

FILED

UNITED STATES DISTRICT COURT
DISTRICT OF NEW MEXICO

UNITED STATES DISTRICT COURT

DEC 30 2013

for the
District of New Mexico

MATTHEW J. DYKMAN
CLERK

In the Matter of the Search of

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

AN APPLE IPHONE CELLULAR TELEPHONE, MODEL
A1387, FCC ID: BCG-E2430A, IC: 579C-E2430A

Case No. 13MR1026

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

located in the _____ District of New Mexico, there is now concealed (identify the person or describe the property to be seized):
See Attachment B

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>
Title 21 U.S.C. Sections 841 and 846	Distribution of Heroin, Conspiracy to Distribute Heroin

The application is based on these facts:
See Attached Affidavit

- Continued on the attached sheet.
- 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.

Julie Olmsted

Applicant's signature

Julie A. Olmsted, Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: December 30, 2013

Karen B. Molzen

Judge's signature

City and state: Albuquerque, NM

Karen B. Molzen, Chief U.S. Magistrate Judge

Printed name and title

IPHONE IN THE UNITED STATES DISTRICT COURT
FOR DISTRICT OF NEW MEXICO

IN THE MATTER OF THE SEARCH OF AN
APPLE IPHONE CELLULAR TELEPHONE,
MODEL A1387, FCC ID: BCG-E2430A, IC:
579C-E2430A CURRENTLY LOCATED AT
THE DRUG ENFORCEMENT
ADMINISTRATION, 2660 FRITTS
CROSSING SE, ALBUQUERQUE, NM
87106

Case No. _____

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

I, Julie A. Olmsted, 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 are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Drug Enforcement Administration (DEA), and have been since January 2012. My experience as a Special Agent includes, but is not limited to, conducting surveillance, interviewing witnesses, writing affidavits for and executing search warrants, working with undercover agents and informants. I have received training in and have experience in the investigation of violations of the federal drug and offenses, including the offenses listed below. I have investigated numerous drug trafficking conspiracies and have participated in multiple Title III operations. I am, and agents assisting in this investigation are,

familiar with matters including, but not limited to, the means and methods used by persons, and drug trafficking organizations (“DTOs”), to purchase, transport, store, and distribute illegal drugs and to hide profits generated from those transactions. I also have experience in analyzing and interpreting drug codes and cryptic dialogue used by drug traffickers. I am aware that DTOs are concerned about the efforts law enforcement make to disrupt and dismantle their activities.

3. 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.

4. Through my training and experience I have learned that:

- a. Drug traffickers often conceal names, addresses, telephone numbers, email addresses, or other pertinent codes and or contact information for their current or past illegal drug source(s) of supply, customers, or criminal associates in the electronic memory of their telephones/personal digital assistant PDA;
- b. Drug traffickers often conceal photographs of drugs, vehicles, locations, or photographs of drug associates in the electronic memory of their telephones/PDA;
- c. Drug traffickers often communicate with their illegal drug source(s) of supply, customers, or criminal associates by text messaging and/or e-mail from their cellular telephones/personal digital assistants. Accordingly pertinent text and/or email messages are often stored in the electronic memory of the cellular telephone/PDA; and
- d. Drug traffickers must maintain and have quick access to large amounts of United States currency or other liquid assets in order to maintain and finance their ongoing drug business. As such they often store bank account information, drug ledgers, or list where assets are stored in the electronic memory of the cellular telephone/PDA.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

5. The property to be searched is a white Apple iPhone, Model A1387, FCC ID: BCG-E2430A, IC: 579C-E2430A, contained in a Marilyn Monroe iPhone case, hereinafter referred to as the "Device." The Device is currently located at 2660 Fritts Crossing SE, Albuquerque, NM 87106.

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. Agents from the DEA Albuquerque District Office have been investigating the David REYNOLDS DTO since approximately June 2012. Based on surveillance, on June 12, 2013, Agents identified Daniel JIRON as a member of the REYNOLDS DTO. On June 25, 2013, Agents established surveillance at JIRON's residence of 627 82nd Street SW, Albuquerque, NM in relation to intercepted phone calls over (505) 270-8336 (REYNOLDS PHONE 6). During these intercepted phone calls, REYNOLDS arranged to meet Humberto "Butch" HERNANDEZ at JIRON's residence in order for REYNOLDS to provide illegal proceeds to HERNANDEZ for illegal drugs. Surveillance did, in fact, observe REYNOLDS meet with HERNANDEZ on the night of June 25, 2013 at JIRON's residence.

8. Prior to identifying JIRON on June 12, 2013, based on the telephone number belonging to JIRON and voice comparison, Agents intercepted phone calls between REYNOLDS and JIRON over REYNOLDS PHONE 6. On May 31, 2013, where JIRON agreed to provide ten ounces of illegal drugs to REYNOLDS to give to Robert HERRERA, who is

another member of the REYNOLDS DTO. At approximately 12:55 p.m., agents intercepted a phone call where REYNOLDS told JIRON that HERRERA was asking with for an "estimate" (time frame on receiving illegal drugs) and JIRON advised REYNOLDS that "they" (illegal drugs) had been ready since "6:00 a.m." REYNOLDS told JIRON that he would stop by "in a minute." After this conversation, at approximately 1:44 p.m., REYNOLDS and HERRERA agreed to meet at HERRERA'S house located at 1505 Secret Valley Dr. SW, Albuquerque, NM in order to drop off the ten ounces of illegal drugs. At approximately 1:55 p.m., Agents did, in fact, observe REYNOLDS arrive at HERRERA's house. Therefore, I believe, between 12:55 p.m., and 1:55 p.m., JIRON provided ten ounces of illegal drugs to REYNOLDS in order for REYNOLDS to give them to HERRERA.

9. Based on the surveillance operations described above and the intercepted phone calls, I believe JIRON was a highly trusted member of the REYNOLDS DTO and assisted in the distribution of illegal drugs.

10. On December 4, 2013, a Federal Grand Jury returned an indictment charging Daniel JIRON, *inter alia*, with a violation of Title 21 United States Code Section 846 Conspiracy to Distribute 1000 grams or more of heroin. On December 12, 2013, Agents from the United States Marshals Service (USMS) executed the Federal Arrest Warrant for JIRON at 3001 University Boulevard SE, Albuquerque, NM. USMS took custody of JIRON and transported JIRON to the DEA Albuquerque District Office (ADO) for processing.

11. During the execution of the arrest by the USMS, Agents conducted a search of JIRON's person and located the Device. The DEA then took custody of the Device and secured it as evidence at the DEA Albuquerque District Office.

12. The Device is currently in the lawful possession of the DEA. The Device came into the DEA's possession during the execution of the arrest warrant as described above.

13. Based on the above mentioned details, the Device is believed to contain information relating to the drug transactions described above and of other drug transactions in which JIRON has been involved. This information could include, but is not limited to:

- a. lists of customers and related identifying information;
- b. types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;
- c. any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information);
- d. any information recording JIRON'S schedule or travel from January 1, 2013 through the date of the execution of the warrant;
- e. any text messages and voicemails; and
- f. all bank records, checks, credit card bills, account information, and other financial records.

14. The Device is currently in storage at 2660 Fritts Crossing SE, Albuquerque, NM 87106. 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 DEA.

TECHNICAL TERMS

15. 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. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 “wi-fi” networks, or otherwise. Tablets typically 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 e-mail, and participating in Internet social networks.

- g. Pager: A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a

telecommunications network. Some pagers enable the user to send, as well as receive, text messages.

- h. **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 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.
- i. **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.

16. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a wireless telephone to include text message and voicemail, digital camera, portable media player, GPS navigation device, access to the internet and PDA. In my training and experience, examining data stored on the device of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

17. 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.

18. There is probable cause to believe that things that were once stored on the Device may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

19. *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). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the

storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

- 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.
- f. I know that when an individual uses an electronic device to obtain unauthorized access to a victim electronic device over the Internet, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

20. *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.

21. *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 premise. 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

22. 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,



Julie A. Olmsted
Special Agent
Drug Enforcement Administration

Subscribed and sworn to before me
on December 30, 2013:



KAREN B. MOLZEN
CHIEF UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched is a white Apple iPhone, Model A1387, FCC ID: BCG-E2430A, IC: 579C-E2430A, contained in a Marilyn Monroe iPhone case, hereinafter referred to as the "Device." The Device is currently located at 2660 Fritts Crossing SE, Albuquerque, NM 87106.

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

Mon

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of Title 21 U.S.C. Sections 841 and 846 involving Daniel JIRON, including:
 - a. lists of customers and related identifying information;
 - b. types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;
 - c. any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information);
 - d. any information recording Daniel JIRON'S schedule or travel;
 - e. any text messages and voicemails
 - f. 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;

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 computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

KBM

FILED

UNITED STATES DISTRICT COURT
ALBUQUERQUE, NEW MEXICO

pw FEB 05 2014

IN THE UNITED STATES DISTRICT COURT
FOR DISTRICT OF NEW MEXICO

MATTHEW J. DYKMAN
CLERK

IN RE ORDER REQUIRING APPLE, INC.
TO ASSIST IN THE EXECUTION OF A
SEARCH WARRANT FOR AN APPLE I-
PHONE, SERIAL NUMBER
C8PHGFQ1DTFC, MODEL A1387, FCC ID:
BCG-E2430A, IC: 579C-E2430A, ISSUED
BY THIS COURT

Case No. 13mr1026

APPLICATION

Filed Under Seal

INTRODUCTION

The United States of America, by and through Steven C. Yarbrough, Acting United States Attorney, and Joel Meyers, 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 Drug Enforcement Administration (DEA) currently has in its possession an iOS device that is the subject of a search warrant issued by this Court. 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 Serial Number C8PHGFQ1DTFC, Model #A1387, FCC ID# BCG-E2430A and IC: 579C-E2430A.

Apple, the creator of the iOS operating system and producer of the iOS device, may have the capability retrieving data stored on the iOS device that is not currently accessible to the DEA

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.

On December 30, 2013, Chief U.S. Magistrate Judge Karen B. Molzen issued a Court Order for Apple to unlock the iPhone listed above. Apple was unable to execute the order due to the Serial Number for the iPhone being unknown at the time of the signing of the Court Order. The Serial Number for the iPhone is C8PHGFQ1DTFC and is now included in the attached Court Order to Apple.

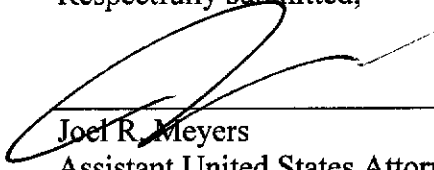
DISCUSSION

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,



Joel R. Meyers
Assistant United States Attorney

Date: January 29, 2014

FILED
UNITED STATES DISTRICT COURT
ALBUQUERQUE, NEW MEXICO

FEB 05 2014

IN THE UNITED STATES DISTRICT COURT
FOR DISTRICT OF NEW MEXICO

MATTHEW J. DYKMAN
CLERK

IN RE ORDER REQUIRING APPLE, INC.
TO ASSIST IN THE EXECUTION OF A
SEARCH WARRANT FOR AN APPLE I-
PHONE, SERIAL NUMBER
C8PHGFQ1DTFC, MODEL A1387, FCC ID:
BCG-E2430A, IC: 579C-E2430A, ISSUED
BY THIS COURT

Case No. 13mr 1026a

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 Serial Number C8PHGFQ1DTFC, Model #A1387, FCC ID# BCG-E2430A and IC: 579C-E2430A (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,

Robert H. Scott

Robert Hayes Scott
Chief U.S. Magistrate Judge

Date: 1-31-14