

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means

Original

Duplicate Original

UNITED STATES DISTRICT COURT

FILED
LODGED
ENTERED
RECEIVED

for the
Western District of Washington

FEB 04 2020

AT SEATTLE
CLERK U.S. DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
DEPUTY

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

)
)
)
)
)
)

Case No. MJ20-021

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

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

The Subject Account as described in Attachment A, which is attached hereto and incorporated herein by this 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, which is attached hereto and incorporated herein by this reference.

YOU ARE COMMANDED to execute this warrant on or before January 31, 2020 (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 U.S. Magistrate Judge (United States Magistrate Judge)

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: 01/17/2020 10:00 am


Judge's signature

City and state: Seattle, Washington

Brian A. Tsuchida, CHIEF U.S. MAGISTRATE JUDGE
Printed name and title

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means (Page 2)

Return

Case No.: MJ20-021	Date and time warrant executed: 1-28-20 0912	Copy of warrant and inventory left with: See below
-----------------------	---	---

Inventory made in the presence of: Alex Juhn

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

A zip folder containing data from iCloud account belonging to Jon LAKEY. Account slave524@icloud.com.



Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: 2-3-20

(MAT)

[Signature]
Executing officer's signature

Toby Ledgerwood Special Agent
Printed name and title

UNITED STATES DISTRICT COURT

for the
Western District of Washington

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

)
)
)
)

Case No. MJ20-021

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)*:

The Subject Account as further described in Attachment A, which is attached hereto and incorporated herein by this reference.

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

See Attachment B, incorporated herein 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:


<i>Code Section</i>	<i>Offense Description</i>
Title 18, U.S.C. § 2252 (a)(2)	Receipt or Distribution of Child Pornography
Title 18, U.S.C. § 2252(a)(4)(B)	Possession of Child Pornography

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.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: by reliable electronic means; or: telephonically recorded.



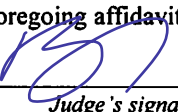
Applicant's signature

Toby G. Ledgerwood, Special Agent (HSI)

Printed name and title

- The foregoing affidavit was sworn to before me and signed in my presence, or
- The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 01/17/2020



Judge's signature

City and state: Seattle, Washington

Brian A. Tsuchida, Chief United States Magistrate Judge

Printed name and title

ATTACHMENT A

Description of Property to be Searched

This warrant applies to information associated with the Apple iCloud account/email: slave524@icloud.com (the “account”), that is stored at premises owned, maintained, controlled, or operated by Apple, Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.



1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

ATTACHMENT B
ITEMS TO BE SEIZED

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

1 c. The contents of all emails associated with the account, including stored or
2 preserved copies of emails sent to and from the account (including all draft emails and
3 deleted emails), the source and destination addresses associated with each email, the date
4 and time at which each email was sent, the size and length of each email, and the true and
5 accurate header information including the actual IP addresses of the sender and the
6 recipient of the emails, and all attachments;

7 d. The contents of all instant messages associated with the account from,
8 including stored or preserved copies of instant messages (including iMessages, SMS
9 messages, and MMS messages) sent to and from the account (including all draft and
10 deleted messages), the source and destination account or phone number associated with
11 each instant message, the date and time at which each instant message was sent, the size
12 and length of each instant message, the actual IP addresses of the sender and the recipient
13 of each instant message, and the media, if any, attached to each instant message;

14 e. The contents of all files and other records stored on iCloud, including all
15 iOS device backups, all Apple and third-party app data, all files and other records related
16 to iCloud Photo Library, Photo Stream, iCloud Drive, Safari Browsing History, and all
17 address books, contact and buddy lists, notes, reminders, calendar entries, images, videos,
18 voicemails, device settings, and bookmarks;

19 f. All activity, connection, and transactional logs for the account (with
20 associated IP addresses including source port numbers), including FaceTime call
21 invitation logs, messaging and query logs (including iMessage, SMS, and MMS
22 messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases,
23 downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs,
24 sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My
25 Friends logs, logs associated with web-based access of Apple services (including all
26 associated identifiers), and logs associated with iOS device purchase, activation, and
27 upgrades;

28

1 g. All records and information regarding locations where the account or
2 devices associated with the account were accessed, including all data stored in connection
3 with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

4 h. All records pertaining to the types of service used;

5 i. All records pertaining to communications between Apple and any person
6 regarding the account, including contacts with support services and records of actions
7 taken; and

8 j. All files, keys, or other information necessary to decrypt any data produced
9 in an encrypted form, when available to Apple (including, but not limited to, the
10 keybag.txt and fileinfolist.txt files).

11 Apple is hereby ordered to disclose the above information to the government
12 within 14 days of service of this warrant.

13 **II. Information to be seized by the government**

14 All information described above in Section I that constitutes fruits, contraband,
15 evidence and instrumentalities of violations of Title 18 U.S.C. § 2252(a)(2) (Receipt or
16 Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child
17 Pornography) those violations occurring in or after September 2014, found in the
18 Account listed on Attachment A, including the following:

19 a. Evidence of registration and use of Apple accounts, including
20 communications sent via iMessage or FaceTime;

21 b. Evidence of registration;

22 c. Evidence of visual depictions of minors engaged in sexually explicit
23 conduct;

24 d. Evidence that serves to identify any person who uses or accesses the
25 Account or who exercises in any way any dominion or control over the Account;

26 e. Evidence that may reveal the current or past location of the
27 individual or individuals using the Account;

28

1 f. Evidence of efforts to maintain anonymity online, including by
2 accessing VPNs;

3 g. Other log records, including IP address captures, associated with the
4 specified Accounts;

5 h. Subscriber records associated with the specified Accounts, including
6 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session
7 times and durations; 4) length of service (including start date) and types of services
8 utilized; 5) telephone or instrument number or other subscriber number or identity,
9 Including any temporarily assigned network address such as IP address, media access
10 card addresses, or any other unique device identifiers recorded by internet service
11 provider in relation to the account; 6) account log files (login IP address, account
12 activation IP addresses, and IP address history); 7) detailed billing records/logs; 8) means
13 and source of payment; and 9) lists of all related accounts;

14 i. Records of communications between the internet service provider
15 and any person purporting to be the account holder about issues relating to the Account,
16 such as technical problems, billing inquiries, or complaints from other users about the
17 specified Account. This to include records of contacts between the subscriber and the
18 provider's support services, as well as records of any actions taken by the provider or
19 subscriber as a result of the communications;

20 j. iPhone identification number, MEID, IMSI, ICCID, and cellular
21 telephone number;

22 k. Information identifying accounts that are linked or associated with
23 the Accounts.

24
25
26
27
28

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Apple, Inc. (“Apple”), and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Apple. The attached records consist of _____ [GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Apple, and they were made by Apple as a regular practice; and

b. such records were generated by Apple’s electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Apple in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Apple, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date: _____

Signature: _____

AFFIDAVIT

1
2
3 STATE OF WASHINGTON)
4) ss
5 COUNTY OF WHATCOM)
6

7 I, Toby Ledgerwood, being duly sworn on oath, depose and state:

8 **I. INTRODUCTION AND AGENT BACKGROUND**

9 1. I am a Special Agent with the U.S. Department of Homeland Security,
10 Homeland Security Investigations (HSI), assigned to the Assistant Special Agent in
11 Charge (ASAC) Blaine, Washington, field office. I have been employed as an HSI
12 Special Agent since 2006. Prior to this assignment, I worked as a United States Customs
13 Inspector from 2002 to 2006. In my capacity as a Special Agent, I am responsible for
14 conducting investigations into the numerous federal laws enforced by HSI. Since 2013, I
15 have investigated criminal violations relating to child exploitation and child pornography,
16 including violations pertaining to the unlawful production, importation, distribution,
17 receipt, attempted receipt, and possession of child pornography and material involving
18 the sexual exploitation of minors in violation of 18 U.S.C. §§ 2251, 2252(a), and
19 2252A(a). I am a graduate of the Federal Law Enforcement Training Center (FLETC),
20 HSI Special Agent Training Program, and have received further specialized training in
21 investigating child pornography and child exploitation crimes. My training included
22 courses in law enforcement techniques, federal criminal statutes, conducting criminal
23 investigations, and the execution of search warrants. I have observed and reviewed
24 thousands of examples of child pornography (as defined in 18 U.S.C. § 2256(8)). I have
25 participated in the execution of many search warrants which involved child exploitation
26 and/or child pornography offenses and the search and seizure of computers and other
27 digital devices. Further, I have served as the affiant on numerous search warrants and
28 complaints relating to child exploitation investigations. I am a member of the Internet

1 Crimes Against Children (ICAC) Task Force in the Western District of Washington, and
2 work with other federal, state, and local law enforcement personnel in the investigation
3 and prosecution of crimes involving the sexual exploitation of children. I have attended
4 periodic seminars, meetings, and training. I attended the ICAC Undercover
5 Investigations Training Program in Alexandria, Virginia, in June 2014 regarding child
6 exploitation. I also attended the Crimes Against Children Conference in Dallas, Texas, in
7 August 2014, where I received training relating to child exploitation, including training in
8 the Ares Peer to Peer (P2P) file sharing program. In September 2015, I received training
9 in the Emule (P2P) file sharing program. I received a Bachelor of Science degree in
10 Criminal Justice with a minor in Sociology from the University of Missouri-St. Louis.

11 2. I am submitting this affidavit in support of an application under for a search
12 warrant for information associated with an account that is stored at premises controlled
13 by Apple Inc. ("Apple"), located at One Apple Park Way in Cupertino, California,
14 ("THE PROVIDER").

15 3. This affidavit is made in support of an application for a search warrant
16 pursuant to Title 18, United States Code, Sections 2703(a), 2703(b)(1)(A) and
17 2703(c)(1)(A) to require **THE PROVIDER** to disclose to the government copies of the
18 information, including the content of communications, further described in Section I of
19 Attachments B, pertaining to the following Apple iCloud account and email address:

20 **slave524@icloud.com ("SUBJECT ACCOUNT")**

21 user information of **iCloud account**:

22 Name: jon lakey

23 Address: 7317 elaine street

24 Blaine, WA 98230

25 Mobile Phone: 3605106600

26 4. Upon receipt of the information described in Section I of Attachments B,
27 government-authorized persons will review that information to locate the items described
28

1 in Section II of Attachments B. This warrant is requested in connection with an on-going
2 investigation in this district by Homeland Security Investigations.

3 5. The warrant would authorize a search of the **SUBJECT ACCOUNT**, for
4 the purpose of identifying electronically stored data as particularly described in
5 Attachment B, for evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§
6 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B)
7 (Possession of Child Pornography).

8 6. The facts set forth in this Affidavit are based on my own personal
9 knowledge; knowledge obtained from other individuals during my participation in this
10 investigation, including other law enforcement officers; review of documents and records
11 related to this investigation; communications with others who have personal knowledge
12 of the events and circumstances described herein; and information gained through my
13 training and experience.

14 7. Because this affidavit is submitted for the limited purpose of establishing
15 probable cause in support of the application for a search warrant, it does not set forth
16 each and every fact that I or others have learned during the course of this investigation. I
17 have set forth only the facts that I believe are relevant to the determination of probable
18 cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §
19 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B)
20 (Possession of Child Pornography), will be found in **SUBJECT ACCOUNT**.

21 8. This Affidavit is being presented electronically pursuant to Local Criminal
22 Rule CrR 41(d)(3).

23 II. DEFINITIONS

24 9. The following definitions apply to this Affidavit:

25 Internet Service Providers

26 a. “Internet Service Providers” (ISPs), as used herein, are commercial
27 organizations that are in business to provide individuals and businesses access to the
28 internet. ISPs provide a range of functions for their customers including access to the

1 Internet, web hosting, email, remote storage, and co-location of computers and other
2 communications equipment. ISPs can offer a range of options in providing access to the
3 Internet including telephone based dial up, broadband based access via digital subscriber
4 line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs
5 typically charge a fee based upon the type of connection and volume of data, called
6 bandwidth, which the connection supports. Many ISPs assign each subscriber an account
7 name – a user name or screen name, an “email address,” an email mailbox, and a
8 personal password selected by the subscriber. By using a computer equipped with a
9 modem, the subscriber can establish communication with an ISP over a telephone line,
10 through a cable system or via satellite, and can access the Internet by using his or her
11 account name and personal password. ISPs maintain records pertaining to their
12 subscribers (regardless of whether those subscribers are individuals or entities). These
13 records may include account application information, subscriber and billing information,
14 account access information (often times in the form of log files), email communications,
15 information concerning content uploaded and/or stored on or via the ISP's servers.

16 Internet Protocol (IP) Addresses

17 b. “Internet Protocol address” or “IP address” refers to a unique number used
18 by a computer to access the Internet. An IP address looks like a series of four numbers,
19 each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer
20 connected to the Internet must be assigned an IP address so that the Internet traffic sent
21 from, and directed to, that computer may be properly directed from its source to its
22 destination. Most ISPs control the range of IP addresses.

23 Apple ID

24 c. Apple services are accessed through the use of an “Apple ID,” an account
25 created during the setup of an Apple device or through the iTunes or iCloud services. A
26 single Apple ID can be linked to multiple Apple services and devices, serving as a central
27 authentication and syncing mechanism. An Apple ID takes the form of the full email
28 address submitted by the user to create the account; it can later be changed. Users can

1 submit an Apple-provided email address (often ending in @icloud.com, @me.com, or
2 @mac.com) or an email address associated with a third-party email provider (such as
3 Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services
4 (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to
5 a “verification email” sent by Apple to that “primary” email address. Additional email
6 addresses (“alternate,” “rescue,” and “notification” email addresses) can also be
7 associated with an Apple ID by the user. Apple uses a unique

8 Virtual Private Network (VPN)

9 d. A VPN connection is a means of connecting to a private network over a
10 public network such as the Internet. A VPN is created by establishing a virtual point-to-
11 point connection through the use of dedicated connections, virtual tunneling protocols, or
12 traffic encryption. VPN’s are also frequently used by people who wish to circumvent
13 geographic IP limitations and censorship, and to connect to proxy servers for the purpose
14 of obfuscating the source of an internet connection or transmission.

15 **III. The CyberTip and ESP Apple Inc**

16 11. This investigation arose from a CyberTip submitted to the National Center
17 for Missing and Exploited Children (NCMEC). NCMEC is a private non-profit
18 organization operating under a Congressional mandate to act as the nation’s law
19 enforcement clearing house for information concerning online child sexual exploitation.
20 In partial fulfillment of that mandate, NCMEC operates a CyberTip line, a resource for
21 reporting online crimes against children. Electronic Service Providers (ESPs) report to
22 NCMEC, via the CyberTip line, whenever they discover that a subscriber has violated the
23 terms of service and/or their services have been used to transmit child pornography over
24 the Internet.

25 12. The CyberTip giving rise to the instant investigation came from ESP Apple,
26 Inc., an electronic communication/service provider and digital device manufacturer
27 headquartered in Cupertino, California.

28 **IV. STATEMENT OF PROBABLE CAUSE**

1 13. In October 2019, Homeland Security Investigations (HSI) Blaine,
2 Washington received CyberTip report #55619888 from the Seattle Internet Crimes
3 Against Children (ICAC) Task Force. In the CyberTip, Apple reported one of its users,
4 Jon Lakey, using email address slave524@icloud.com, uploaded several images of
5 suspected child pornography from IP Address 172.98.86.39 (the SUBJECT IP
6 ADDRESS) on September 17, 2019.

7 14. The uploads occurred in conjunction with attempts to send emails
8 containing images of suspected child pornography from slave524@icloud.com to
9 another email address. The CyberTip also indicated that this email contained the text
10 “Sent from my iPhone,” which is indicative of that email being sent using an Apple
11 iPhone. However, an Apple representative confirmed in response to an inquire from me
12 that Apple cannot definitively say whether or not the user of email address
13 slave524@icloud.com was in fact using an iPhone at the time.

14 15. A query of a publicly available database revealed the SUBJECT IP
15 ADDRESS belonged to ISP Total Server Solutions.

16 16. In response to an administrative summons seeking subscriber information
17 for the SUBJECT IP ADDRESS at the time of the upload of suspected child
18 pornography to Apple, Total Server Solutions responded with the following information:
19 “Hello, We received your subpoena request. Total Server Solutions provides
20 Infrastructure this client. This specific client would have a client on their end that was
21 using the IP addresses provided in the subpoena. Hence, a subpoena directed towards
22 them to retrieve that customer information would be needed. We are unsure of logs that
23 our clients have as we just host their infrastructure within our data centers. We do not
24 manage the actual applications on those servers. I have attached that information so you
25 can proceed. If anything additional is required please let me know.”

26 17. SA Ledgerwood reviewed the attachment, and the information provided
27 indicated the SUBJECT IP ADDRESS belonged to Tefincom S.A. located in Panama
28 City, Panama.

1 18. On November 19, 2019, SA Ledgerwood sent a request for assistance to SA
2 Harry Schmidt, HSI Panama. On November 20, 2019, SA Schmidt responded with the
3 following; “appears that company is another server type company here in Panama. We
4 have seen it before.” “Send us the IP, dates, times, etc. that you want to look at and we
5 will do a subpoena through Panama prosecutors and hopefully obtain the subscriber
6 info.” To date, there has been no further information provided by SA Schmidt.

7 19. From my training and experience, I believe it is likely the user of the
8 SUBJECT ACCOUNT was using a VPN to access that account at the time Apple
9 detected the attempted upload of child pornography to its servers. Thus, although the
10 SUBJECT IP ADDRESS appears to be owned by a provider in Panama, I believe it is
11 likely that the user of SUBJECT ACCOUNT is located in the Western District of
12 Washington.

13 20. Included with the CyberTip was identifying information associated with the
14 email address slave524@icloud.com, including the following:

15 Name: Jon Lakey

16 Address: 7317 Elaine Street, Blaine, Washington, 98230

17 Mobile Phone: 3605106600

18 21. The same Apple representative explained that the name, address, and phone
19 number, were all provided by the user at the time of creation of the
20 slave524@icloud.com account.

21 22. The Apple representative further explained, “I also went back and reviewed
22 the actual emails. As I mentioned, we use hash matching on outgoing email. When we
23 intercept the email with suspected images they do not go to the intended recipient. This
24 individual [, slave524@icloud.com,] sent 8 emails that we intercepted. [Seven] of those
25 emails contained 12 images. All 7 emails and images were the same as was the recipient
26 email address. The other email contained 4 images which were different than the 12
27 previously mentioned. The intended recipient was the same. I suspect what happened
28 was he was sending these images to himself and when they didn’t deliver he sent them

1 again repeatedly. Either that or he got word from the recipient that they did not get
2 delivered.”

3 23. Before submitting the CyberTip, employee(s) of Apple Inc examined each
4 of these images of suspected of child pornography.

5 24. I have reviewed these images as well, which Apple provided as part of the
6 CyberTiP, and describe them below:

7 **File 1**

8 This color image depicts a prepubescent female (hereinafter the “child victim”).
9 The child victim is nude and laying on her stomach facing the camera. The child
10 victim is nude from the waist down except for her socks. An erect penis is seen in
11 front of the child victim’s face. The child victim appears to have a large amount
12 of ejaculate on her face near her mouth and nose. The child victim is very small
13 in stature and lacks muscular development. The child victim appears to be
14 approximately 6 to 8 years old.

15 **File 2**

16 This color image depicts a prepubescent female (hereinafter the “child victim”).
17 An adult male is nude laying on a bed with the child victim, who is also
18 completely nude and sitting on top of the adult male. She is fully visible. The
19 child victim’s legs are spread apart and the male’s erect penis is inserted into her
20 vagina. The child victim’s breasts are exposed. She lacks muscular and breast
21 development, lacks visible pubic hair, and is very small in stature. The child
22 victim appears to be approximately 8-10 years old.

23 **File 3**

24 This color image depicts a prepubescent female (hereinafter the “child victim”).
25 The child victim is wearing black stockings, a pink collar, and hoop earrings. The
26 child victim’s breasts and genitals are exposed. An adult male’s hairy, erect penis
27 is seen being inserted or placed into the child victim’s vagina. The child victim
28 lacks muscular and breast development, lacks visible pubic hair, and is very small
in stature. The child victim appears to be approximately 6-8 years old.

29 25. On November 5, 2019, at approximately 1200 hrs. Group Supervisor (GS)
30 James Healy conducted surveillance of the SUBJECT PREMISES. It is a gray, single
31 story residence with white trim bearing address “7317” in black numbers on white trim
32 to the right of the door when facing the residence from the street. GS Healy took several
33 photographs of the residence and saw children’s toys in front of the residence on a table
34 against the residence next to a black barbecue grill. Later, at approximately 1500 hrs,

1 GS Healy saw two cars parked in the driveway of the residence, a white Acura passenger
2 car bearing license plate WAUS/APX8330 and a light green Kia Soul SUV bearing
3 license plate WAUS/BPA5152. At approximately 1520 hours GS Healy saw a balding
4 white male, heavy set, with a long beard wearing black hoodie and pants leave the home
5 walking a small dog and proceed south on Elaine St toward Bay Rd. That person
6 appeared to be the same person shows on the Washington DOL photo associated with
7 Jon Lakey (discussed below). At approximately 1535 hours GS Healy saw the same
8 man return to the home accompanied by a minor male.

9 26. On November 6, 2019, GS Healy conducted a search via the Washington
10 State Department of Licensing (WSDOL) and learned that Jon LAKEY has a 2007
11 Acura, registered at the SUBJECT PREMISES. WSDOL also revealed LAKEY was
12 issued a Washington State driver's license on November 10, 2016, with the SUBJECT
13 PREMISES listed as his address. WSDOL also revealed the Jon LAKEY and R.K. have
14 a 2013 Kia, registered at the SUBJECT PREMISES. WSDOL revealed R.K. was issued
15 a Washington State driver's license on January 18, 2017, with the SUBJECT
16 PREMISES listed as R.K.'s address.

17 27. Records checks conducted via the Whatcom County Assessor's Office
18 revealed that Jon LAKEY and R.K. own the SUBJECT PREMISES. The SUBJECT
19 PREMISES is listed on the Assessor's web-site as a doublewide manufactured home
20 located on .17 acres. According to the Assessor's Office, they purchased the house in
21 2006.

22 28. On December 5, 2019, while conducting surveillance of the SUBJECT
23 PREMISES, I used a portable electronic device to conduct a wireless survey from the
24 public right of way adjacent to the SUBJECT PREMISES and discovered numerous Wi-
25 Fi enabled networks. These Wi-Fi networks were all locked. During that survey, I also
26 detected at least one "xfinitywifi" wireless internet network in the area. Based on my
27 training and experience, I know that Comcast deployed a series of wireless "hotspot"
28 networks for their customers. Comcast accomplished this by providing their wireless

1 internet customers with updated wireless routers capable of broadcasting an additional
2 wireless network. These wireless “hotspot” networks are recognized by the connecting
3 device as “xfinitywifi”. Comcast customers can access “xfinitywifi” networks by
4 logging in with their unique Comcast email or username and previously created
5 password. Of particular importance is that the “xfinitywifi” networks are completely
6 separate from the Comcast customer’s private home wireless network(s). While
7 conducting a prior investigation, an official with Comcast confirmed with me that
8 Comcast’s “xfinitywifi” wireless networks are not linked or connected to the Comcast
9 subscriber’s internet service.

10 29. A query of a publicly available database revealed the phone number 360-
11 510-6600 belonged to ATT. In response to an administrative subpoena seeking
12 subscriber information for that phone number, ATT provided the following information.
13 The billing party for this number is R.K., and the billing address is the SUBJECT
14 PREMISES. ATT reported that the user of the phone is Jon Lakey and that service
15 between in 2004 and was current as of December 2019. The contact email for that user
16 was listed as SLAVE524@HOTMAIL.COM.

17 30. As outlined above, multiple sources of information indicate that LAKEY,
18 currently resides at the SUBJECT PREMISES and resided there on the dates that child
19 pornography files were uploaded from the SUBJECT IP ADDRESS via LAKEY’s
20 email. I believe that LAKEY used likely a mobile device to distribute child pornography
21 via the Internet, and that evidence of that crime will be found in the **SUBJECT**
22 **ACCOUNT**.

23 **IV. BACKGROUND CONCERNING ONLINE ACCOUNTS**

24 31. As explained herein, information stored in connection with an online
25 account may provide crucial evidence of the “who, what, why, when, where, and how” of
26 the criminal conduct under investigation, thus enabling the United States to establish and
27 prove each element or alternatively, to exclude the innocent from further suspicion.
28

1 32. In my training and experience, the information stored in connection with an
2 online account can indicate who has used or controlled the account. This “user
3 attribution” evidence is analogous to the search for “indicia of occupancy” while
4 executing a search warrant at a residence. For example, email communications, contacts
5 lists, and images sent (and the data associated with the foregoing, such as date and time)
6 may indicate who used or controlled the account at a relevant time.

7 33. Further, information maintained by the online provider can show how and
8 when and where the account was accessed or used. For example, as described below,
9 online providers typically log the Internet Protocol (IP) addresses from which users
10 access an account, along with the time and date of that access. By determining the
11 physical location associated with the logged IP addresses, investigators can understand
12 the chronological and geographic context of the email account access and use relating to
13 the crime under investigation. This geographic and timeline information may tend to
14 either inculpate or exculpate the account owner. Additionally, information stored at the
15 user’s account may further indicate the geographic location of the account user at a
16 particular time (e.g., location information integrated into an image or video sent via
17 email).

18 34. Stored electronic data may provide relevant insight into the online account
19 owner’s state of mind as it relates to the offense under investigation. For example,
20 information in the email account may indicate the owner’s motive and intent to commit a
21 crime (e.g., communications relating to the crime), or consciousness of guilt (e.g.,
22 deleting communications in an effort to conceal them from law enforcement).

23 **Apple’s Services**

24 35. Apple is a United States company that produces the iPhone, iPad, and iPod
25 Touch, all of which use the iOS operating system, and desktop and laptop computers
26 based on the Mac OS operating system. Apple provides a variety of services that can be
27 accessed from Apple devices or, in some cases, other devices via web browsers or mobile
28

1 and desktop applications (“apps”). As described in further detail below, the services
2 include email, instant messaging, and file storage:

3 36. Apple provides email service to its users through email addresses at the
4 domain names mac.com, me.com, and icloud.com.

5 37. iMessage and FaceTime allow users of Apple devices to communicate in
6 real-time. iMessage enables users of Apple devices to exchange instant messages
7 (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime
8 enables those users to conduct video calls.

9 38. iCloud is a file hosting, storage, and sharing service provided by Apple.
10 iCloud can be utilized through numerous iCloud-connected services, and can also be used
11 to store iOS device backups and data associated with third-party apps. iCloud can be
12 utilized to transfer data from an old device to a new device, including data derived from
13 device backups and third-party applications.

14 39. iCloud-connected services allow users to create, store, access, share, and
15 synchronize data on Apple devices or via icloud.com on any Internet-connected device.
16 For example, iCloud Mail enables a user to access Apple-provided email accounts on
17 multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream
18 can be used to store and manage images and videos taken from Apple devices, and
19 iCloud Photo Sharing allows the user to share those images and videos with other Apple
20 subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other
21 documents. iCloud Tabs enables iCloud to be used to synchronize webpages opened in
22 the Safari web browsers on all of the user’s Apple devices. iWorks Apps, a suite of
23 productivity apps (Pages, Numbers, and Keynote), enables iCloud to be used to create,
24 store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a
25 user to keep website username and passwords, credit card information, and Wi-Fi
26 network information synchronized across multiple Apple devices.

1 40. Location Services allows apps and websites to use information from
2 cellular, Wi-Fi, Global Positioning System (“GPS”) networks, and Bluetooth, to
3 determine a user’s approximate location.

4 41. App Store and iTunes Store are used to purchase and download digital
5 content. iOS apps can be purchased and downloaded through App Store on iOS devices,
6 or through iTunes Store on desktop and laptop computers running either Microsoft
7 Windows or Mac OS. Additional digital content, including music, movies, and television
8 shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop
9 computers running either Microsoft Windows or Mac OS.

10 42. Apple captures information associated with the creation and use of an
11 Apple ID. During the creation of an Apple ID, the user must provide basic personal
12 information including the user’s full name, physical address, and telephone numbers.
13 The user may also provide means of payment for products offered by Apple. The
14 subscriber information and password associated with an Apple ID can be changed by the
15 user through the “My Apple ID” and “iForgot” pages on Apple’s website. In addition,
16 Apple captures the date on which the account was created, the length of service, records
17 of log-in times and durations, the types of service utilized, the status of the account
18 (including whether the account is inactive or closed), the methods used to connect to and
19 utilize the account, the Internet Protocol address (“IP address”) used to register and
20 access the account, and other log files that reflect usage of the account.

21 43. Additional information is captured by Apple in connection with the use of
22 an Apple ID to access certain services. For example, Apple maintains connection logs
23 with IP addresses that reflect a user’s sign-on activity for Apple services such as iTunes
24 Store and App Store, iCloud, and the My Apple ID and iForgot pages on Apple’s
25 website. Apple also maintains records reflecting a user’s app purchases from App Store
26 and iTunes Store, “call invitation logs” for FaceTime calls, and “mail logs” for activity
27 over an Apple-provided email account. Records relating to the use of the Find My
28

1 iPhone service, including connection logs and requests to remotely lock or erase a device,
2 are also maintained by Apple.

3 44. Apple also maintains information about the devices associated with an
4 Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains
5 the user's IP address and identifiers such as the Integrated Circuit Card ID number
6 ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone
7 number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or
8 iMessage. Apple also may maintain records of other device identifiers, including the
9 Media Access Control address ("MAC address"), the unique device identifier ("UDID"),
10 and the serial number. In addition, information about a user's computer is captured when
11 iTunes is used on that computer to play content associated with an Apple ID, and
12 information about a user's web browser may be captured when used to access services
13 through icloud.com and apple.com. Apple also retains records related to communications
14 between users and Apple customer service, including communications regarding a
15 particular Apple device or service, and the repair history for a device.

16 45. Apple provides users with five gigabytes of free electronic space on iCloud,
17 and users can purchase additional storage space. That storage space, located on servers
18 controlled by Apple, may contain data associated with the use of iCloud-connected
19 services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My
20 Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and
21 other files (iWorks and iCloud Drive); and web browser settings and Wi-Fi network
22 information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS
23 device backups, which can contain a user's photos and videos, iMessages, Short Message
24 Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail
25 messages, call history, contacts, calendar events, reminders, notes, app data and settings,
26 and other data. Records and data associated with third-party apps may also be stored on
27 iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be
28 configured to regularly back up a user's instant messages on iCloud. Some of this data is

1 stored on Apple's servers in an encrypted form but can nonetheless be decrypted by
2 Apple.

3 46. In this case, I am investigating, among other things, the use of an Apple
4 account to distribute child pornography. In my training and experience, evidence of who
5 was using an Apple ID and from where, and evidence related to criminal activity of the
6 kind described above, may be found in the files and records described above. Stored e-
7 mails, chats, and other files may not only contain communications relating to the crimes
8 under investigation, but also help identify the participants in those crimes. Address
9 books and contact lists may help identify and locate the distributor, or those associated
10 with him/her. Search and browsing history may also constitute direct evidence of the
11 crimes under investigation to the extent the browsing history or search history might
12 include searches and browsing history and other evidence of the crimes under
13 investigation or indications of the true identity of the account user. In my training and
14 experience, I also know that the commission of the violations in the manner set forth
15 above necessarily requires the use of computers, smart phones, tablets, or other computer
16 devices.

17 47. In addition, the user's account activity, logs, stored electronic
18 communications, and other data retained by Apple can indicate who has used or
19 controlled the account. For example, subscriber information, email and messaging logs,
20 documents, and photos and videos (and the data associated with the foregoing, such as
21 geo-location, date and time) may be evidence of who used or controlled the account at a
22 relevant time. As an example, because every device has unique hardware and software
23 identifiers, and because every device that connects to the Internet must use an IP address,
24 IP address and device identifier information can help to identify which computers or
25 other devices were used to access the account. Such information also allows
26 investigators to understand the geographic and chronological context of access, use, and
27 events relating to the crime under investigation.

1 48. Other information connected to an Apple ID may lead to the discovery of
2 additional evidence. In addition, emails, instant messages, Internet activity, documents,
3 and contact and calendar information can lead to the identification of the distributor and
4 instrumentalities of the crimes under investigation. Therefore, Apple's servers are likely
5 to contain stored electronic communications and information concerning subscribers and
6 their use of Apple's services.

7 **V. PERSONS WITH A SEXUALIZED INTEREST IN**
8 **CHILDREN AND DEPICTIONS OF CHILDREN**

9 49. Based upon my knowledge, experience, and training in child pornography
10 investigations, and the training and experience of other law enforcement officers with
11 whom I have had discussions, I know that there are certain characteristics common to
12 individuals who have a sexualized interest in children and depictions of children:

13 a. They may receive sexual gratification, stimulation, and satisfaction
14 from contact with children; or from fantasies they may have viewing children engaged in
15 sexual activity or in sexually suggestive poses, such as in person, in photographs, or other
16 visual media; or from literature describing such activity.

17 b. They may collect sexually explicit or suggestive materials in a
18 variety of media, including photographs, magazines, motion pictures, videotapes, books,
19 slides, and/or drawings or other visual media. Such individuals often times use these
20 materials for their own sexual arousal and gratification. Further, they may use these
21 materials to lower the inhibitions of children they are attempting to seduce, to arouse the
22 selected child partner, or to demonstrate the desired sexual acts. These individuals may
23 keep records, to include names, contact information, and/or dates of these interactions, of
24 the children they have attempted to seduce, arouse, or with whom they have engaged in
25 the desired sexual acts.

26 c. They often maintain any "hard copies" of child pornographic
27 material that is, their pictures, films, video tapes, magazines, negatives, photographs,
28 correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of

1 their home or some other secure location. These individuals typically retain these “hard
2 copies” of child pornographic material for many years, as they are highly valued.

3 d. Likewise, they often maintain their child pornography collections
4 that are in a digital or electronic format in a safe, secure and private environment, such as
5 a computer and surrounding area. These collections are often maintained for several
6 years and are kept close by, often at the individual’s residence or some otherwise easily
7 accessible location, to enable the owner to view the collection, which is valued highly.
8 They also may opt to store the contraband in cloud accounts. Cloud storage is a model of
9 data storage where the digital data is stored in logical pools, the physical storage can span
10 multiple servers, and often locations, and the physical environment is typically owned
11 and managed by a hosting company. Cloud storage allows the offender ready access to
12 the material from any device that has an Internet connection, worldwide, while also
13 attempting to obfuscate or limit the criminality of possession as the material is stored
14 remotely and not on the offender’s device.

15 e. They also may correspond with and/or meet others to share
16 information and materials; rarely destroy correspondence from other child pornography
17 distributors/collectors; conceal such correspondence as they do their sexually explicit
18 material; and often maintain lists of names, addresses, and telephone numbers of
19 individuals with whom they have been in contact and who share the same interests in
20 child pornography.

21 f. They generally prefer not to be without their child pornography for
22 any prolonged time period. This behavior has been documented by law enforcement
23 officers involved in the investigation of child pornography throughout the world.

24 g. E-mail itself provides a convenient means by which individuals can
25 access a collection of child pornography from any computer, at any location with Internet
26 access. Such individuals therefore do not need to physically carry their collections with
27 them but rather can access them electronically. Furthermore, these collections can be
28

1 stored on email “cloud” servers, which allow users to store a large amount of material at
2 no cost, without leaving any physical evidence on the users’ computer(s).

3 50. In addition to offenders who collect and store child pornography, law
4 enforcement has encountered offenders who obtain child pornography from the internet,
5 view the contents and subsequently delete the contraband, often after engaging in self-
6 gratification. In light of technological advancements, increasing Internet speeds and
7 worldwide availability of child sexual exploitative material, this phenomenon offers the
8 offender a sense of decreasing risk of being identified and/or apprehended with quantities
9 of contraband. This type of consumer is commonly referred to as a ‘seek and delete’
10 offender, knowing that the same or different contraband satisfying their interests remain
11 easily discoverable and accessible online for future viewing and self-gratification. I
12 know that, regardless of whether a person discards or collects child pornography he/she
13 accesses for purposes of viewing and sexual gratification, evidence of such activity is
14 likely to be found on computers and related digital devices, including storage media, used
15 by the person. This evidence may include the files themselves, logs of account access
16 events, contact lists of others engaged in trafficking of child pornography, backup files,
17 and other electronic artifacts that may be forensically recoverable.

18 51. Given the above-stated facts, including the circumstances surrounding the
19 Apple Inc CyberTip and based on my knowledge, training and experience, along with my
20 discussions with other law enforcement officers who investigate child exploitation
21 crimes, I believe that the iCloud account/email slave524@icloud.com user likely has a
22 sexualized interest in children and depictions of children. I therefore believe that
23 evidence of child pornography is likely to be found in the **SUBJECT ACCOUNT**.

24 **VI. INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

25 52. Pursuant to Title 18, United States Code, Section 2703(g), this application
26 and affidavit for a search warrant seeks authorization to require **THE PROVIDERS**, and
27 their agents and employees, to assist agents in the execution of this warrant. Once issued,
28 the search warrant will be presented to **THE PROVIDERS** with direction that they

1 identify the accounts described in Attachments A to this affidavit, as well as other
2 subscriber and log records associated with the accounts, as set forth in Section I of
3 Attachments B to this affidavit.

4 53. The search warrant will direct **THE PROVIDERS** to create an exact copy
5 of the specified account and records.

6 54. I, and/or other law enforcement personnel will thereafter review the copy of
7 the electronically stored data and identify from among that content those items that come
8 within the items identified in Section II to Attachments B for seizure.

9 55. Analyzing the data contained in the forensic copy may require special
10 technical skills, equipment, and software. It could also be very time-consuming.
11 Searching by keywords, for example, can yield thousands of “hits,” each of which must
12 then be reviewed in context by the examiner to determine whether the data is within the
13 scope of the warrant. Merely finding a relevant “hit” does not end the review process.
14 Keywords used originally need to be modified continuously, based on interim results.
15 Certain file formats, moreover, do not lend themselves to keyword searches, as keywords,
16 search text, and many common email, database and spreadsheet applications do not store
17 data as searchable text. The data may be saved, instead, in proprietary non-text format.
18 And, as the volume of storage allotted by service providers increases, the time it takes to
19 properly analyze recovered data increases, as well. Consistent with the foregoing,
20 searching the recovered data for the information subject to seizure pursuant to this
21 warrant may require a range of data analysis techniques and may take weeks or even
22 months. All forensic analysis of the data will employ only those search protocols and
23 methodologies reasonably designed to identify and seize the items identified in Section II
24 of Attachments B to the warrant.

25 56. Based on my experience and training, and the experience and training of
26 other agents with whom I have communicated, it is necessary to review and seize a
27 variety of e-mail communications, chat logs and documents, that identify any users of the
28

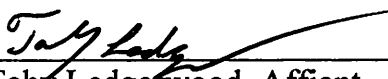
1 subject account and e-mails sent or received in temporal proximity to incriminating e-
2 mails that provide context to the incriminating communications.

3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28



VII. CONCLUSION

57. Based on the foregoing, I believe there is probable cause that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography), are located in the **SUBJECT ACCOUNT** as more fully described in Attachment A to this Affidavit. I therefore request that the court issue a warrant authorizing a search of the **SUBJECT ACCOUNT** specified in Attachment A for the items more fully described in Attachment B.


Toby Ledgerwood, Affiant
Special Agent
Department of Homeland Security
Homeland Security Investigations

The above named agent provided a sworn statement attesting to the truth of the forgoing affidavit this 17 day of January, 2020.


BRIAN A. TSUCHIDA
Chief United States Magistrate Judge



ATTACHMENT A

Description of Property to be Searched

This warrant applies to information associated with the Apple iCloud account/email: slave524@icloud.com (the “account”), that is stored at premises owned, maintained, controlled, or operated by Apple, Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.



1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

ATTACHMENT B
ITEMS TO BE SEIZED

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

1 c. The contents of all emails associated with the account, including stored or
2 preserved copies of emails sent to and from the account (including all draft emails and
3 deleted emails), the source and destination addresses associated with each email, the date
4 and time at which each email was sent, the size and length of each email, and the true and
5 accurate header information including the actual IP addresses of the sender and the
6 recipient of the emails, and all attachments;

7 d. The contents of all instant messages associated with the account from,
8 including stored or preserved copies of instant messages (including iMessages, SMS
9 messages, and MMS messages) sent to and from the account (including all draft and
10 deleted messages), the source and destination account or phone number associated with
11 each instant message, the date and time at which each instant message was sent, the size
12 and length of each instant message, the actual IP addresses of the sender and the recipient
13 of each instant message, and the media, if any, attached to each instant message;

14 e. The contents of all files and other records stored on iCloud, including all
15 iOS device backups, all Apple and third-party app data, all files and other records related
16 to iCloud Photo Library, Photo Stream, iCloud Drive, Safari Browsing History, and all
17 address books, contact and buddy lists, notes, reminders, calendar entries, images, videos,
18 voicemails, device settings, and bookmarks;

19 f. All activity, connection, and transactional logs for the account (with
20 associated IP addresses including source port numbers), including FaceTime call
21 invitation logs, messaging and query logs (including iMessage, SMS, and MMS
22 messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases,
23 downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs,
24 sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My
25 Friends logs, logs associated with web-based access of Apple services (including all
26 associated identifiers), and logs associated with iOS device purchase, activation, and
27 upgrades;

28

1 g. All records and information regarding locations where the account or
2 devices associated with the account were accessed, including all data stored in connection
3 with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

4 h. All records pertaining to the types of service used;

5 i. All records pertaining to communications between Apple and any person
6 regarding the account, including contacts with support services and records of actions
7 taken; and

8 j. All files, keys, or other information necessary to decrypt any data produced
9 in an encrypted form, when available to Apple (including, but not limited to, the
10 keybag.txt and fileinfolist.txt files).

11 Apple is hereby ordered to disclose the above information to the government
12 within 14 days of service of this warrant.

13 **II. Information to be seized by the government**

14 All information described above in Section I that constitutes fruits, contraband,
15 evidence and instrumentalities of violations of Title 18 U.S.C. § 2252(a)(2) (Receipt or
16 Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child
17 Pornography) those violations occurring in or after September 2014, found in the
18 Account listed on Attachment A, including the following:

19 a. Evidence of registration and use of Apple accounts, including
20 communications sent via iMessage or FaceTime;

21 b. Evidence of registration;

22 c. Evidence of visual depictions of minors engaged in sexually explicit
23 conduct;

24 d. Evidence that serves to identify any person who uses or accesses the
25 Account or who exercises in any way any dominion or control over the Account;

26 e. Evidence that may reveal the current or past location of the
27 individual or individuals using the Account;

28

1 f. Evidence of efforts to maintain anonymity online, including by
2 accessing VPNs;

3 g. Other log records, including IP address captures, associated with the
4 specified Accounts;

5 h. Subscriber records associated with the specified Accounts, including
6 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session
7 times and durations; 4) length of service (including start date) and types of services
8 utilized; 5) telephone or instrument number or other subscriber number or identity,
9 Including any temporarily assigned network address such as IP address, media access
10 card addresses, or any other unique device identifiers recorded by internet service
11 provider in relation to the account; 6) account log files (login IP address, account
12 activation IP addresses, and IP address history); 7) detailed billing records/logs; 8) means
13 and source of payment; and 9) lists of all related accounts;

14 i. Records of communications between the internet service provider
15 and any person purporting to be the account holder about issues relating to the Account,
16 such as technical problems, billing inquiries, or complaints from other users about the
17 specified Account. This to include records of contacts between the subscriber and the
18 provider's support services, as well as records of any actions taken by the provider or
19 subscriber as a result of the communications;

20 j. iPhone identification number, MEID, IMSI, ICCID, and cellular
21 telephone number;

22 k. Information identifying accounts that are linked or associated with
23 the Accounts.

1 **CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT**
2 **TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)**

3 I, _____, attest, under penalties of perjury by
4 the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the
5 information contained in this certification is true and correct. I am employed by Apple,
6 Inc. (“Apple”), and my title is _____. I am qualified to
7 authenticate the records attached hereto because I am familiar with how the records were
8 created, managed, stored, and retrieved. I state that the records attached hereto are true
9 duplicates of the original records in the custody of Apple. The attached records consist of
10 _____ [GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]. I
11 further state that:

12 a. all records attached to this certificate were made at or near the time of the
13 occurrence of the matter set forth by, or from information transmitted by, a person with
14 knowledge of those matters, they were kept in the ordinary course of the regularly
15 conducted business activity of Apple, and they were made by Apple as a regular practice;
16 and

17 b. such records were generated by Apple’s electronic process or system that
18 produces an accurate result, to wit:

19 1. the records were copied from electronic device(s), storage
20 medium(s), or file(s) in the custody of Apple in a manner to ensure that they are true
21 duplicates of the original records; and

22 2. the process or system is regularly verified by Apple, and at all times
23 pertinent to the records certified here the process and system functioned properly and
24 normally.

25 I further state that this certification is intended to satisfy Rules 902(11) and
26 902(13) of the Federal Rules of Evidence.

27 Date: _____

Signature: _____