

JUN 11 2015

UNITED STATES DISTRICT COURT

CLERK, U.S. DISTRICT COURT EASTERN DISTRICT OF CALIFORNIA

for the

BY DEPUTY CLERK

Eastern District of California

In the Matter of the Search of )
White and Gold Apple iPhone 6 Plus, )
CURRENTLY LOCATED AT 7000 Michael )
N. Canalis Blvd., French Camp, CA 95231 )

Case No. 2:15-SW-0333- EFB

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):

- [x] 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:

Table with 2 columns: Code Section, Offense Description. Row 1: 18 U.S.C. § 2252(a)(1),(a)(2), and (a)(4)(B); Activities Relating to Material Involving the Sexual Exploitation of Minors

The application is based on these facts:

SEE AFFIDAVIT, attached hereto and incorporated by reference.

- [] Continued on the attached sheet.
[] Delayed notice 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.

Greg Wenning (Signature)

Greg Wenning, Special Agent, FBI (Printed name and title)

Sworn to before me and signed in my presence.

Date: 6-11-2015

Edmund F. Brennan (Signature)

Edmund F. Brennan, U.S. Magistrate Judge (Printed name and title)

City and state: Sacramento, California

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF CALIFORNIA

IN THE MATTER OF THE SEARCH OF A  
**White and Gold Apple iPhone 6 Plus**  
CURRENTLY LOCATED at 7000 Michael N.  
Canalis Blvd., French Camp, CA 95231

Case No. \_\_\_\_\_

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

I, **Greg Wenning**, 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. I am a Special Agent with the Federal Bureau of Investigation (FBI), and have been since February 2013. I received over twenty weeks of training at the FBI Academy, at Quantico, Virginia, in various investigative techniques and legal matters, including the topics of Fourth Amendment searches, criminal complaints, and computer and criminal investigations. I have also received additional training regarding Peer-to-Peer programs used to trade child pornography. Prior to becoming a special agent I was employed by the FBI in Denver, Colorado as a Staff Operations Specialist, conducting research for securities fraud and mortgage fraud cases. As part of my daily duties as a special agent, I have conducted numerous investigations and written multiple search warrants regarding criminal violations relating to sexual exploitation of minors and child pornography, including violations pertaining to the illegal production, distribution, receipt and possession of child pornography, in violation of 18 U.S.C. §§ 2252A, 2252. I have received training and, as part of my duties, I have observed and reviewed examples

of child pornography and visual depictions of minors engaged in sexually explicit conduct (as defined in 18 U.S.C. § 2256) in all forms of media, including digital media. In conjunction with the FBI's Computer Analysis Response Team (CART) I have used forensic software to review electronic and digital evidence including Cell phones, computers and tablets and subsequently used that information in criminal complaints and grand jury testimony.

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. I know that on February 12, 2015, a search warrant for the content of email account Kimprudhomme1994@yahoo.com was issued by this court under 2:15-SW-0017 KJN. The information received pursuant to that warrant is outlined in further detail below. Several subpoenas were also issued to Yahoo!, Comcast and AT&T for information related to the above email account and the Internet Protocol ("IP") address used to access the account.

5. I know that on May 21, 2015, a search warrant was issued under 2:15-SW-0262 DAD to search the premises at 13390 Brookwood Way, Lathrop CA 95330. That warrant was executed on May 28, 2015. The information received pursuant to that warrant is outlined in further detail below in paragraphs 56 to 61.

6. I know that on May 28, 2015 a search warrant was issued by this court to search the premises at 651 E. Watters Rd., French Camp, CA. That warrant was executed on May 28, 2015. The information received pursuant to that warrant is outlined in further detail below in paragraph 66.

#### **IDENTIFICATION OF THE DEVICE TO BE EXAMINED**

7. The property to be searched is a white and gold iPhone 6 Plus on the New Cingular Wireless PCS/AT&T network with access number (phone number) 650-630-6280, Model number A1522, IMEI 354386063360379 and FCC ID# BCG-E2817A IC: 579C-E2817A (hereinafter referred to as the "DEVICE"). The DEVICE is currently stored in an evidence locker at the San Joaquin County Sheriff, located at 7000 Michael N. Canalis Blvd., French Camp, CA 95231, under case number 15-0012718, item 1.

8. 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**

**Website A**

9. Since at least July of 2012, the Federal Bureau of Investigation's Major Case Coordination Unit, in conjunction with an international law enforcement agency, has been investigating an online website used extensively by persons interested in exchanging images depicting child pornography ("CP"). Through the website, people can meet and become trading partners. This website is referred to as "Website A" in this affidavit since it is still under investigation and many website users have been the subject of search warrants. Because other users may also become suspects, law enforcement would like to identify as many suspects as possible before the nature and details of the investigation become public.

10. Below is a description of how Website A operated since at least in or about June 2012. Website A is a photo (still image) sharing website, hosted outside of the United States. Membership to Website A is free and includes unlimited hosting storage and free photo sharing of digital images (not videos). Website A is organized by different forums according to topic. Examples include topic-based forums such as "architecture," "travel," "family," and "autos." Each Website A Forum contains albums posted and named by the registered Website A user that created the album.

11. To register an account, and thus become a "member" of Website A, a user must create a username and provide a valid email address in order to receive a password provided by Website A. Upon receiving this password, the user is prompted to create a new password which can be used to log in to Website A. Once this is done, the user, as a member, may create albums and post images within these albums.

12. A user's albums are listed under his/her username. A member can create one or more photo albums and has the choice to make an album available to all individuals on the Web (i.e., a "public album"), or to make it a password protected album, accessible only to individuals

who know or have the password. When a member creates an album he or she may choose to have his or her contact email address displayed under his or her username (which appears at the top of the album) to others visiting the albums, or instead ask others to “contact via comments.” Even in instances where a member does not post his email address so other members can see it, it is not uncommon for the member to post the address in the comment section as a means of contact or when responding to a specific request from another member.

13. An album consists of all of the pictures associated with that album, along with any posted comments. When a member creates an album he or she has a choice via a scroll-down menu to allow: (1) only Website A members who have created albums on Website A to add a comment, (2) only Website A members to comment (regardless of whether these members have created their own albums on Website A), (3) anyone accessing Website A (whether or not they are a Website A member) to anonymously comment on the album, or (4) to disable the comment feature.

14. Anytime an individual posts a comment to an album, the owner of that album is automatically notified by Website A via the email address he provided as his contact email address. The email message states that a comment was made, and includes the file name of the image commented on, the comment itself, the Website A user name of the person making the comment (if the person posting the comment is a Website A member) and a hyperlinked URL to the image with the corresponding comment. The member /owner of an album cannot directly opt out of receiving these email notifications. However, if he or she were to go back into his or her membership profile and delete the email address provided to Website A as his or her contact information, he or she will not receive these automated email notifications.

15. Any individual on the Internet can view and post comments to non-password protected albums (“public albums”) on Website A and download the images in those albums. Only members can create albums and upload pictures to albums. When a Website A member posts a comment to an album that member’s username, a country flag corresponding to the originating IP address, and the date and time of the comment are displayed next to the comment. When a comment is posted by a non-member of Website A, portions of the originating IP address and a country flag corresponding to that IP address are displayed next to that comment.

Regardless of whether the individual posting a comment is a member or non-member, Website A logs the full originating IP address of the individual posting the comment.

16. Website A has become a popular means for individuals to trade CP images, in particular through the “nudity” and “kids” forums. Examples of the names of albums within these two forums are “13 yo boy pics,” “street boys,” “Cute little brunette,” “Baby and Toddler Boys,” and “Maria cute chubby 16 yo (nude) (password protected).” Some Website A albums associated with some of the subjects of law enforcement operations are known to contain CP. In these cases, the CP is most likely to be in a password-protected album, rather than in a public album.

17. While most of the images law enforcement has seen posted in public albums may not constitute CP, often evidence from the images, and comments posted about the album (either by other individuals or the member who created the album), indicates that the particular poster or person who created the album has a sexual interest in children, and that these individuals’ interest in Website A lies in the ability to meet other individuals for the private trading of CP.

18. A common scenario is for such a user to post child erotica or preview pictures of children, accompanied by a sexually suggestive title or comment, in a public album as a way to entice or attract other individuals with a sexual interest in children. It appears the poster’s purpose is often to solicit comments on the pictures posted from like-minded individuals. Once these individuals meet on Website A, they then agree to trade Website A passwords, or trade their private CP collections elsewhere, often by email, rather than risking trading CP on Website A itself.

19. Individuals on the Internet, including Website A users, may regularly monitor public albums on Website A and post provocative comments or images in specific albums related to children with the hope of obtaining the password to other password protected albums or information on individuals that are willing to trade CP.

20. I am aware that the High Technology Investigative Unit, located within the U.S. Department of Justice’s Child Exploitation and Obscenity Section, has been involved in the investigation of more than two dozen Website A users who either posted sexually explicit images

of children to Website A or distributed sexually explicit images of children to another user to obtain their password. In more than half of these cases, investigation revealed that these individuals were actively molesting children and, in some instances, posting images of that abuse to Website A.

21. As one example, United States Immigration and Customs Enforcement investigators in Stockton, California received information that J.M., a resident of Turlock, California, had used the site in the middle of 2012 to set up multiple user accounts, several of which were terminated for violations of terms of service. J.M., using various accounts, posted comments about photos that indicated his/her interest in exchanging images of child pornography. J.M. was a registered sex offender due, in part, to a prior conviction he/she suffered in federal court in Fresno for possession of child pornography in approximately 2000. J.M. also had various state law violations for sexual offenses involving minors. A federal search warrant was issued on December 12, 2013 and, when it was executed on December 19, 2013, investigators seized a large quantity of child pornography at J.M.'s residence. J.M. has since been charged with receipt/distribution of child pornography in a second federal case in Fresno, California.

22. In approximately August of 2013, the United States Department of Homeland Security, Homeland Security Investigations ("HSI") obtained a certain portion of Website A data, including information related to Website A usernames, album names, album passwords, user comments, and associated email addresses and IP logs associated with specific albums.

23. On January 16, 2015, HSI provided me with information from Website A regarding Kimprudhomme1994@yahoo.com (hereinafter referred to as the "Subject Account"). I reviewed the information from Website A, and determined that there were multiple Website A accounts associated with the Subject Account. On Website A, the Subject Account was associated with IP address 99.43.117.34.

24. The Subject Account was associated with user accounts of moth3rsdesire, mommylikesitto, daddysdribble, and kissmykitty. The Subject Account was also associated

with email accounts [mommylikesittoo@hotmail.com](mailto:mommylikesittoo@hotmail.com), [daddys0h0rny@yahoo.com](mailto:daddys0h0rny@yahoo.com), and [daddysdribble@yahoo.com](mailto:daddysdribble@yahoo.com).

25. The Website A account with username daddysdribble was locked by Website A for distribution of child pornography.

26. On Website A, the user account moth3rsdesire, with email account [mommylikesittoo@hotmail.com](mailto:mommylikesittoo@hotmail.com), posted three albums with the tags of “ass, butt, cock, cousin, cum, daddy, incest, les lick, mom, mommy, penetration, pussy, sister, teen, tits young, web.” This profile had the following under the “User Info” section: “Horny mother looking for people who share the same interest in young beauty. I can never get enough of smelling the roses tasting the peaches or savoring the nectar of any ripe fruit! I love to trade and chat but trading is what I’m looking for. Send what you would like to have and we can start from there.”

27. On January 21, 2015, I sent a request to the National Center for Missing and Exploited Children (“NCMEC”) to search the above usernames and email accounts in their database. On the same date, NCMEC provided me with a report showing that Detective Kuchenreuther of the Minnehaha County Sheriff’s Department queried the username Mommylikesittoo with NCEMC.

28. On January 26, 2015, I spoke with Detective Kuchenreuther, who advised that he conducted an investigation into an individual who was trading child pornography and using the Website A user name YoungisBetter12. While Detective Kuchenreuther was reviewing returns from a search warrant regarding email accounts associated with his subject, he located emails on March 28, 2012 and March 29, 2012, between his subject and [mommylikesittoo@hotmail.com](mailto:mommylikesittoo@hotmail.com), which contained twelve images of nude children.

### **FBI Search Warrant**

29. On July 29, 2013, FBI Special Agent Bianca Pearson received a search warrant return from YAHOO, INC. for information related to e-mail account [Johlove28@yahoo.com](mailto:Johlove28@yahoo.com). SA Pearson located an email sent on June 26, 2013, from [8568@hotmail.co.za](mailto:8568@hotmail.co.za) to the Subject



Account. This email contained 46 images of child pornography and four images of child erotica as attachments. All of these images were from a series titled Tori\_9yo.

30. On June 26, 2013, the Subject Account replied to [8568@hotmail.co.za](mailto:8568@hotmail.co.za), with the following text:

*"I'm sorry if I wasn't clear.... I enjoy cock and the girls and boys that suck them. I like to see men get blowjobs and blow their loads. I truly enjoy penetration and can never get enough of watching these daddies/uncles and brothers received pleasure. If you have anything like this please send to me so we can correspond. Girls or boys"*

31. I received a copy of the above email and the attached images. I reviewed the images contained in the above email received by the Subject Account and determined that the following images meet the definition of child pornography under 18 U.S.C. § 2256:

- Email Attachment Tori\_9yo\_(30) – Photo depicts genital oral sex between an adult male whose penis is touching the lips of a minor female who is topless with her chest area exposed and visible to the camera
- Email Attachment Tori\_9yo\_(39) – Photo depicts lascivious display of genitals by a nude minor female who is posing for a photo, on her back with her legs spread and vagina exposed
- Email Attachment Tori\_9yo\_(43) – Photo depicts lascivious display of genitals by a nude minor female who is posing for a photo, on her back with her legs spread and vagina exposed
- Email Attachment Tori\_9yo\_(47) – Photo depicts lascivious display of genitals by a nude minor female who is posing for a photo, kneeling on a bed looking toward the camera over her shoulder with her vagina exposed
- Email Attachment Tori\_9yo\_(49) – Photo depicts lascivious display of genitals by a nude minor female who is posing for a photo, kneeling on a bed looking toward the camera through her legs with her vagina exposed

## Subpoena Returns

32. On September 12, 2014, pursuant to a subpoena, Yahoo provided the following subscriber information and IP logs for kimprudhomme1994@yahoo.com:

Registration IP address:	99.43.117.34
Account Created:	December 27, 2012, 21:49:11 GMT
Full Name:	Kim Prudhomme
Account status:	Active

33. Yahoo! showed that kimprudhomme1994@yahoo.com was accessed 83 times from IP address 99.43.117.34, between December 28, 2012 and June 24, 2014 and only three times from a different IP address during this time frame.

34. On September 13, 2014, AT&T Internet Services provided the following subscriber and billing information for IP address 99.43.117.34 from October 17, 2011 through September 13, 2014:

IP:	99.43.117.34
Name:	Jennifer Johnson
Service/Billing:	13390 Brookwood Way, Lathrop, CA 95330
Account Status:	Active
Preferred E-mail:	<u>jennifer7780@hotmail.com</u>
Member ID:	<u>dantejen@att.net</u>
Phones:	209-740-1337; 209-475-8062
Established:	June 17, 2011
Type:	U-Verse only

35. On January 15, 2015, Yahoo! provided updated subscriber information and IP logs for kimprudhomme1994@yahoo.com. Subscriber information remained the same as above and the account was active as of January 15, 2015. IP logs showed the account was again accessed from IP 99.43.117.34 on October 18, 2014.

36. On April 10, 2015, AT&T Internet Services provided updated subscriber and billing information for IP address 99.43.117.34 from October 10, 2012 through February 27, 2015. Subscriber information remained the same as above with the addition of phone number 209-565-5835 to the account.

37. AT&T Internet Services U-Verse internet accounts do not have traditional session records with a standard log on/log off format. U-Verse customers have a unique IP directly provisioned to the account. This means that the IP address assigned to U-Verse internet accounts is static and the above IP was assigned to this user from October 10, 2012 through February 27, 2015.

**FBI Sacramento Search Warrant on Subject Account - kimprudhomme1994@yahoo.com**

38. On January 29, 2015, a federal search warrant was issued under case number 2:15-SW-0017 KJN, in the Eastern District of California, by Honorable Kendall J. Newman, United States Magistrate Judge, for contents of the email account kimprudhomme1994@yahoo.com.

39. On February 26, 2015, Yahoo! provided a DVD with the complete contents of the email account kimprudhomme1994@yahoo.com, including IP logs, emails, and email attachments.

40. I reviewed the emails in the inbox and sent folders of the account and located approximately 140 emails sent or received between January, 2013 and December, 2014 with attachments containing child pornography. Many of these emails contained multiple attachments with pictures and videos depicting child pornography. The following are an example of emails which contained child pornography:

41. On June 24, 2014, an email was sent from kimprudhomme1994@yahoo.com to yantre57@gmail.com, with the subject line "This", with an attached file named "20100629". I viewed this video which is approximately one minute and ten seconds long and depicts a female child approximately 10 years old involved in oral genital sex with an adult male.

42. On June 24, 2014, an email was sent from kimprudhomme1994@yahoo.com to yantre57@gmail.com, with the subject line "Yes", with an attached file named "(pthc\_frifam\_lolitifuck)\_8o\_sucks\_cock\_and\_gets\_a\_facial\_-\_New\_2012.avi". I viewed this video which is approximately two minutes and ten seconds long and depicts a female child approximately 12 years old involved in oral genital sex with an adult male.

43. On June 24, 2014, an email was sent from kimprudhomme1994@yahoo.com to yantre57@gmail.com, with the subject line “I want to marry this guy”, with an attached file named “3yo Sleep Fuck.wmv”. I viewed this video which is approximately fourteen seconds long and depicts an adult male involved in genital genital sex with a female child approximately 5 years old, who appears to be sleeping face down on a bed.

44. On June 18, 2014, an email was sent from kimprudhomme1994@yahoo.com to sdee2537@gmail.com, with the subject line “Bad daddy”, with an attached file named “1-1 (BEC-ALD 5yo Nice Penetration by Man-Dad).wmv”. I viewed this video which is approximately twenty six seconds long and depicts an adult male involved in genital genital sex with a pre-pubescent female child, who is laying on her back on a bed.

45. In the email folders for kimprudhomme1994@yahoo.com, I also located the email described in paragraph 25, sent on 06/26/2013 from 8568@hotmail.co.za, which contained the email attachments starting with the name “Tori\_9yo\_”, which depicted a nude minor female engaged in sexual acts and posed in a sexual manner.

46. Yahoo! logs showed that Kimprudhomme1994@yahoo.com was accessed from IP 99.43.117.34 four times in 2015, most recently on January 27, 2015. On this date, the IP was serviced by AT&T, with a subscriber of Jennifer Johnson at 13390 Brookwood Way, Lathrop, CA 95330. As of February 27, 2015, AT&T records showed active service for this IP at 13390 Brookwood Way, Lathrop CA 95330.

47. Kimprudhomme1994@yahoo.com also sent three emails to DanteSJohnson@yahoo.com as follows:

48. January 28, 2015, at 2:44 PM, with the subject line “Kimmy P” and no content.

49. January 28, 2015, at 2:53 PM, with the subject line “Hi”, and an attached file named “IMG\_0976.mov”. This video is approximately 11 seconds long and depicts a white adult female masturbating.

50. January 28, 2015, at 4:52 PM, with the subject line "Help" and an attached file named "IMG\_0976.mov". This video is approximately 17 seconds long and depicts a white adult female masturbating.

51. On April 23, 2015, I conducted searches of open source Law Enforcement databases and California Department of Motor Vehicles and located records for an individual named Dante S. Johnson residing at 13390 Brookwood Way, Lathrop CA 95330 along with Jennifer Johnson, the subscriber to the AT&T IP address used to access [kimprudhomme1994@yahoo.com](mailto:kimprudhomme1994@yahoo.com). These databases also show that Dante and Jennifer share a P.O. Box in Manteca, CA.

52. The open source Law Enforcement database record for Dante S. Johnson indicates that he is associated with email account [dantesjohnson@yahoo.com](mailto:dantesjohnson@yahoo.com).

53. [Kimprudhomme1994@yahoo.com](mailto:Kimprudhomme1994@yahoo.com) was accessed from IP 67.181.111.155 two times on January 28, 2015. On March 2, 2015 Comcast provided information regarding this IP address. The IP address was assigned to Lisa Irons at 651 E. Watters Rd., French Camp, CA on the date and time it was used to access the email account.

54. On April 23, 2015, I travelled to 13390 Brookwood Way, Lathrop CA 95330 and observed a sign with the words "The Johnsons", hanging over the front door. I also observed a vehicle parked in the driveway bearing California License plate 6HSN883, registered to Jennifer Johnson at 13390 Brookwood Way, Lathrop CA 95330.

55. As of April 24, 2015, the United States Postal Service advised that Jennifer Johnson and another individual with the last name of Johnson were currently receiving mail at 13390 Brookwood Way, Lathrop CA 95330.

#### **FBI Search of 13390 Brookwood Way**

56. On May 28, 2015, investigators searched 13390 Brookwood Way pursuant to search warrant 2:15-SW-0262 DAD, which was issued on May 21, 2015 in the Eastern District of California. During the search, investigators spoke with Jennifer Johnson. They learned that Dante S. Johnson and Jennifer Johnson were divorced in 2005, but reconciled in approximately

2007 and continued to live together until December of 2014. Dante stayed at 13390 Brookwood on December 25, 2014, when [Kimprudhomme1994@yahoo.com](mailto:Kimprudhomme1994@yahoo.com) was accessed from the AT&T IP assigned to this residence. Jennifer Johnson told investigators that Dante Johnson still has a key and access to the residence at 13390 Brookwood Way, but he has been staying with his girlfriend, Lisa Irons, at her house. Jennifer indicated that Dante does come and go from 13390 Brookwood Way from time to time, but it had been a couple of weeks since he was there last. Jennifer Johnson denied possessing or trafficking in child pornography and an on-site forensic computer review by the FBI Computer Analysis Response Team did not locate any child or adult pornography on computer devices owned by Jennifer. Jennifer has no known criminal history and currently works in accounting for the City of Stockton. She indicated that Dante Johnson has pretended to be a woman online in the past. She also indicated that she was nervous about talking with law enforcement about Dante Johnson because there have been domestic violence issues between them in the past. Prior to investigators completing the search warrant at approximately 11:00 a.m., Dante attempted to call Jennifer several times and text messaged her stating he heard the police were at 13390 Brookwood Way, and asking if she was okay.

57. Investigators found approximately 300 pills which field tested positive for the presence of ecstasy in the nightstand in the master bedroom. Investigators also found an empty gun box for a Glock handgun under the bed in the master bedroom. Inside the gun box were two test fired shell casings and a paper with the serial number TLY952, which is a Glock 23 .40 caliber hand gun, reported as stolen in 2013. Investigators also found two partially-full boxes of handgun ammunition (.40 caliber and .380 caliber) in the master bedroom closet.

58. Jennifer Johnson said she had not seen Dante Johnson in possession of a firearm in the past. However, he recently called her and told her that he had been mugged and had determined who mugged him. He asked her to confirm that the ammunition was still in the master bedroom closet, which she did. Jennifer did not have any knowledge of the Glock gun box located under the master bed.

59. Jennifer and her father Dean also told investigators that Dante currently worked for B&G Trucking.

60. On May 28, 2015, Bobby Walker of B&G Trucking told investigators that Dante Johnson was driving a red Kenworth tractor-trailer (number 36, license plate 9E91419), which belongs to B&G Trucking. Walker contacted Dante Johnson on phone number 630-650-6280 and Dante told Walker he would return to B&G in the early afternoon that day.

61. According to law enforcement records, it appears Dante Johnson suffered a felony conviction for manslaughter in approximately 2001.

**651 E. Watters Rd., French Camp, CA**

62. On May 28, 2015, at approximately 1:30 p.m., investigators saw the Red Kenworth tractor-trailer truck parked in the vicinity of 651 East Watters Rd. and went to the residence to see if Lisa Irons or Dante Johnson were home and would speak with them. They encountered both Lisa Irons and Dante Johnson at the premises. Johnson was arrested on state charges after being called out of the house by Lisa Irons who was also arrested on state charges. While conducting a security sweep of the house, investigators observed a laptop computer in plain view in one of the bedrooms.

63. Dante Johnson spoke to investigators after being given a Miranda warning. He said the following: (1) he has never accessed Kimprudhomme1994@yahoo.com; (2) Kim Prudhomme is a 21-year-old, African-American female who he had sex with at both 13390 Brookwood Way and the 651 E Watters; (3) Prudhomme may have accessed Kimprudhomme1994@yahoo.com from those locations while they were there together; (4) he does not have her phone number or any way of contacting her, but used to be friends with her on facebook; (5) Prudhomme may be a prostitute in the Stockton area, but he did not pay to have sex with her; (6) he purchased the ammunition and gun box found at 13390 Brookwood Way, as well as a gun lock, however he denied purchasing a gun; and (7) he suffered a felony conviction for manslaughter in 1998.

64. Dante Johnson had an Apple iPhone 6 Plus on his person at the time of his arrest, which he unlocked with a pin code that he would not provide to investigators. Dante provided the phone number as 630-650-6280 and verbally agreed to allow Law Enforcement to search the phone in his presence. An initial visual inspection of the DEVICE revealed no child

GW  
MB  
pornography, but did confirm that he used email account DanteSjohson@yahoo.com and investigators located one email in his inbox from Kimprudhomme1994@yahoo.com. Dante told investigators that Kim Prudhomme sent him the email, which depicted her friend. This appeared to be one of the emails from paragraph <sup>49</sup> 46 or <sup>50</sup> 47 above. Dante also told investigators that he used his iPhone to access the wireless internet connection at 651 E. Watters. After being given a Miranda warning, Lisa Irons also told investigators that Dante Johnson used his iPhone to access the wireless internet connection at 651 E. Watters and that she did not use or have any knowledge of email account Kimprudhomme1994@yahoo.com. Irons also told investigators that Dante connected and backed up his iPhone to a computer at 13390 Brookwood Way.

65. As mentioned above, Kimprudhomme1994@yahoo.com was accessed from Comcast IP 67.181.111.155 twice on January 28, 2015. That IP address was assigned to "Lisa Irons" at the 651 E. Watters Rd., French Camp, CA on the date and time it was used to access the email account.

#### **FBI Search of 651 E. Watters**

66. On May 28, 2015, investigators searched 651 E. Watters Rd., French Camp, CA, pursuant to a search warrant signed by Hon. Dale Drozd, which was issued on May 28, 2015 in the Eastern District of California. During the search, investigators located a Bersa .380 caliber pistol and the magazine for the pistol which was loaded with nine rounds of .380 caliber rounds stamped "380 Auto RP". The gun and ammo were found on the top shelf in the master bedroom closet. This is the same caliber ammo that was found at 13390 Brookwood, which Dante Johnson admitted to purchasing. Investigators also located and seized approximately 1,000 pills that appeared to be MDMA or ecstasy and \$6,660 in cash. In a recorded statement, Irons denied having any knowledge of the gun or pills and said they must belong to Dante.

#### **Information Regarding Sade Prudhomme**

67. On May 29, 2015 I conducted open source records checks and was unable to locate an individual by the name of Kim Prudhomme in California, matching the description provided by Dante. I contacted an investigator at the Stockton Police Department who conducted a records check but did not locate any contact with a Kim Prudhomme. The



investigator did locate an individual by the name of Sade Prudhomme, born in 1992, who had been arrested for prostitution. I obtained the California DMV record for this individual and subsequently located a facebook profile for a Sade Prudhomme who appears to be the same individual. The facebook profile for Sade Prudhomme shows that she is friends with Dante Johnson and she moved to Las Vegas, NV on November 30, 2014.

### **Interview of Jennifer Johnson**

68. On June 9, 2015, I spoke with Jennifer Johnson, who said that Dante Johnson purchased his iPhone 6 Plus, phone number 650-630-6280, in approximately November 2014. Dante used his iPhone to access the wireless internet connection at her house at 13390 Brookwood Way. Jennifer does not know anyone with the name of Sade or Kim Prudhomme. Jennifer did not believe that anyone came to 13390 Brookwood Way with Dante on December 25, 2014, one of the days the Subject Account was accessed from the IP address at this house.

### **The DEVICE**

69. Because the DEVICE was in the possession of Dante Johnson, who had access to the internet connection at both residences from where [Kimprudhomme1994@yahoo.com](mailto:Kimprudhomme1994@yahoo.com) was accessed, it is possible that the DEVICE was used to log into the email account. Additionally, Dante had several hours between when he became aware that investigators were at 13390 Brookwood and when he gave consent to search the DEVICE, during which time he could have deleted information associated with [Kimprudhomme1994@yahoo.com](mailto:Kimprudhomme1994@yahoo.com), which would have been discovered during the limited consensual search. Although investigators conducted a limited consensual search of the DEVICE in the presence of Dante Johnson, a complete forensic review of the DEVICE will be necessary to determine if it was used to access the email account and store, send or receive child pornography. The limited consensual search did not produce evidence of child pornography. The limited consensual search focused on his email account only; it did not include a review his photos, videos, or internet history.

70. The DEVICE is currently in the lawful possession of the San Joaquin County Sheriff. It came into the San Joaquin County Sheriff's possession on May 28, 2015, when Dante Johnson was arrested on local charges. The DEVICE was on his person and was seized incident

to his arrest. Therefore, while the San Joaquin County Sheriff 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.

71. The DEVICE is currently stored in an evidence locker at the San Joaquin County Sheriff, at 7000 Michael N. Canalis Blvd., French Camp, CA 95231. 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 San Joaquin County Sheriff.

### **TECHNICAL TERMS**

72. 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. 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.
- 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.

73. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product technical specifications available online at <https://Apple.com> 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**

74. 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.

75. *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.

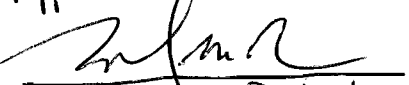
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored 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.

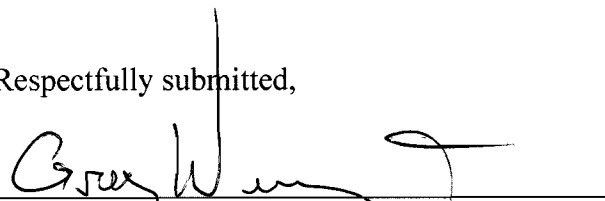
76. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the DEVICE consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted 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.

77. *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.

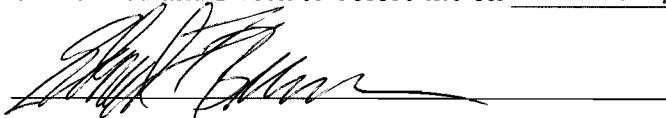
CONCLUSION

78. 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.

Approved as to Form:  
  
Michael M. Beckwith

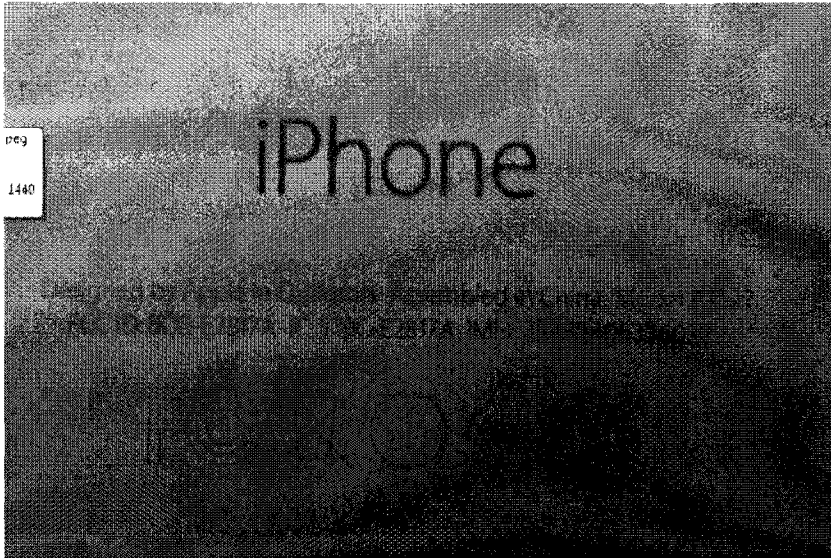
Respectfully submitted,  
  
GREG WENNING  
Special Agent  
Federal Bureau of Investigation

Subscribed and sworn to before me on 6-11-2015 :

  
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A**

The property to be searched is a white and gold iPhone 6 Plus on the New Cingular Wireless PCS/AT&T network with access number (phone number) 650-630-6280, Model number A1522, IMEI 354386063360379 and FCC ID# BCG-E2817A IC: 579C-E2817A (hereinafter referred to as the "DEVICE"). The DEVICE is currently stored in an evidence locker at the San Joaquin County Sheriff, located at 7000 Michael N. Canalis Blvd., French Camp, CA, under case 15-0012718, item 1.



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 and information relating to violations of 18 U.S.C. §§ 2252 (a)(1), (a)(2), and (a)(4)(B) – Activities Relating to Material Involving the Sexual Exploitation of Minors – occurring after June 17, 2011, including:

- a. emails and attachments associated with this account which are stored on the DEVICE
- b. images depicting child pornography stored on the DEVICE which may have been sent or received using the above email account;
- c. any other communications or records stored on the DEVICE which may show who created or used the email account

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;

3. Evidence of software that would allow others to control the DEVICE, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence

4. Records evidencing the use of the Internet Protocol address 99.43.117.34 and 67.181.111.155 to communicate with Yahoo! mail servers, including:

- a. records of Internet Protocol addresses used;
- b. records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

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.

IN THE UNITED STATES DISTRICT COURT  
FOR THE 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. \_\_\_\_\_

APPLICATION

Filed Under Seal

**INTRODUCTION**

The United States of America, by and through Ben 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 San Joaquin County Sheriff’s Office 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 by the FBI revealed that it is locked. Because the iOS device is locked, law enforcement agents are not able to forensically examine the data stored on the iOS device as commanded by the search warrant.

The iOS device is a white and gold iPhone 6 Plus on the New Cingular Wireless PCS/AT&T network with access number (phone number) 650-630-6280, Model number A1522, IMEI 354386063360379 and FCC ID# BCG-E2817A IC: 579C-E2817A.

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 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

Date: 6/10/15

UNITED STATES DISTRICT COURT

for the

Eastern District of California

In the Matter of the Search of )

White and Gold Apple iPhone 6 Plus, CURRENTLY )  
LOCATED AT 7000 Michael N. Canalis Blvd., )  
French Camp, CA 95231 )

Case No.

2:15 - SW 0333 + EFB

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 \_\_\_\_\_ (not to exceed 14 days)

[X] 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.

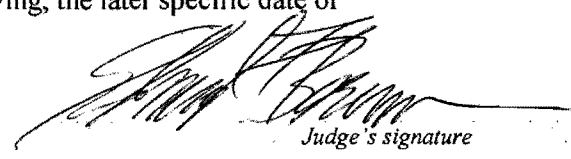
Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

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: 6-11-2015  
9:11:05 A.M.

  
Judge's signature

City and state: Sacramento, California

Edmund F. Brennan, U.S. Magistrate Judge  
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2) (modified)

**Return**

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

JUN 11 2015

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF CALIFORNIA

CLERK, U.S. DISTRICT COURT  
EASTERN DISTRICT OF CALIFORNIA

BY \_\_\_\_\_ DEPUTY CLERK

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

Case No. **2:15 - SW 0333** EFB

**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 white and gold iPhone 6 Plus on the New Cingular Wireless PCS/AT&T network with access number (phone number) 650-630-6280, Model number A1522, IMEI 354386063360379 and FCC ID# BCG-E2817A IC: 579C-E2817A (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.

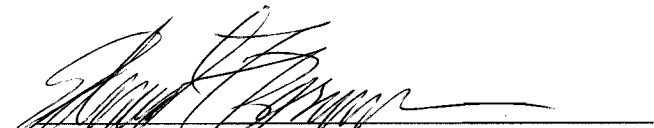
FURTHER ORDERED that, to the extent that data on the iOS Device is encrypted, Apple may provide a copy of the encrypted data to law enforcement, but Apple is not required to attempt to decrypt, or otherwise enable law enforcement’s attempts to access any encrypted data;

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,



EDMUND F. BRENNAN]

UNITED STATES MAGISTRATE JUDGE

Date:

6-11-2015