

AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the
District of Colorado

In the Matter of the Search of)
Apple iPhone Model #A1387, IMEI #) Case No. 13-sw-05636-KLM
013072007554078, Serial # C8PHT314DTD1 and)
FCC ID # BCG-E2430A)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

SEE "ATTACHMENT A", which is attached to and incorporated in this Application and Affidavit

located in the ___ State and ___ District of ___ Colorado ___, there is now concealed (*identify the person or describe the property to be seized*):

SEE "ATTACHMENT B", which is attached to and incorporated in this Application and Affidavit

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- evidence of a crime;
- contraband, fruits of crime, or other items illegally possessed;
- property designed for use, intended for use, or used in committing a crime;
- a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
U.S.C. §§ 371; 1546; and 201(b)(2)	Conspiracy; Visa Fraud; Bribery of Public Official

The application is based on these facts:

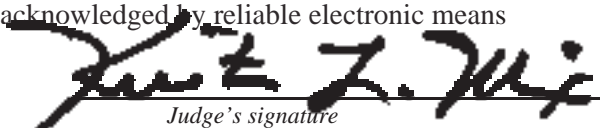
- Continued on the attached affidavit, which is incorporated by reference.
- Delayed notice of ___ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

s/Simon Dinitz, Special Agent
Applicant's signature

Simon Dinitz, Special Agent, Diplomatic Security Service, United States Department of State
Printed name and title

Sworn to before me and: ___ signed in my presence.
___^x submitted, attested to, and acknowledged by reliable electronic means

Date: **23 Jul 2013**



Kristen L. Mix, U.S. Magistrate Judge
Printed name and title

City and state: Denver, CO

ATTACHMENT A

The property to be searched is described as follows:

The property to be searched is a white Apple iPhone Model #A1387, IMEI# 013072007554078, serial# C8PHT314DTD1 and FCC ID# BCG-E2430A (“the iPhone”). The iPhone is currently located at the Diplomatic Security Service Denver Resident Office, at 8101 East Prentice Avenue, Suite 550, Greenwood Village, Colorado, 80111, Evidence Storage Area, Shelf D.

This warrant authorizes the forensic examination of the iPhone for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records and items on the iPhone described in Attachment A that relate to violations of 18 U.S.C. § 371 (Conspiracy), 18 U.S.C. § 1546 (Visa Fraud), 18 U.S.C. 201§ (b)(2) (Bribery of a Public Official), those violations involving Truc Huynh, including correspondence, records, documents, photographs, videos, electronic mail, chat logs, text messages, and electronic messages, including:
 - a. records or information relating to the preparation of visa applications, making or confirmation of visa appointments, meetings with visa customers, collecting money from visa customers, or recruiting additional recruiters or visa applicants;
 - b. records or information relating to TRUC HUYNH's whereabouts, schedule, travel, or activities;
 - c. records or information relating to TRUC HUYNH's conversations with any and all known and unknown co-conspirators, including SESTAK, BINH VO, ALICE NGUYEN, and HONG VO;
 - d. all communications to or from TRUC HUYNH from January 1, 2012 to present;
 - e. all communications, records, or documents related to the transfer or intended transfer or funds in the United States or abroad, between January 1, 2012 and the present;
 - f. all communications, records, or documents related to the attempt to launder money or structure deposits between January 1, 2012 and the present;
 - g. records or information relating to the state of mind of TRUC HUYNH;
 - h. records or information relating to the state of mind of any known or unknown conspirators or visa applicants concerning the visa fraud, bribery, and money laundering scheme detailed in the accompanying Affidavit;
 - i. records or information relating to who used, owned, or controlled the iPhone; and

j. records or information relating to the times and/or locations where the iPhone was used, including Internet Protocol addresses.

2. As used above, 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 electronic storage and any photographic form.

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, Special Agent Simon Dinitz, being duly sworn, depose and state as follows:

AGENT BACKGROUND

1. I am a Special Agent with the Diplomatic Security Service (“DSS”) of the United States Department of State. I am currently assigned to the Criminal Fraud Investigation Branch where I conduct investigations in support of the Department of State in addition to other duties. I have been a DSS Special Agent since 2008. I have completed numerous law enforcement academies and training seminars, including the Criminal Investigator Training Program at the Federal Law Enforcement Training Center in Brunswick, Georgia.

2. In my current capacity as a DSS Special Agent, I have participated in numerous investigations involving criminal violations of federal law. Specifically, I am familiar with the federal laws relating to fraud and the misuse of visas and other consular documents, bribery of public officials, immigration fraud, financial fraud, and money laundering. Through my experience (i) debriefing witnesses and defendants concerning public corruption in the visa process, immigration fraud, bribery of public officials, and money laundering; (ii) reviewing records that reflect telephonic or email associations consistent with corruption in the visa process; (iii) conducting surveillance of individuals; (iv) monitoring and collecting data on typical and atypical patterns of visa approvals and denials; and (v) executing both physical and electronic search warrants; I am able to identify the patterns and methods by which government officials and middlemen obtain bribes in exchange for approving fraudulent visas.

3. The facts set forth in this affidavit are based on information that I have obtained from my personal involvement in the investigation and from other law enforcement officers who have been involved in this investigation; documents that I have reviewed; and my training and

experience. Because this affidavit is being submitted for a limited purpose, I have not set forth all of the information known to me concerning this investigation. Instead, I have set forth information that I believe to be sufficient to establish probable cause in support of this application for a search warrant. Where I have reported statements made by others, or from documents that I have reviewed, those statements are reported in substance and in part, unless otherwise indicated.

IDENTIFICATION OF PROPERTY TO BE SEARCHED

4. The property to be searched is a white Apple iPhone Model #A1387, IMEI# 013072007554078, serial# C8PHT314DTD1 and FCC ID# BCG-E2430A (hereinafter “the iPhone”). The iPhone is currently located at the Diplomatic Security Service Denver Resident Office, at 8101 East Prentice Avenue, Suite 550, Greenwood Village, Colorado, 80111, Evidence Storage Area, Shelf D. The applied-for warrant would authorize the forensic examination of the iPhone for the purpose of identifying electronically stored data particularly described in Attachment B.

STATUTORY AUTHORITY

5. For the reasons set forth below, I believe there is probable cause to conclude that the iPhone is and contains evidence, fruits, and/or instrumentalities of criminal violations of 18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 1546 (visa fraud), and 18 U.S.C. § 201(b)(2) (bribery of a public official). As set forth in greater detail below, an investigation by the Department of State’s Diplomatic Security Service (“DSS”) has revealed probable cause that, beginning sometime in or around February 2012, while working as a Consular Officer in the Non-Immigrant Visa (“NIV”) Unit of the United States Consulate in Ho Chi Minh City (“the Consulate”), Vietnam, Michael T. SESTAK (“SESTAK”) conspired with others, including

TRUC HUYNH to solicit bribes from visa applicants in exchange for which SESTAK facilitated the approval of their visas through the Consulate.

FACTS ESTABLISHING PROBABLE CAUSE

6. The conspiracy includes, among other persons, SESTAK, a U.S. national; BINH T. VO, a U.S. national (“BINH VO”); ANHDAO T. NGUYEN, a Vietnamese national (“ALICE NGUYEN”); HONG VO, a U.S. national; and TRUC THANH HUYNH (“TRUC HUYNH”), a Vietnamese national. Between August 2010 and September 2012, SESTAK, a Foreign Service Officer with the U.S. Department of State, worked in the NIV Unit of the Consular Section of the Consulate.¹ SESTAK was the Consulate’s NIV Chief and supervised approximately four other consular officers.²

7. BINH VO, who resided in Vietnam, was the General Director of the Vietnam office of a multi-national company located in Vietnam. SESTAK and BINH VO are acquaintances who were known to socialize together in Ho Chi Minh City. ALICE NGUYEN is BINH VO’s spouse, and resided in Vietnam. HONG VO is BINH VO’s sibling, and resided in Vietnam. TRUC HUYNH is BINH VO and HONG VO’s cousin, and resided in Vietnam. Facts specific to TRUC THANH HUYNH and the iPhone to be searched begin on page 18 of this affidavit.

A. Overview of the Fraudulent Visa Scheme

8. Based on evidence uncovered through the course of the investigation, your affiant believes that the scheme operated as follows: SESTAK agreed to approve NIVs for applicants

1 The Consular Section of the Consulate is made up of three working units – Immigrant Visa, Non-Immigrant Visa, and American Citizen Services.

2 SESTAK was employed at the Consulate from August of 2010, until leaving post on September 6, 2012, in preparation for an active duty tour with the U.S. Navy.

for a fee. HONG VO, BINH VO, and other co-conspirators had “agents” working to recruit customers – or to recruit other recruiters – to the visa scheme. HONG VO reached out to people in Vietnam, and in the U.S., and would advertise that “the deal” was being facilitated by a “lawyer” who could guarantee visas for people to come to the United States. SESTAK’s co-conspirators also underscored that the lawyer could get visas for people who generally would not be able to get visas on their own, such as people who had been previously refused visas, people who resided in the countryside, people who had not traveled outside of Vietnam, etc. (The investigation has uncovered no evidence of any attorney being involved in the effort to acquire visas.) BINH VO, HONG VO, TRUC HUYNH, and others would then obtain biographical data and photos from customers in order to prepare their visa applications for them. They would submit the customers’ applications online and obtain appointments for interviews at the Consulate. TRUC HUYNH and others would also assist people in preparing for NIV consular interviews by providing sample questions and answers. Soon after submitting the visa application – in typically 3 days or less – the customer would receive an appointment at the Consulate, be interviewed by SESTAK, and be approved for a visa. The co-conspirators advertised that the charge would be between \$50-70,000 per visa, but also that they would sometimes charge less. They also encouraged recruiters to raise the price and keep the amount they charged over the established rate as their own commission. Customers would pay for their visas in Vietnam, or by routing money to co-conspirators in the United States. TRUC HUYNH and others would collect money from customers in Vietnam. SESTAK received several million dollars in bribes for approving the visas. He ultimately moved the money out of Vietnam by using money launderers through off-shore banks, primarily based in China, to move funds to a bank account in Thailand that he opened in May 2012. He then used the money to purchase real

estate in Phuket and Bangkok, Thailand. BINH VO and ALICE NGUYEN also had money laundered through off-shore banks to bank accounts in the United States.

B. Investigative Leads

9. In July 2012, the Consulate received a letter from a confidential source (“the Letter”) that claimed that a “facilitator” was soliciting bribes from applicants in exchange for the issuance of U.S. visas. In the Letter, the source claimed that between May 20, 2012, and early July 2012, between 50 and 70 people from a specific village in Vietnam (“the Group”) had obtained U.S. visas by way of a fraudulent visa scheme. The source claimed that one could pay \$55,000 in order to be guaranteed a tourist visa to the United States. The Letter included the names, dates of birth, and photographs of seven of the individuals alleged to have procured visas through this fraudulent scheme.

10. All NIV applications are submitted electronically via the Department of State's Consular Electronic Application Center (“CEAC”). The Internet Protocol (“IP”) address from which an applicant accesses the CEAC is captured and retained both at the time an application is first created, and at the time the application is submitted. Therefore, for every application submitted through the CEAC, there are two associated IP addresses.

11. DSS investigation resulted in the identification of five of the seven applicants named in the Letter. All five applicants had visas approved by SESTAK between May 20 and May 31, 2012. A review of these applications showed that they were connected to two IP addresses. Four of the five applications had been accessed from what appeared to be a dynamic IP address beginning with the digits 216.131.79, and which was later ascertained to be assigned to a Virtual Private Network (“VPN”) hosted by a U.S. Internet Service Provider (“ISP”), see infra par. 14 (“IP Address A”); or from IP address 118.69.37.10 (“IP Address B”). One

application had not been accessed by either IP address A or B; however, this application, dated May 21, 2012, was for an applicant whose sister's NIV application had been accessed by IP address A, and whose visa was issued by SESTAK two days later, on May 23, 2012.

C. The Three Tainted IP Addresses

12. DSS review of Consulate records revealed that many of the applications adjudicated by SESTAK were accessed from one of three IP addresses (hereinafter "Tainted IP Addresses"). Further investigation showed that the three IP addresses from which the applications were accessed were connected to HONG VO, BINH VO, and ALICE NGUYEN and her family.

13. DSS review of Consulate records revealed that approximately 425 NIV applications (for 419 unique applicants)³ had been accessed from IP Address A or IP Address B, between February and September 2012. SESTAK conducted the initial interview for 404 of the 419 applicants and approved visas for 386 applicants. SESTAK tried to issue visas to an additional 11 of the 404 applicants that he initially interviewed, but the system kicked back the applications due to certain data mismatches; all 11 applicants were ultimately re-adjudicated and approved by other officers without further interviewing. SESTAK gave 4 of the 404 applicants that he initially interviewed "soft refusals,"⁴ because they were missing documentation or had not paid certain fees required for their specific visa classes; all 4 of these applications were subsequently issued visas by other consular officers. Of the 15 applicants initially interviewed by other officers, 13 were refused visas. SESTAK overturned the refusal of one of these 13. Six

³ Several of the 419 visa applicants submitted more than one visa application.

⁴ When an applicant receives a soft refusal, the applicant can have the visa re-adjudicated without having to submit a new application.

others submitted new applications between 1 and 6 days after their refusal and were re-interviewed and issued visas by SESTAK.

i. IP Address A is Registered to HONG VO

14. A review of records on the American Registry for Internet Numbers (“ARIN”) website revealed that IP Address A was assigned to Black Oak Computers Inc. (“Black Oak”), an ISP with headquarters in California. Records obtained from Black Oak revealed that a single Black Oak Virtual Private Network (“VPN”)⁵ account was used to access all 408 NIV applications submitted from IP Address A, and that the subscriber on this account was HONG VO of an address in Denver, Colorado (“Denver Address”), with a Google e-mail address that included HONG VO’s first and last name (“HONG VO Google Account”). A subsequent check of Department of State passport records revealed that HONG VO had also listed the Denver address on her U.S. passport application in 2006.

15. There is also evidence that BINH VO used the Black Oak VPN Account. In a Google chat, dated July 10, 2012, recovered from a court-authorized search warrant executed on the HONG VO Google Account, BINH VO wrote to HONG VO, “strong VPN has not been working all night, what’s up w/ that? I figured you . . . were on then . . .” HONG VO replied that BINH VO should try again and that the VPN was working.

ii. IP Address B is Associated with BINH VO’s Work Office in Vietnam

⁵ A VPN is a technology that isolates one computer’s traffic to another computer’s traffic by creating an encrypted tunnel between two computers. By using a VPN, a person can route all of his traffic to the Internet through a second computer, thereby making it appear that he is accessing the Internet directly from the second computer. Some websites block traffic coming from certain IP addresses or certain countries. In order to circumvent such blocks, a user can use a VPN connection through an IP address or country that is allowed to visit the blocked website. Once a user establishes his Internet connection through the VPN, all of his traffic will appear to originate from the ISP that hosts the VPN.

16. DSS investigation revealed that, unlike IP Address A, IP Address B was an IP address with service provided by an ISP in Vietnam.⁶ Review of evidence in the form of IP address trails, and geographic tags embedded in photographs emailed by the co-conspirators indicated that IP Address B is tied to BINH VO's workplace.

17. BINH VO was the General Director of the Vietnam office of a multi-national company ("BINH VO Company"). The Company's website lists an address for the Company's office in Ho Chi Minh City ("BINH VO Company Address").

18. Review of information obtained through a court-authorized search warrant executed on BINH VO's Google Account ("BINH VO Google Account"), revealed that BINH VO repeatedly accessed his personal email from IP Address B. The header information for at least 17 emails in BINH VO's Google email account indicated that they were sent from IP Address B. At least three of these emails contained photograph attachments, for a total of five photos; all three emails had been sent from an iPhone. Approximately four of the photographs had GPS coordinates embedded in the exchangeable image file format ("EXIF") data⁷ that appeared to correspond to approximately a one-block vicinity of the BINH VO Company Address. The timestamps in the headers of the emails were within approximately 1 to 4 minutes of the timestamps in the photographs' EXIF data, which strongly suggests that the emails were sent from a location in close proximity to where the photographs were taken. Furthermore, the header information for another email located in BINH VO's Google email account, dated March

⁶ According to the APNIC website, IP Address B and IP Address C are assigned to ISP's located in Vietnam. Therefore, the United States cannot serve legal process to receive subscriber information for the relevant IP address log-ins.

⁷ EXIF data is encoded in digital photographs and may include geographic information, including GPS location information for where a photograph is taken.

7, 2012, included the name of a server that the email was routed through. The name of the server contained the name of the BINH VO Company, which strongly suggests that the BINH VO Company operated the server.

iii. Applications Connected to IP Address C

19. DSS review of Consulate records revealed that SESTAK also exhibited a pattern of approving visas connected to a third IP Address. Approximately 80 visa applications were created or last accessed from IP address 113.161.71.157 (“IP Address C”), between February 2012 and September 2012. SESTAK interviewed and issued visas to 75 of these 80 applicants.

iv. IP Address C is Associated with ALICE NGUYEN’s Family Home in HCM, Vietnam

20. DSS investigation revealed that, like IP Address B, IP Address C is an IP address with service provided by an ISP in Vietnam. Evidence in the form of IP address trails, and geographic tags embedded in photographs emailed by the co-conspirators, indicates that IP Address C is tied to the residence where ALICE NGUYEN’s parents live in Vietnam (“ALICE NGUYEN Family Home”).

21. Open source information indicated that the ALICE NGUYEN Family Home is a residential rental building.

22. DSS investigation revealed that BINH VO and ALICE NGUYEN repeatedly accessed their personal email accounts from IP Address C.

23. A court-authorized search warrant was executed on a Yahoo email account belonging to ALICE NGUYEN’s father. Review of the IP logs for this account indicated that ALICE NGUYEN’s father had logged into his account approximately 256 times between November 2, 2011, and December 12, 2012. Over 80% of these log-ins were made from IP Address C. ALICE NGUYEN’s father’s 2011 U.S. NIV application listed the ALICE NGUYEN

Family Home as his residence and his place of employment; ALICE NGUYEN's father's NIV application, which was submitted from IP Address C on October 12, 2011, also listed BINH VO as the individual who had prepared the application.

24. Additionally, ALICE NGUYEN's sister-in-law and brother listed the ALICE NGUYEN Family Home as their home address and their work address on their 2012 US visa applications. Their visa applications were accessed from IP Address C.

25. The header information for approximately 19 emails in the BINH VO Email Account (which spanned the date range of April 18, 2011 through September 10, 2012) indicated that BINH VO sent them via IP Address C.

26. Of the 19 emails sent from the BINH VO Google Account via IP Address C, at least 7 had photograph attachments that were taken with an iPhone. Two of these emails, dated November 29, 2011, and April 13, 2012, contained photos with EXIF data that included GPS tags of where the photographs were taken. The coordinates in the EXIF data of both photographs were within approximately one block of the ALICE NGUYEN Family Home. The time stamps captured in both photographs' EXIF data was within approximately one minute of the time stamps captured in the headers of the emails, which strongly suggests that the pictures had been sent from within close proximity of the ALICE NGUYEN Family Home.

D. SESTAK Approved Visas For Personal Associates of BINH VO

27. DSS review of Consulate records revealed that, while working at the Consulate, SESTAK approved visas for at least seven applicants who listed BINH VO, or one of BINH VO's parents, as their U.S. point of contact.

28. DSS review of Consulate records revealed that SESTAK also approved visas for ALICE NGUYEN, on April 28, 2011, October 24, 2011, and August 28, 2012. Review of

Google records revealed that on October 25, 2011, the day after he approved a visa for ALICE NGUYEN, SESTAK had the following Google chat with BINH VO:

BINH VO: thanks for Alice's visa and sorry about the application; She wasn't sure if she had to fill it out, etc.; hence, she asked you in her email. Great that you handled everything, which is greatly appreciated.

SESTAK: no worries. i will fedex it back to her address in austin, right?

SESTAK: ok i will send it tomorrow at lunch after they print the visa.

BINH VO then provided SESTAK with ALICE NGUYEN's address in Austin, Texas.

29. DSS review of Consulate records revealed that SESTAK approved a visa for ALICE NGUYEN's father, on October 13, 2011. It was submitted on October 12, 2011, from IP Address C.

30. DSS review of information acquired through various court-authorized search warrants executed through the course of the investigation revealed electronic chats and emails written by HONG VO which described the relationship that BINH VO purposefully cultivated with SESTAK in order to get SESTAK to approve visas for BINH VO.

31. During an electronic chat dated June 1, 2011, HONG VO stated "last night we went out with this guy who works at the consulate — he's the one that approves peoples visas... and he's this single guy who wants to find someone to be with... and my brother knows that - so he's been trying to get this guy out and introduce him to people... so then later he can do him favors like ... have him approve visas for people."

32. In another email dated June 1, 2011, HONG VO stated, "This guy who works for the US consulate here came out and joined us for dinner. He's the guy that approves Visas for Vietnamese people to go to the United States so he's a really good connection to have. My brother plans on using him to get [a sister-in-law's Visa to go to the States so [the sister-in-law] will most likely travel back with me in August . . . he just likes to people watch -- he does this with the consulate guy (Mike) and they check out girls."

33. During an electronic chat dated June 27, 2011, HONG VO discussed the sister-in-law referenced in the above paragraph. “I applied for her Visa...so her interview is July 13th . . . and i told the consulate guy . . . so he said he’ll pull her file . . . but now he knows our family . . . so he’s more trusting . . . but she’ll most likely get accepted this time . . . because Mike will pull up her file . . . and he considers Binh like his best friend.”

34. During an electronic chat dated July 13, 2011, the same day that SESTAK issued a visa to the sister-in-law discussed in the above paragraphs 32 and 33, BINH VO and HONG VO had the following exchange:

BINH VO: so [the sister-in-law] has her visa now, what did she say?
BINH VO: did Mike interview her?
HONG VO: because when she sat and waited
HONG VO: the number she had... wasn’t supposed to be for Mike’s room
HONG VO: but she ended up in his room
HONG VO: of course he interviewed her . . .
HONG VO: we have to figure out how
HONG VO: she can stay over there LEGIT though . . .
HONG VO: so it doesnt make mike look bad.

35. During an electronic chat with ALICE NGUYEN dated October 12, 2011, BINH VO wrote, “Finished yr parents applications... Mike is w/a couple of girls at Windows, but I am too lazy to join him. . . . I’ll text him soon to see if he has finished yet so that I can go give him the applications so that he can get the visas by Fri. for us.” The following day, SESTAK approved visas for ALICE NGUYEN’s parents.

E. Wire Transfers to ALICE NGUYEN from Individuals Linked to Five Applicants Who Received Visas From SESTAK

36. DSS review of financial records revealed that on or about May 21, 2012, a \$35,000 money transfer was made from the Sun Trust Bank account of Person 3 to defendant ALICE NGUYEN’s Wells Fargo account.

37. DSS review of consular records revealed that on or about May 21, 2012, a visa

application was submitted to the Consulate for T.T.M.L and listed Person 3 as T.T.M.L.'s U.S. point of contact and Person 3's work address as the U.S. destination.

38. DSS review of consular records revealed that on or about May 22, 2012, defendant SESTAK issued a visa to T.T.M.L. Additionally, this applicant's biographical data was located in a shell email account used by members of the conspiracy. See infra pars. 66-71..

39. DSS review of consular records revealed that on or about May 22, 2012, a visa application was submitted to the Consulate for N.T.M.L. from the HONG VO IP Address and listed Person 3 as N.T.M.L.'s U.S. point of contact and Person 3's work address as the U.S. destination.

40. DSS review of consular records revealed that on or about May 23, 2012, defendant SESTAK issued a visa to N.T.M.L.

41. DSS review of consular records revealed that on or about May 21, 2012, a visa application was submitted to the Consulate for K.M.T. from the HONG VO IP Address and listed an address in Hawaii as the destination address (hereinafter "Hawaii Address"); Person 4, Person 5, and Person 6 were all associated with the Hawaii Address or with residents of the Hawaii Address.

42. DSS review of financial records revealed that on or about May 21, 2012, Person 4, who lived at the Hawaii Address, transferred \$45,000 from a Bank of Hawaii account to defendant ALICE NGUYEN's Wells Fargo account.

43. DSS review of financial records revealed that on or about May 22, 2012, Person 5 transferred \$20,000 from a Bank of Hawaii account to defendant ALICE NGUYEN's Wells Fargo account.

44. DSS review of financial records revealed that on or about May 22, 2012, Person 6

transferred \$15,000 from a Wells Fargo account to defendant ALICE NGUYEN's Wells Fargo account.

45. DSS review of consular records revealed that on or about May 22, 2012, defendant SESTAK issued a visa to K.M.T.

46. DSS review of consular records revealed that on or about May 23, 2012, a visa application was submitted to the Consulate for T.T.N. and listed the destination address as the Hawaii Address.

47. DSS review of consular records revealed that on or about May 23, 2012, defendant SESTAK issued a visa to T.T.N.

48. DSS review of consular records revealed that on or about May 22, 2012, a \$20,000 money transfer was made from Person 7's Bank of Hawaii account to defendant ALICE NGUYEN's Wells Fargo account.

49. DSS review of consular records revealed that on or about May 30, 2012, a visa application was submitted to the Consulate for T.V.P. from the BINH VO IP Address and listed Person 7 as the U.S. point of contact.

50. DSS review of consular records revealed that on or about May 31, 2012, defendant SESTAK issued a visa to T.V.P.

F. SESTAK's Transfer of Funds to a Thai Bank Account During the Conspiracy

51. DSS investigation revealed that SESTAK opened at least one bank account at the Siam Commercial Bank PLC located in Bangkok, Thailand ("SESTAK Thailand Bank Account"), in May 2012.

52. DSS review of financial records revealed that between June 20, 2012, and September 11, 2012, 35 transfers totaling approximately \$3.2 million dollars were made to the

SESTAK Thailand Bank Account. The majority of the transfers came from the Bank of China.

53. The investigation has revealed evidence that ALICE NGUYEN's father and Person 11, aided the conspirators in moving money out of Vietnam to Thailand and to the United States. On June 28, 2012, ALICE NGUYEN's father sent ALICE NGUYEN an email forwarding the transaction details for a \$150,000 USD transfer to the SESTAK Thailand Bank Account that was made on June 25, 2012, from a Bank of China account. The body of the email contained forwarding information that indicated that it was originally sent to ALICE NGUYEN's father by Person 11.

54. A total of 4 emails were sent from ALICE NGUYEN's father to ALICE NGUYEN containing transaction details of a total of \$600,000 in transfers to the SESTAK Thailand Bank Account, and a \$100,000 transfer to the ALICE NGUYEN Wells Fargo Account. All four emails appeared to have originated from Person 11.

55. Additionally, a total of three emails were sent from Person 11 to ALICE NGUYEN containing transaction details of a total of approximately \$1.46 million in transfers to the SESTAK Thailand Bank Account, and \$200,000 in transfers to the ALICE NGUYEN Wells Fargo Account.

56. DSS investigation revealed that over the calendar year before September 2012, SESTAK earned approximately \$7,500 per month after taxes from both his position as a Foreign Service Officer with the U.S. Department of State, and as a reservist with the U.S. Navy.

G. Transfer of Funds to ALICE NGUYEN's U.S. Wells Fargo Account

57. DSS investigation revealed that between June 25, 2012, and September 6, 2012, approximately 39 international transfers totaling approximately \$2,999,400.18 were made into the ALICE NGUYEN Wells Fargo Account. Thirty-six of the transfers came from the Bank of

China. At least one of the transfers appeared to originate from the same Bank of China account that had transferred some of the funds to the SESTAK Thailand Bank Account.

58. DSS review of records from the ALICE NGUYEN Wells Fargo Account from January 18, 2011, through May 20, 2012, revealed that the main source of income into the account were direct deposits from Company A. Company A is a real estate company. From January 31, 2011, to February 29, 2012, ALICE NGUYEN received approximately \$60,114.34 from Company A.

H. Statements Made By Co-Conspirators Regarding the Conspiracy

59. DSS review of information acquired through several court-authorized search warrants executed during the investigation revealed electronic chats and emails from HONG VO and BINH VO advertising and discussing aspects of the fraudulent visa scheme.

60. In a chat dated July 16, 2012, HONG VO discussed the fraudulent visa scheme with an acquaintance that it was encouraging to locate customers. She described it as a “unique opportunity” and stated “you could also make some good \$\$ on the side.” HONG VO stated that she had met “this lawyer . . . who is really close to me now.” She further described that the “lawyer” could guarantee people visas to the United States, including people who “can’t get a VISA to the States . . . or want to go but they have no chance.” She stated that people who received the visas usually overstayed the visas. When asked about the price, HONG VO said the cost was \$50-70,000, but that the “lawyer” could go as low as \$20,000. HONG VO also stated that the recipient of the email could take a commission for referring a customer.

61. In an email dated July 5, 2012, HONG VO discussed the fraudulent visa scheme with an acquaintance. HONG VO asked if the acquaintance or the acquaintance’s parents,

“know anyone in Vietnam who wants to go to the US but can’t because either 1) they will most likely get rejected or 2) they have already been rejected and there’s no way for them to come.” She described that she knew someone who can “get people to the States” and that it cost about \$50,000. She continued, “[t]his opportunity will only last for a few more months and after that it’s over. . . . It’s only for a tourist Visa (not citizenship) but once you go . . . you can disappear (get married) or return back to Vietnam and get the green light to go whenever you apply for another Visa to go to the States. Please keep this information on the dl.” At the time the email was written, the scheme would have been expected to only last a few additional months, because SESTAK was scheduled to depart Ho Chi Minh City in September 2012 for a deployment with the U.S. Navy.

62. In an electronic chat dated July 20, 2012, HONG VO described the visa scheme, stating that she knew a “lawyer” who guaranteed visas to the US, even for people who had been rejected, but that he would only be “doing it for about 2 more months and he’s going to stop.” HONG VO continued that some people had paid \$50-70,000 to go. She then described the two groups of people who generally can’t receive visas to the US as “1) the ones that have been rejected 2) the ones that live in the countryside and don’t have a strong enough background that will make the us officials comfortable to let them to abroad.” She later added, “oh! Here’s the other part – he does it within 3 days . . . gets them into an interview right away. . . and he has a girl who will train them how to do their interviews.”

63. In an electronic chat between BINH VO and a family member, dated April 9, 2012, BINH VO said that it may have someone who would want to pay in the US, “and if so, I will have that person transfer money to your bank account.” BINH VO then stated, “You should open a USD account at Vietcombank to be safe as HSBC can be checked by US gov’t. . . . Just

to be safe, you should not have over \$10 grand in your HSBC account, but you can in the Vietcombank account.”

I. TRUC HUYNH's Participation in the Bribery Scheme

64. During an electronic chat dated June 28, 2012, BINH VO and one of his siblings discussed TRUC HUYNH: “[TRUC HUYNH]’s my runner now and deals w/ all the agents, etc., and I specifically told [TRUC HUYNH] not to tell ANYONE. I got [TRUC HUYNH] a US visa also already.” BINH VO’s sibling then stated that it was easier to target Vietnamese-Americans “as they have money and are desperate to bring their relatives over.” BINH VO responded, “That’s fine, have them call Truc and say who refer[red them]. BINH VO then stated, “[TRUC HUYNH's] name is Thanh. Truc=Thanh. We all have different names.” Notably, TRUC HUYNH's Shell E-mail Account, thanhnguyen896@gmail.com, included the alias name “Thanh.” See *infra* pars. 68-71.

65. In an electronic chat dated July 31, 2012, HONG VO and an acquaintance discussed a person called “T:”

HONG VO: the client will work with Thanh to get the V now
...
ACQUAINTANCE : who is collecting the money?
HONG VO: T will
ACQUAINTANCE: kk in VN?
HONG VO: T will sit with the lady at a coffee shop . . . to collect the \$. . . until the girl gets her V
ACQUAINTANCE: should someone be backing her up? . . . just in case?
HONG VO: she’s been doing this for a while... so it’s okay.

Your affiant believes that “T” is TRUC HUYNH, who was also known as Thanh.

J. Shell Email Accounts Used by BINH VO, TRUC HUYNH, and Other Co-Conspirators

66. DSS review of information acquired through a court-authorized search warrant executed on the BINH VO Google Account revealed an email that contained what appeared to be a list of approximately 11 email accounts and accompanying passwords (“Shell Email Accounts”).

67. DSS review of information acquired through search warrants executed on the 11 Shell Email Accounts revealed that the co-conspirators used several of the Shell Email Accounts to receive biographical information for visa applicants, to include scans of identity documents and visa photos, which were sent by applicants and by other co-conspirators. The Shell Email Accounts were also used to receive interview appointment confirmations from the Consulate; and to email visa photos, appointment confirmations, or biographical information for visa applicants to other known members of the conspiracy.

68. DSS investigation revealed that an additional Google email account, thanhnguyen896@gmail.com, (“TRUC HUYNH Shell Email Account”) was a shell account controlled by TRUC HUYNH.

69. Review of the subscriber information for the TRUC HUYNH Shell Email Account revealed a phone number that matched a phone number listed on TRUC HUYNH’s 2012 visa application. Further review of the subscriber information revealed that the alternate email address listed, huynh.thanhtruc83@gmail.com, was subsequently used by TRUC HUYNH to correspond with representatives of the Consulate regarding her visa status in 2013.

70. Review of the contents of the TRUC HUYNH Shell Email Account, which were obtained pursuant to a court-authorized search warrant, revealed that the account was used to send biographical data or visa photographs for at least 222 applicants to whom SESTAK issued visas to, to one of the Shell Email Accounts. This causes your affiant to believe that TRUC

HUYNH recruited customers to the fraudulent visa scheme, and assisted BINH VO with formatting applicants' biographical information for visa applications.

71. Between July 11 and August 26, 2012, TRUC HUYNH sent approximately six emails from the TRUC HUYNH Shell Email Account, in which she provided model questions and answers in Vietnamese that would be asked during a typical NIV interview, to unknown persons. For example:

Question: Have you ever traveled to a foreign country before?

Answer: I have

Question: What country have you traveled to?

Answer: I have been to Australia

Question: Why is it not on your passport?

Answer: Because my passport had expired, I changed to a new passport therefore I did not bring it with me.

Question: What year did you travel?

Answer: I went in 2011

72. On May 6, 2013, Chief Judge Royce Lamberth of the U.S. District Court for the District of Columbia issued an arrest warrant for TRUC HUYNH. See miscellaneous Case No. 13-458. On May 8, 2013, TRUC HUYNH was arrested in Denver, Colorado on the warrant. At the time of her arrest, TRUC HUYNH was holding the iPhone in her hand. The iPhone was seized by DSS Agents and taken to the DSS Denver Resident Office for safekeeping. The iPhone has remained at the DSS Denver Resident Office since that time. The iPhone model A1387 was first released by Apple in 2011, before the start of the conspiracy. It is reasonable to believe that the iPhone may contain evidence of the conspiracy.

73. On May 31, 2013, United States Magistrate Judge Alan Kay of the U.S. District Court for the District of Columbia issued an arrest warrant pursuant to a criminal complaint charging TRUC HUYNH with one count of Conspiracy in violation of 18 U.S.C. § 371. See *United States v. Truc Thanh Huynh*, Criminal Case No. 1:13-mj-0463. On June 3, 2013,

TRUC HUYNH was arrested on the warrant in the District of Columbia.

On July 9, 2013, TRUC HUYNH was indicted for violations of 18 U.S.C. § 371 (Conspiracy), 18 U.S.C. § 201(b)(2) (Bribery), 18 U.S.C. § 2 (Aiding and Abetting and Causing an Act to be Done), and 18 U.S.C. § 1546 (Fraud and Misuse of Visas).

TECHNICAL TERMS RELATED TO THE SEARCH OF THE IPHONE

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

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and email; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; and storing dates, appointments, and other information on personal calendars. Wireless telephones can be used to access the Internet through cellular networks, 802.11 “wi-fi” networks, or otherwise. Some wireless telephones contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving email, and participating in Internet social networks. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

b. Digital camera: a digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or video.

c. Portable media player: A portable media player (or “MP3 Player” or iPod”) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage

media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: a GPS navigation device uses the Global Positioning System to display its current location. It often contains records of the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System, (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.

f. IP address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range of 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static – that is long-term – IP addresses, while other computers have dynamic – that is, frequently changed – IP addresses.

g. 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.

75. Based on my training, experience, and research, I know that the iPhone has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on this type of “smart” cellular phone can uncover, among other things, evidence that reveals or suggests who possessed or used the device, emails, texts, email addresses used, IP address information, and internet browsing history.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

76. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time, including text messages. Texts messages sent or received on a cellular phone can be stored on a cellular phone at little or no cost. Even when text messages have been deleted by the user of a cellular phone, those text messages, or remnants of those deleted text files, can be recovered months after they have been deleted from a cellular phone. This is so because when a user of a cellular phone “deletes” a text message, the data contained in that message does not actually disappear; rather, that data remains on the cellular phone until it is overwritten with new data. Deleted text messages, or remnants of deleted text messages, may reside on the cellular phone for long periods of time before they are overwritten. Such data can sometimes be recovered with forensic tools.

77. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information on the iPhone that might serve as evidence of the crimes described on the warrant, but also forensic evidence that establishes how the iPhone was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the iPhone 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).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. Identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic 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 device 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.

78. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the iPhone consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the iPhone to human inspection in order to determine whether it is evidence described by the warrant.

79. *Manner of Execution.* Because this warrant seeks only permission to examine a iPhone already in law enforcement’s possession, the execution of this warrant does not involve

the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

80. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the iPhone described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

s/ Simon Dinitz
Special Agent Simon Dinitz
Diplomatic Security Service

Reviewed and submitted by Assistant United States Attorney Pegeen D. Rhyne.

Sworn telephonically and signed electronically on this 23rd day of July, 2013 at Denver, CO.


UNITED STATES MAGISTRATE JUDGE

UNITED STATES DISTRICT COURT

for the
District of Colorado

In the Matter of the Search of)
(Briefly describe the property to be searched)
or identify the person by name and address))

Case No. 13-sw-05636-KLM

Apple iPhone Model #A1387, IMEI # 013072007554078.
Serial # C8PHT314DTD1 and FCC ID # BCG-E2430A)
)
)

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the State District of Colorado
(identify the person or describe the property to be searched and give its location):
See Attachment A

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized):
See Attachment B

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before August 6, 2013
(not to exceed 14 days)

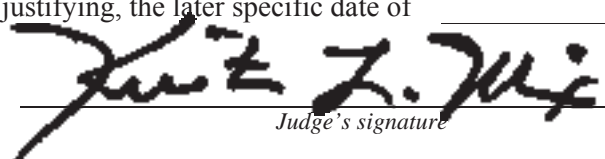
in the daytime 6:00 a.m. to 10 p.m. at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge Kristen L. Mix
(name)

I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 and 3103(a) (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box) for days (not to exceed 30).
 until, the facts justifying, the later specific date of .

Date and time issued: 11:03 am, Jul 23, 2013


Judge's signature

City and state: Denver, CO Kristen L. Mix, U.S. Magistrate Judge
Printed name and title

AO 93 (Rev. 12/09) Search and Seizure Warrant (Page 2)

<i>Return</i>		
<i>Case No.:</i>	<i>Date and time warrant executed:</i>	<i>Copy of warrant and inventory left with:</i>
<i>Inventory made in the presence of :</i>		
<i>Inventory of the property taken and name of any person(s) seized:</i>		
<i>Certification</i>		
<p style="text-align: center;"><i>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</i></p>		
<i>Date:</i> _____	_____ <i>Executing officer's signature</i>	
	_____ <i>Printed name and title</i>	

ATTACHMENT A

The property to be searched is described as follows:

The property to be searched is a white Apple iPhone Model #A1387, IMEI# 013072007554078, serial# C8PHT314DTD1 and FCC ID# BCG-E2430A (“the iPhone”). The iPhone is currently located at the Diplomatic Security Service Denver Resident Office, at 8101 East Prentice Avenue, Suite 550, Greenwood Village, Colorado, 80111, Evidence Storage Area, Shelf D.

This warrant authorizes the forensic examination of the iPhone for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records and items on the iPhone described in Attachment A that relate to violations of 18 U.S.C. § 371 (Conspiracy), 18 U.S.C. § 1546 (Visa Fraud), 18 U.S.C. 201§ (b)(2) (Bribery of a Public Official), those violations involving Truc Huynh, including correspondence, records, documents, photographs, videos, electronic mail, chat logs, text messages, and electronic messages, including:

- a. records or information relating to the preparation of visa applications, making or confirmation of visa appointments, meetings with visa customers, collecting money from visa customers, or recruiting additional recruiters or visa applicants;
- b. records or information relating to TRUC HUYNH's whereabouts, schedule, travel, or activities;
- c. records or information relating to TRUC HUYNH's conversations with any and all known and unknown co-conspirators, including SESTAK, BINH VO, ALICE NGUYEN, and HONG VO;
- d. all communications to or from TRUC HUYNH from January 1, 2012 to present;
- e. all communications, records, or documents related to the transfer or intended transfer or funds in the United States or abroad, between January 1, 2012 and the present;
- f. all communications, records, or documents related to the attempt to launder money or structure deposits between January 1, 2012 and the present;
- g. records or information relating to the state of mind of TRUC HUYNH;
- h. records or information relating to the state of mind of any known or unknown conspirators or visa applicants concerning the visa fraud, bribery, and money laundering scheme detailed in the accompanying Affidavit;
- i. records or information relating to who used, owned, or controlled the iPhone; and

j. records or information relating to the times and/or locations where the iPhone was used, including Internet Protocol addresses.

2. As used above, 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 electronic storage and any photographic form.

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

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

Case No. 13-sw-05636-KLM

APPLICATION

INTRODUCTION

The United States of America, by and through John Walsh, United States Attorney, and Pegeen Rhyne, Assistant United States Attorney, hereby moves this Court under the All Writs Act, 28 U.S.C. § 1651, for an order requiring Apple, Inc. (“Apple”) to assist in the execution of a federal search warrant by bypassing the lock screen of an iOS device, specifically, a white Apple iPhone Model #A1387, IMEI# 013072007554078, serial# C8PHT314DTD1 and FCC ID# BCG-E2430A (hereinafter “the iPhone”). The iPhone is currently located at the Diplomatic Security Service Denver Resident Office, at 8101 East Prentice Avenue, Suite 550, Greenwood Village, Colorado, 80111, Evidence Storage Area, Shelf D.

FACTS

The Diplomatic Security Service (“DSS”) came into possession of the iPhone as follows: On May 8, 2013, defendant Truc Thanh Huynh was arrested in Denver, Colorado on an arrest warrant issued on May 6, 2013 by Chief Judge Royce Lamberth of the U.S. District Court for the District of Columbia, see District of Columbia miscellaneous Case No. 13-458.

On May 31, 2013, United States Magistrate Judge Alan Kay of the U.S. District Court for the District of Columbia issued an arrest warrant pursuant to a criminal complaint charging Truc Thanh Huynh with one count of Conspiracy in violation of 18 U.S.C. § 371. See United States v. Truc Thanh Huynh, Criminal Case No. 1:13-mj-0463. Truc Thanh Huynh was arrested in the District of Columbia on the warrant on June 3, 2013.

At the time of her arrest in Denver, Colorado, defendant Truc Thanh Huynh had the iPhone in her possession. The government is submitting a separate application for a warrant to search the iPhone, concurrently with this application, to the United States District Court for Colorado.

A visual inspection of the iPhone revealed that it is locked. Because the iPhone is locked, law enforcement agents are not able to examine the data stored on the iPhone pursuant to the search warrant application being submitted concurrently with this application.

Apple, the creator of the iPhone's operating system and producer of the iPhone, may have the capability retrieving data stored on the iPhone that is not currently accessible to DSS because the iPhone is locked. This Application seeks an order requiring Apple to use any such capability, so as to assist agents in complying with the search warrant.

DISCUSSION

The All Writs Act provides that “[t]he Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law.” 28 U.S.C. § 1651(a). As the Supreme Court explained, “[t]he All Writs Act is a residual source of authority to issue writs that are not otherwise covered by statute.” *Pennsylvania Bureau of Correction v. United States Marshals Service*, 474 U.S. 34, 43 (1985). “The power conferred by the Act extends, under appropriate circumstances, to persons who, though not parties to the original action or engaged in wrongdoing, are in a position to frustrate the implementation of a court order or the proper administration of justice... and encompasses even those who have not taken any affirmative action to hinder justice.” *United States v. New York Tel. Co.*, 434 U.S. 159, 174 (1977). Specifically, in *United States v. New York Tel. Co.*, the Supreme Court held that the All Writs

Act permitted district courts to order a telephone company to effectuate a search warrant by installing a pen register. Under the reasoning of *New York Tel. Co.*, this Court has the authority to order Apple to use any capabilities it may have to assist in effectuating the search warrant.

The government is aware, and can represent, that in other cases, courts have ordered Apple to assist in effectuating search warrants under the authority of the All Writs Act. Additionally, Apple has complied with such orders.

The requested order would enable agents to comply with this Court's warrant commanding that the iOS device be examined for evidence identified by the warrant. Examining the iPhone without Apple's assistance, if it is possible at all, would require significant resources and may harm the iPhone. Moreover, the order is not likely to place any unreasonable burden on Apple.

Respectfully submitted,

s/Pegeen Rhyne
Pegeen Rhyne
ASSISTANT UNITED STATES ATTORNEY

Date: July 23, 2013

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

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

Case No. 13-sw-05636-KLM

APPLICATION

ORDER

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

ORDERED that Apple assist law enforcement agents in the examination of the iPhone, Model #A1387, IMEI# 013072007554078, serial# C8PHT314DTD1 and FCC ID# BCG-E2430A (hereinafter "the iPhone"), acting in support of a search warrant issued separately by the United States District Court for the District of Colorado;

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

FURTHER ORDERED that, to the extent that data on the iPhone 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 iPhone user's passcode so that the agents may search the iPhone, extracting data from the iPhone and copying the data onto an external hard drive or other storage medium that law enforcement agents may search, or otherwise circumventing the iPhone 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 iPhone, 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.

Signed

MAGISTRATE KRISTEN L. MIX
UNITED STATES MAGISTRATE JUDGE

Date: 23 Jul 2013