Chinese fighter jet in August 2012.

11. I have also reviewed transcripts of email communications between the defendant and a UC, in which the defendant arranged to meet the UC in the United States to take possession of a sample of carbon fiber and negotiate a long-term deal.

12. On August 30, 2012, the defendant informed a UC, via email, that his customer needed a sample of carbon fiber, to be used in connection with a test flight of a "fighter plane." Later that day, the defendant confirmed his itinerary for travel to the United States during the week of September 10, 2012. A subsequent review of IP login information indicated that the defendant's emails were transmitted via a computer server located in China.

13. On September 6, 2012, a UC shipped two spools of carbon fiber, labeled M60JB-3000-50B, from Brooklyn, New York to an

² According to its website, "NORINCO has demonstrated the solid strength of Chinese national defense industry and technology in precision strike systems, amphibious assault weapons and equipment, long-range suppression weapon systems, anti-aircraft & anti-missile systems, information & night vision products, highly effective destruction systems, anti-terrorism & anti-riot equipment as well as small arms."

agreed upon location in the United States, in anticipation of the meeting with the defendant. Thereafter, the UC traveled to the United States, and again communicated with the defendant, who was staying in a hotel, via email in order to confirm the time and place of the meeting.

14. On September 7, 2012, United States Magistrate Judge Cheryl L. Pollak issued an arrest warrant for the defendant for violating the IEEPA by attempting to export carbon fiber from the United States to China without first obtaining the necessary export license.³

15. On September 14, 2012, UCs met with the defendant in a hotel room to provide him with a carbon fiber sample and to further discuss the details of a long-term deal for multiple tons of carbon fiber to be exported to China from the United States. During the meeting, the defendant confirmed his intent to acquire the carbon fiber, and provided shipping information to the UCs in an effort to have the sample delivered to a location in China via courier service. The meeting was covertly recorded. The defendant also provided the UCs with \$1,000 in U.S. dollars as a good faith down payment on the shipment. Agents arrested the defendant at the conclusion of the meeting. He was subsequently removed to the Eastern District of New York.

³ On October 18, 2012, a grand jury sitting in this district returned an indictment charging the defendant with one count of attempting to violate the IEEPA. See 12 CR 666 (NGG).

16. The defendant was searched incident to his arrest, and agents performed a routine inventory of the items recovered. In addition, the defendant provided the agents with his consent to recover his personal items from his hotel room. The defendant signed a form authorizing the agents "to take any letters, papers, materials, or any other items/property which they may desire," which included express "consent to search iPad, hard drives, USB drives, cellphones, flash drives, and other electronic storage devices." The consent to search form was written in Mandarin as well as English.

17. On the defendant's person, among other items, agents discovered a small, brown notebook with the word "NORINCO" on the cover. NORINCO is an abbreviation for the "North China Industries Corporation," which, as noted above, is an aerospace and defense manufacturing company located in China. In performing a routine inventory of the defendant's personal items, agents briefly flipped through the notebook and determined that it contains approximately 100 pages, some of which contain handwritten notes in the Mandarin language. Agents then ceased inspecting the notebook, and pursued the instant application for a search warrant. The notebook is currently located at the DOC office in Staten Island, New York.

18. Agents also recovered the following electronic devices, all of which are capable of storing digital media:

a. One Apple iPad 2, 16GB, black in color on the front, with a camera on the top, and silver in color on the back, with serial number DN6HNU22ZDFHW;

b. one Nikon Coolpix S6100 digital camera, serial number 30113801;

c. one HTC cellular telephone, serial number HC27NMG05191;

d. one Coolpad cellular telephone, serial number 2010CP2894;

e. one Kingsun cellular telephone, serial number B8T1003313; and

f. one Kingston 16GB DataTraveler G3 thumbdrive, all of which also are currently located in the offices of the DOC in Staten Island, New York.

19. Based on my training, experience, participation in other investigations, execution of search warrants, debriefing of witnesses and extensive discussions with other experienced law enforcement officers, I am familiar with how technology smugglers and export violators circumvent U.S. licensing requirements to export goods to foreign countries.

20. Based on my knowledge of a substantial number of residential and commercial searches executed in connection with export violations, I am aware that unlicensed exporters often maintain close at hand the addresses, telephone numbers and

addresses of their criminal associates, including information pertaining to their contacts and customers, and to the end use of the commodities they are seeking to export. In addition, unlicensed exporters frequently maintain books, records, receipts, notes, ledgers, and other documents, including photographic and digital images, relating to the international shipment of licensable commodities. Such documents are generally maintained where the exporters have ready access to them, such as on their persons, in their residences and hotel rooms, and in readily accessible storage media, including computers, tablets, flash drives, thumb drives, cellphones and cameras. In addition, I know that the memory cards in digital cameras can be used to store images, documents and other electronic media.

V. EVIDENCE OF IEEPA VIOLATIONS WITHIN THE SUBJECT PREMISES

21. Based on my conversations with other investigators, as well as my review of recorded telephone conversations between the defendant and others and copies of email correspondence, I believe that notes, copies of communications, documents, diagrams, images, travel records, itineraries, transmission records and other forms of relevant information will be found in the SUBJECT PREMISES.

22. Moreover, based on my experience and my conversations with other investigators, there is probable cause to believe that records related to export violations will be recovered from the

SUBJECT PREMISES that would provide corroborative evidence in this investigation. Furthermore, there is probable cause to believe that personal records, such as the names, addresses and telephone numbers of co-conspirators, transshipment companies, and courier services will be recovered from the SUBJECT PREMISES. In addition, there is probable cause to believe that financial records related to export violations will be recovered from the SUBJECT PREMISES.

VI. TECHNICAL BACKGROUND

23. As described above and in Attachment B, this application seeks permission to search for records that might be found within the SUBJECT PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

24. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is

so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

25. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, in space on the storage medium that is not currently being used by an active file - for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

26. Wholly apart from user-generated files, computer storage media - in particular, computers' internal hard drives - contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

27. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

28. As further described in Attachment B, this application seeks permission to search for not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves.

Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

29. I know that when an individual uses a computer to facilitate the unlicensed export of controlled commodities, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

30. In most cases, a thorough search of a premises for information that might be stored on storage media often requires

agents to seize physical storage media and later review the media consistent with the warrant. In this connection, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and

configurations. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data. However, reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

31. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

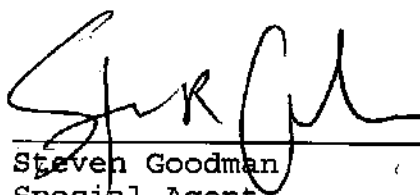
VII. CONCLUSION

32. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that within the SUBJECT PREMISES, as more fully described in Attachment A, there exists evidence of federal crimes, as set

forth in Attachment B. Accordingly, a search warrant is requested. Because the government's investigation is ongoing, and the disclosure of this application may lead to the destruction of evidence, the I respectfully request that it be filed under seal, except that a copy may be provided to defense counsel in discovery pursuant to a protective order in 12 CR 666 (NGG).

WHEREFORE, your deponent respectfully requests that the requested search warrant be issued for THE PREMISES KNOWN AND DESCRIBED AS ONE SMALL BROWN NOTEBOOK WITH THE WORD "NORINCO" ON THE FRONT COVER; ONE APPLE iPad 2, 16GB, BLACK IN COLOR ON THE FRONT, SERIAL NUMBER DN6HNU22ZDFHW; ONE NIKON COOLPIX S6100 DIGITAL CAMERA, SERIAL NUMBER 30113801; ONE HTC CELLULAR TELEPHONE, SERIAL NUMBER HC27NMG05191; ONE COOLPAD CELLULAR TELEPHONE, SERIAL NUMBER 2010CP2894; ONE KINGSUN CELLULAR

TELEPHONE, SERIAL NUMBER B8T1003313; AND ONE KINGSTON 16GB
DATATRAVELER G3 THUMBDRIVE, AS FURTHER DESCRIBED HEREIN AND IN
ATTACHMENT A.



Steven Goodman
Special Agent
Homeland Security Investigations

Sworn to before me this
30th day of November, 2012

THE HONORABLE CHERYL L. POLLAK
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A
Property to Be Searched

The property to be searched consists of one small, brown notebook with the word "NORINCO" on the front cover, as well as the following electronic devices:

- a. one Apple iPad 2, 16GB, black in color on the front, with serial number DN6HNU22ZDFHW;
- b. one Nikon Coolpix S6100 digital camera, serial number 30113801;
- c. one HTC cellular telephone, serial number HC27NMG05191;
- d. one Coolpad cellular telephone, serial number 2010CP2894;
- e. one Kingsun cellular telephone, serial number B8T1003313; and
- f. one Kingston 16GB DataTraveler G3 thumbdrive,

all of which are currently located in the offices of the Department of Commerce in Staten Island, New York.

ATTACHMENT B
Property to be Seized

1. All records¹ relating to violations of Title 50, United States Code, Sections 1702 and 1705 and Title 15 Code of Federal Regulations § 764.2 and involving Ming Suan Zhang and his accomplices and coconspirators since January 2011, as contained in the SUBJECT PREMISES as set forth in Attachment A, including:
- a. lists of customers and related identifying information;
 - b. types, amounts, and prices of controlled commodities as well as dates, places, and amounts of specific transactions relating to those commodities;
 - c. any information related to sources of controlled commodities (including names, addresses, phone numbers, or any other identifying information);
 - d. any information regarding Ming Suan Zhang's travel, locations and accommodations from January 2011 to the present;
 - e. any information relating to Ming Suan Zhang's contacts with foreign governments and/or foreign corporations;
 - f. any information relating to the end use of controlled commodities, including carbon fiber;
 - g. all bank records, checks, credit card bills, account information, and other financial records relating to the export, purchase or sale of controlled commodities or the facilitation of the export, purchase or sale of controlled commodities;
 - h. shipping documents;
 - i. documents, records and handwritten notes relating to transactions and proposed transactions for export

¹ As used herein, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

services;

- j. documents and records showing the names, addresses and telephone numbers of exporters and freight forwarding companies, as well as the identities of their confederates;
- K. documents and records relating to the potential end users of controlled commodities, including individuals, government organizations and manufacturers;
- l. documents and records relating to the identities of individuals and corporations involved in the production of high technology goods and materials, including but not limited to NORINCO;
- m. documents, technical data and records relating to the production of aerospace components, including but not limited to jet aircraft; and
- n. documents and records relation to the production of nuclear materials, weapons and weapons systems.

all of which constitute evidence, fruits, and instrumentalities of violations of Title 50, United States Code, Sections 1702 and 1705 and Title 15 Code of Federal Regulations § 764.2.

2. Computers² or storage media³ that contain or in which is stored records or information (hereinafter "COMPUTER") used as a means to commit violations of 50 U.S.C. §§ 1702 and 1705. All information obtained from such computers or storage media will be maintained by the government for the purpose of authentication and any potential discovery obligations in any related prosecution. The information shall be reviewed by the government only for the purpose of identifying and seizing information that

² As used herein, the term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

³ As used herein, the term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic optical media.

constitutes fruits, evidence and instrumentalities of violations of Title 50, United States Code, Sections 1702 and 1705 and Title 15 Code of Federal Regulations § 764.2, involving Ming Suan Zhang and his accomplices and coconspirators since January 2011, including:

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
 - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - c. evidence of the lack of such malicious software;
 - d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
 - e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
 - f. evidence of the times the COMPUTER was used;
 - g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
 - h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
 - i. contextual information necessary to understand the evidence described in this attachment;
3. Records and things evidencing the use of the Internet Protocol address to communicate with accomplices and coconspirators, including:
- a. routers, modems, and network equipment used to connect computers to the Internet;

b. Internet Protocol addresses used by the COMPUTER;

c. records or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

all of which constitute evidence, fruits, and instrumentalities of violations of Title 50, United States Code, Sections 1702 and 1705 and Title 15 Code of Federal Regulations § 764.2, involving Ming Suan Zhang and his accomplices and coconspirators.

12 1 083

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK

IN RE ORDER REQUIRING APPLE, INC.
TO ASSIST IN THE EXECUTION OF A
SEARCH WARRANT ISSUED BY THIS
COURT

Case No. _____

ORDER

Before the Court is the Government's motion for an order requiring Apple, Inc. to assist law enforcement agents in the search of an Apple iOS Device. Upon consideration of the motion, and for the reasons stated therein, it is hereby

ORDERED that Apple Inc. assist law enforcement agents in the examination of the iPad 2, black and silver in color, with serial number DN6HNU22ZDFHW (the "iOS Device"), acting in support of a search warrant issued separately by this Court;

FURTHER ORDERED that Apple shall provide reasonable technical assistance to enable law enforcement agents to obtain access to unencrypted data ("Data") on the iOS Device.

FURTHER ORDERED that, to the extent that data on the iOS Device is encrypted, Apple may provide a copy of the encrypted data to law enforcement, but Apple is not required to attempt to decrypt, or otherwise enable law enforcement's attempts to access any encrypted data;

FURTHER ORDERED that Apple's reasonable technical assistance may include, but is not limited to, bypassing the iOS Device user's passcode so that the agents may search the iOS Device, extracting data from the iOS Device and copying the data onto an external hard drive or other storage medium that law enforcement agents may search, or otherwise circumventing the iOS Device's security systems to allow law enforcement access to Data and to provide law enforcement with a copy of encrypted data stored on the iOS Device;

FURTHER ORDERED that although Apple shall make reasonable efforts to maintain the integrity of data on the iOS Device, Apple shall not be required to maintain copies of any user data as a result of the assistance ordered herein; all evidence preservation shall remain the responsibility of law enforcement agents.

FURTHER ORDERED that the application and this Order are sealed until otherwise ordered by the Court, except that they may be produced to defense counsel, to the extent that disclosure is necessary, pursuant to the terms of a protective order in case number 12 CR 666 (NGG).

Signed,

HONORABLE CHERYL L. POLLAK
UNITED STATES MAGISTRATE JUDGE

Date: NOVEMBER 30, 2012
Brooklyn, New York