UNITED STATES DISTRICT COURT

for the

Eastern District of California

In the Matter of the Search of)
IPHONE (COLOR: WHITE. MODE[.: A 1428; IMEI: 013425001705775) CURRENTLY LOCATED AT FEDERAL BUREAU OF INVESTIGATION,45OO ORANGE CROVEAVE. SACRAMENTO CA 9584I EVIDENCE ITEM BAR CODE E5196474)

Case No. 2:15-SW-0211 AC

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, attached hereto and incorporated by reference.

located in the Eastern District of California , there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B, attached hereto and incorporated by reference

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:

Code Section	*Offense Description*
18 U.S.C. § 201	Bribery of a Public Official

The application is based on these facts:

SEE AFFIDAVIT, attached hereto and incorporated by reference.

☑ Continued on the attached sheet.

Applicant's signature

Matthew Young, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 5/7/15

Judge's signature

City and state: Sacramento, California

Allison Claire, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR EASTERN DISTRICT OF CALIFORNIA

IN THE MATTER OF THE SEARCH OF IPHONE (COLOR: WHITE, MODEL: A1428, IMEI: 013425001705775), CURRENTLY LOCATED AT FEDERAL BUREAU OF INVESTIGATION, 4500 ORANGE GROVE AVE, SACRAMENTO, CALIFORNIA 95841; EVIDENCE ITEM BAR CODE E5196474	Case No. 2:15-SW-0211 AC

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Matthew Young, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. A previous search warrant was obtained for this item, however, due to a device security code that the technical agent code not by bypass or disable, the item was unable to be searched within the time frame specified in the original warrant. As a result, and to remedy the issue, an additional order is being request to compel Apple, Inc to assist in the execution of the search warrant.

3. I am a Special Agent with the Federal Bureau of Investigation and have been since October 1998. I received over four months of investigative training at the FBI Academy in

Quantico, Virginia. I have attended several training course during the past 16 years that directly relate to corruption investigations. During my time as a Special Agent with the FBI, I have conducted and/or participated in hundreds of criminal investigations involving, but not limited to: Corruption of Public Officials, Money Laundering, Criminal Enterprises, Terrorism, National Security Matters, Bank Fraud, Mail Fraud, Drugs, Wire Fraud, Computer Fraud, Financial Institution Fraud, Mortgage Fraud, and other white collar crimes. Many of these investigations have involved the use of cooperating witnesses, informants, and confidential human sources. I have conducted and/or participated in numerous search warrants and have written affidavits in support of search warrants. I have conducted physical surveillance and have monitored electronic surveillance. I am currently assigned to the Sacramento Division of the FBI on an investigative squad that handles the investigation of public corruption. I have extensive experience and training related to computers, computer networking, and computer operating systems.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

5. The property to be searched is an IPHONE (COLOR: WHITE, MODEL: A1428, IMEI: 013425001705775), hereinafter the "Device." The Device is currently located at the Evidence Control Room, 4500 Orange Grove Ave, Sacramento, California 95841; Evidence Bar Code: E5196474.

6. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

7. In 2011, AHMED PERVEZ AARIANPUR (hereinafter "AARIANPUR") worked as a private contractor in Afghanistan. His company, Integrity Construction Company, Inc., worked to obtain various contracts from the U.S. military. AARIANPUR met a U.S. Air Force contracting officer, hereinafter referred to as the confidential human source ("CHS"). In 2011, the CHS awarded AARIANPUR multiple contracts in exchange for a bribe payment of $30,000.

8. In May 2012, FBI agents confronted the CHS about his in role accepting bribes in exchange for awarding U.S. government contracts. The confidential human source admitted accepting bribes, decided to cooperate with the FBI in an ongoing investigation.

9. In April 2014, the CHS told the FBI about his illegal relationship with AARIANPUR, which as detailed above, began in 2011 in Afghanistan

10. In July 2014, at the direction of the FBI, the CHS approached AARIANPUR, a resident of Dubai, United Arab Emirates, via e-mail to reestablish their relationship. AARIANPUR responded immediately, and within 10 days he and the CHS began to discuss government contracts. Through numerous emails and recorded phone calls between Dubai, United Arab Emirates and Sacramento, California, the two discussed the acquisition of government contracts and proprietary bid information in exchange for bribe payments.

11. On August 5, 2014, the CHS and AARIANPUR spoke on the phone, and the FBI consensually recorded the call. The CHS told AARIANPUR that the military was issuing

contracts for goods needed in Afghanistan from a unit at Travis AFB. By the terms of the contracts, the goods would need to be shipped to Travis AFB for inspection. If the goods passed inspection, the military would then ship the goods from Travis AFB to Afghanistan. The news seemed to excite AARIANPUR, who asked about available contracts. The CHS informed AARIANPUR about a contract for electronic door locks. They discussed meeting in person after the contract was awarded. AARIANPUR said he would like to meet in Europe. The CHS suggested Prague, Czech Republic. AARIANPUR said he would let the CHS know about his profit from the proposed contract and let the CHS specify his payment. AARIANPUR added he would "take care" of the CHS, who in turn said he would find a contract and "talk dollars later." The CHS suggested that AARIANPUR send in separate bids for his companies in Iraq and Afghanistan.

12. On August 6, 2014, the CHS and AARIANPUR spoke on the phone, and the FBI consensually recorded the call. The CHS told AARIANPUR that he needed to account for a U.S. Air Force contracting officer (herein after the "Contracting Officer") at Travis AFB with any payments he intended to make. The Contracting Officer was also working with the FBI as a CHS. AARIANPUR acknowledged the point and said he would "take care" of both the CHS and the Contracting Officer.

13. On August 25, 2014, the CHS and AARIANPUR spoke on the phone, and the FBI consensually recorded the call. The two discussed the upcoming electronic lock contract, worth more than $1.1 million, and the CHS guaranteed he and the Contracting Officer could make sure AARIANPUR won the contract. When the CHS asked how much he and the Contracting Officer would make on the deal, AARIANPUR eventually said, "I will give you

guys thirty percent of whatever I make; thirty percent for you guys." AARIANPUR expected to make roughly $300,000 in profit. The CHS and AARIANPUR then discussed how the 30% would be divided. They settled on $45,000 for the CHS and $45,000 for the Contracting Officer. The CHS told AARIANPUR that he would let the Contracting Officer know about the arrangement.

14. On August 26, 2014, the CHS and AARIANPUR spoke on the phone, and the FBI consensually recorded the call. At two points during the call, the CHS arranged for the Contracting Officer to join the telephone call under the pretense that the Contracting Officer wanted to verify the arrangement to make sure the CHS would not cheat him out of his portion of the bribe payment. Though AARIANPUR asked the CHS if it was appropriate "to talk in the open," once the Contracting Officer joined the telephone call, AARIANPUR confirmed the 30% cut and the division of that cut between the CHS and the Contracting Officer.

15. On September 1, 2014, the CHS and AARIANPUR spoke on the phone, and the FBI consensually recorded the call. AARIANPUR determined his cost for the electronic door locks and asked the CHS for the maximum bid amount. The CHS said he would talk with the Contracting Officer to identify what other bids might have come in and get back to him.

16. The CHS and AARIANPUR exchanged a number of e-mails after September 1, 2014, in which they discussed the contract and various bids. Using the bid information the CHS and the Contracting Officer provided, AARIANPUR was able to raise his offer from $1.1 million to roughly $1.4 million without losing his status as the lowest bidder.

17. In early September 2014, AARIANPUR promised to purchase a plane ticket for the CHS to travel from California to the Prague, Czech Republic. In addition, AARIANPUR would pay for the CHS' hotel during his stay in Prague. They agreed that the expense for the plane ticket and the lodging would be considered part of the CHS' bribe payment. They planned to meet in Prague in late September and/or early October. AARIANPUR told the CHS that he would not wire the bribe money. AARIANPUR said he would make a bribe payment in person and planned to do so in Prague. They planned to meet in Prague from September 30 through October 2, 2014

18. On September 30, 2014, the CHS and AARIANPUR met in Prague, Czech Republic, to make/receive an initial bribe payment. On that day, after some discussion about future contracts, AARIANPUR gave the CHS an initial bribe payment in the form of a Rolex watch.

19. The following day, October 1, 2014, the CHS and AARIANPUR met again in Prague, Czech Republic and, after more conversation about contracts, AARIANPUR made another bribe payment to the CHS. This bribe payment was $5,000 in cash. AARIANPUR was arrested the next morning on October 2, 2014, by the Czech National Police.

20. On October 2, 2014, the Czech National Police seized an iPhone from AARIANPUR. I witnessed AARIANPUR while conducting surveillance of the CHS meeting with AARIANPUR in Prague, Czech Republic. AARIANPUR possessed and used an iPhone. While in the Czech Republic, the CHS communicated with AARIANPUR by calling and/or texting AARIANPUR's cellular telephone number. The iPhone seized by the Czech National Police was the only cellular telephone found by the Czech National Police during their search of

AARIANPUR's person and hotel room. While AARIANPUR was believed to be in the United Arab Emirates and while AARIANPUR was in Prague, Czech Republic, the CHS called AARIANPUR at telephone number 0097 152 948 015. I do not know if this is the same number as the SIM installed in the target phone.

21. The Device is currently in the lawful possession of the Federal Bureau of Investigation. It came into the Federal Bureau of Investigation's possession in the following way: the Device was seized by the Czech National Police following the arrest of AARIANPUR and immediately turned over to the Federal Bureau of Investigation in accordance with a Mutual Legal Assistance Treaty. Therefore, while the Federal Bureau of Investigation might already have all necessary authority to examine the Device, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Device will comply with the Fourth Amendment and other applicable laws.

22. The Device is currently in storage at Evidence Control Room, 4500 Orange Grove Ave, Sacramento, California 95841; Evidence Bar Code: E5196474. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the Federal Bureau of Investigation.

TECHNICAL TERMS

23. 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. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. 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 e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. 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 videos.

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 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. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital 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. 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.

24. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product technical specifications available online at http://www.apple.com/iphone/, I know that the Device 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 devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

25. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

26. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device 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 Device 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. The process of identifying the exact electronically stored information on a storage medium that are 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.

27. *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 device 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 device to human inspection in order to determine whether it is evidence described by the warrant.

28. *Manner of execution.* Because this warrant seeks only permission to examine a device 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

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

Respectfully submitted,

MATTHEW YOUNG
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on May 6, 2015:

ALLISON CLAIRE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

1. The property to be searched is an IPHONE (COLOR: WHITE, MODEL: A1428, IMEI: 013425001705775), hereinafter the "Device." The Device is currently located at the Evidence Control Room, 4500 Orange Grove Ave, Sacramento, California 95841; Evidence Bar Code: E5196474.

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

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of Title 18, United States Code (Bribery) and involve AHMED AARIANPUR since July 2014, including:

   a. emails sent or received, draft emails, text messages, call records, voice mails, or other communication records;

   b. lists of customers and related identifying information;

   c. types, amounts, and prices of products for the satisfaction of the contract as well as dates, places, and amounts of specific transactions;

   d. any information related to sources of the products for the satisfaction of the contract (including names, addresses, phone numbers, or any other identifying information);

   e. all bank records, checks, credit card bills, account information, and other financial records.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

IN THE UNITED STATES DISTRICT COURT
FOR EASTERN DISTRICT OF CALIFORNIA

IN RE ORDER REQUIRING APPLE, INC. TO ASSIST IN THE EXECUTION OF A SEARCH WARRANT ISSUED BY THIS COURT	Case No. 2:15-SW-0211 AC APPLICATION

INTRODUCTION

The United States of America, by and through Benjamin Wagner, United States Attorney, and Michael Beckwith, 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, an Apple iPhone.

FACTS

The Federal Bureau of Investigation (FBI) currently has in its possession an iOS device that was seized by the Czech National Police following the arrest of AARIANPUR and immediately turned over to the FBI in accordance with a Mutual Legal Assistance Treaty (MLAT). Initial inspection of the iOS device reveals that it is locked. Because the iOS device is locked, law enforcement agents are not able to examine the data stored on the iOS device as commanded by the search warrant.

The iOS device is an iPhone. It has Model # A1428, with access number (phone number) 0097 152 948 0151, IMEI: 01342500170577.

Apple, the creator of the iOS operating system and producer of the iOS device, may be capable of retrieving data stored on the iOS device that is not currently accessible to the FBI because the iOS device 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 iOS device without Apple's assistance, if it is possible at all, would require significant resources and may harm the iOS device. Moreover, the order is not likely to place any unreasonable burden on Apple.

Respectfully submitted,

MICHAEL BECKWITH
Assistant United States Attorney

Date: May 7, 2015

UNITED STATES DISTRICT COURT

for the

Eastern District of California

In the Matter of the Search of)
IPHONE (COLOR: WHITE. MODE[.: A 1428; IMEI: 013425001705775) CURRENTLY LOCATED AT FEDERAL BUREAU OF INVESTIGATION,4500 ORANGE CROVEAVE. SACRAMENTO CA 95841 EVIDENCE ITEM BAR CODE E5196474)

Case No. 2:15-SW-0211 AC

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 Eastern District of California *(identify the person or describe the property to be searched and give its location)*:

SEE ATTACHMENT A, attached hereto and incorporated by reference.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B, attached hereto and incorporated by reference.

YOU ARE COMMANDED to execute this warrant on or before 5/21/15 *(not to exceed 14 days)*

☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good 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: any authorized U.S. Magistrate Judge in the Eastern District of California.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (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: 5/7/15

Judge's signature

City and state: Sacramento, California

Allison Claire, U.S. Magistrate Judge
Printed name and title

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

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

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

Signature of Judge

Date

IN THE UNITED STATES DISTRICT COURT
FOR EASTERN DISTRICT OF CALIFORNIA

IN RE ORDER REQUIRING APPLE, INC. TO ASSIST IN THE EXECUTION OF A SEARCH WARRANT ISSUED BY THIS COURT	Case No. 2:15-SW-0211 AC **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. 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 with Model # A1428, with access number (phone number) 0097 152 948 0151, IMEI: 013425001705775 (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.

Signed,

ALLISON CLAIRE
UNITED STATES MAGISTRATE JUDGE

Date: 5/7/15