AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Central District of California

United States of America
v.
Steve Jackson Rodriguez

Case No. 5:21-mj-00551-Duty

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of January 27, 2018 in the county of San Bernardino in the Central District of California, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. § 2251(a)	Production of Child Pornography

This criminal complaint is based on these facts:

Please see attached affidavit

☑ Continued on the attached sheet.

/s/
Complainant's signature

Derek R. Baker
Printed name and title

Sworn to before me by telephone pursuant to FRCP 4.1.

Date: 8/26/2021, 9:50 am

Judge's signature

City and state: Los Angeles, CA

HON. PEDRO V. CASTILLO, UNITED STATES MAGISTRATE JUDGE
Printed name and title

AUSA:

AFFIDAVIT

I, Derek R. Baker, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the United States Department of Homeland Security ("DHS"), Immigration and Customs Enforcement ("ICE"), Homeland Security Investigations ("HSI"), and have been so employed since June 2018.

II. BACKGROUND OF SPECIAL AGENT DEREK R. BAKER

2. I am currently assigned to the HSI Los Angeles Child Exploitation Task Force, where I investigate criminal violations relating to child exploitation and child pornography, illegal production, distribution, receipt and possession of child pornography, in violation of 18 U.S.C. §§ 2252A and the SUBJECT OFFENSES. I have received training in the area of child pornography and child exploitation offenses and have observed and reviewed various examples of child pornography in all forms of media, including computer media.

3. I have participated in the execution of numerous search warrants, many of which involved child exploitation and/or child pornography offenses, including those relating to subjects who use the Internet and two-way communication devices, such as cellular telephones, to entice or coerce minors to engage in sexually explicit conduct. I make this affidavit based upon my personal knowledge and experience, my review of pertinent documentation, and discussions with other law enforcement officers.

4. Through both my training and my experience, I have become familiar with the methods of operation used by people who commit offenses involving the sexual exploitation of children. I have attended training classes concerning computer crimes and the sexual exploitation of children on the Internet. This training has given me an understanding of how people involved with offenses relating to the sexual exploitation of children use the Internet to further those offenses. My experience in investigations in this regard has supplemented my understanding of how people involved in offenses related to the sexual exploitation of children use the Internet to further those offenses.

III. PURPOSE OF AFFIDAVIT

5. By this affidavit, I seek a criminal complaint for Steve Jackson Rodriguez ("RODRIGUEZ") for Production of Child Pornography, in violation of 18 U.S.C. § 2251(a). The facts set forth in this affidavit are based upon my personal observations, my training and experience, documents, evidence, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

IV. BACKGROUND ON CHILD EXPLOITATION OFFENSES

6. Based upon my training and experience in the investigation of child pornography offenses, and information related to me by other law enforcement officers involving the investigation of child pornography offenses, I know the following information about child pornography:[1]

a. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where: (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

b. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

c. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or

[1] Additional terms and background are contained in the affidavit incorporated by reference attached as exhibit 1.

masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

V. SUMMARY OF PROBABLE CAUSE

7. On or about July 12, 2021, I received information from the National Center for Missing and Exploited Children ("NCMEC") which identified a user who uploaded child pornography files using their Google account, stevoevil22@gmail.com (the "SUBJECT ACCOUNT"). In a later interview with law enforcement, RODRIGUEZ confirmed that he owned the SUBJECT ACCOUNT until it was suspended/terminated by Google.

8. On or about August 6, 2021, I obtained a federal search warrant from the Honorable Maria A. Audero, in case number 2:21-mj-3616, for the SUBJECT ACCOUNT. While searching the SUBJECT ACCOUNT, law enforcement found videos which appeared to depict RODRIGUEZ orally copulating a minor victim who was approximately 5-9 years old[2] ("MV #1").[3] According to data associated with two other images of MV #1 found in the SUBJECT ACCOUNT, these two images were taken using an LG Electronics device, model LG-LS993 cell phone ("LG G6"). On August 25, 2021, law enforcement found an LG G6 cell phone in RODRIGUEZ's

[2] Law enforcement later determined MV #1 was approximately 8 years old at the time this conduct occurred.

[3] Law enforcement has not completed its review of the SUBJECT ACCOUNT. This affidavit does not list all of the items found to date in the SUBJECT ACCOUNT, nor does it represent a full review of the SUBJECT ACCOUNT.

car. In the search of the SUBJECT ACCOUNT, law enforcement also found other images of a person who appeared to be RODRIGUEZ.

9. On or about August 19, 2021, I obtained three federal search warrants from the Honorable Alka Sagar to search the SUBJECT PREMISES, RODRIGUEZ's person, and RODRIGUEZ's suspected vehicle (the "SUBJECT VEHICLE," collectively, the "August 19th Search Warrants"). A copy of the application to search the SUBJECT PREMISES, filed in case number 2:21-mj-3867, is attached to this affidavit as Exhibit 1.[4] Exhibit 1 is attached and wholly incorporated by reference.

10. On August 25, 2021, law enforcement executed the August 19th Search Warrants and interviewed RODRIGUEZ. During this interview law enforcement showed RODRIGUEZ a still image of MV #1 which was taken from a file found in the SUBJECT ACCOUNT. In response to seeing an image of MV #1, RODRIGUEZ identified MV #1 by first and last name and identified her as 9 years old.

11. As set forth below in more detail, I believe there is probable cause that RODRIGUEZ committed the SUBJECT OFFENSE.

VI. STATEMENT OF PROBABLE CAUSE

12. I learned the following information from my review of information from NCMEC, Google, the SUBJECT ACCOUNT, information found from publicly available and law enforcement databases,

[4] The additional search warrant applications to search RODRIGUEZ's person and the SUBJECT VEHICLE were based on the same affidavit and are located in case numbers 2:21-mj-3868, and 2:21-mj-3869.

interviews of witnesses, through my personal observations and investigation, and discussions with other law enforcement agents:

A. Initial Investigation

1. Identification of the SUBJECT ACCOUNT

13. Using data provided by NCMEC and Google, law enforcement was able to determine that a user had uploaded suspected child pornography on the SUBJECT ACCOUNT, as described in more detail in Exhibit 1.

14. According to Google, the SUBJECT ACCOUNT is registered to "Steve Rodriguez," registered with phone number (626) 392-8852 (the "-8852 Number"), verified[5] on January 25, 2016, at 7:30 a.m. UTC. In a later interview with law enforcement RODRIGUEZ stated that the -8852 Number was his phone number, and that he used the SUBJECT ACCOUNT.

15. Google provided EXIF[6] data from two of the 18 files Google reported as containing and/or associated with suspected child pornography uploaded to the SUBJECT ACCOUNT. The EXIF data captured by Google indicated these two files were captured using an LG Electronics device, model LG-LS993 (which is more

[5] According to Google, phone number(s) are provided by the account holder. "Verified" indicates the account holder responded to a request by the PROVIDER to confirm the phone number is valid/correct.

[6] EXIF is abbreviated for exchangeable image file format, which is data contained withing the file, and can contain specific information about that file, including, but not limited to, the camera make/model and date the file was created.

commonly known as a "G6") and on the same date/time, which was January 1, 2018, at 4:09 a.m., however the exact time zone was not indicated. Based on my training and experience, I know EXIF data can potentially help identify the physical device which produced the files, here the child pornography files. This EXIF data for two of the files uploaded into the SUBJECT ACCOUNT appears to match data from RODRIGUEZ's registered cellphone at the time. These two still images appear to depict MV #1. MV #1's face is clearly visible in the images, and she appears to have a colostomy bag attached to her abdomen.[7]

16. During my review of the SUBJECT ACCOUNT, I saw at least two videos that appeared to depict RODRIGUEZ orally copulating MV #1 (the "SUBJECT VIDEOS").[8] During the SUBJECT VIDEOS, you can see MV #1's colostomy bag. The file name of these two files appeared to indicate they were recorded on January 27, 2018. According to metadata provided by Google, the

[7] These two still images of MV #1 may contain child pornography; however, the government is not relying on these two images to establish probable cause in the instant complaint. The government mentions these images and MV #1 to demonstrate that a LG G6 cellphone associated with RODRIGUEZ may have been used to capture and/or store images or videos of child pornography or of MV #1. These images will be referred to as ("IMAGE #1" and "IMAGE #2").

[8] I identified RODRIGUEZ based on a comparison of the SUBJECT VIDEOS with other images contained in the SUBJECT ACCOUNT and his DMV photograph, and I identified MV #1 based on a comparison of the victim in IMAGE #1, IMAGE #2 and the two videos depicting RODRIGUEZ and MV #1 mentioned above.

image's "Photo taken date/time" was listed as January 27, 2018.[9] Therefore, I believe these images were produced on January 27, 2018.

2. DMV Records

17. Through subsequent investigation I was able to obtain DMV records for RODRIGUEZ. Through these records I was able to identify the SUBJECT PREMISES and SUBJECT VEHICLE as RODRIGUEZ's registered address and registered car.

18. RODRIGUEZ's DMV records also include an image of RODRIGUEZ, which I have viewed. RODGIRUGEZ appeared to be a Hispanic male whom according to the record, is approximately 5'08" tall and weighs 158 pounds.

B. Subsequent Investigation

19. On August 25, 2021, the SUBJECT VEHICLE was parked at RODRIGUEZ's workplace, College Hospital in Cerritos, California. SA Radlinski and I approached RODRIGUEZ as he was walking to his car and began a conversation with him. I was able to identify RODRIGUEZ from pictures of RODRIGUEZ I had reviewed earlier, including those located in the SUBJECT ACCOUNT, his DMV photo, and in his child pornography videos with MV #1. RODRIGUEZ was also wearing a nametag which read "Steve."[10]

---

[9] The SUBJECT ACCOUNT appeared to contain additional child pornography images with the same and different victims. The SUBJECT ACCOUNT also appeared to contain additional images showing RODRIGUEZ engaged in additional sexual conduct with minors. I have not included a discussion of these images, nor do I rely on them for the probable cause in the instant complaint.

[10] Steve is RODRIGUEZ's first name.

20. RODRIGUEZ agreed to speak with law enforcement willingly. RODRIGUEZ, SA Radlinski, and I walked to a shaded area in the parking lot of RODRIGUEZ's employer. At that time, I activated a digital audio recorder to memorialize the interview with RODRIGUEZ. Neither SA Radlinski or I wore any attire with a law enforcement insignia and had no weapons visible at any time. All three of us were located in an open parking lot, and law enforcement told RODRIGUEZ that he could end the interview and leave at any time. The interview began at approximately 11:34 a.m. I started the interview by reading RODRIGUEZ his Miranda rights from Immigration and Customs Enforcement ("ICE") Form 73-025. After reading the Statement of Rights to RODRIGUEZ, I gave him the form to sign if he wished. Although he did not sign the form, RODRIGUEZ agreed to speak with us. The below information was learned from the interview with RODRIGUEZ, who stated the following, among other incriminating statements:[11]

a. RODRIGUEZ owned the SUBJECT ACCOUNT until it had been suspended/terminated upon notification by Google that inappropriate content was in the account.

b. RODRIGUEZ is currently employed as a "mental health worker" at a semi-secure facility which houses voluntary and involuntary persons, including both adults and minors, with

[11] The following statements in this affidavit only include statements made during the first portion of law enforcement's interview with RODRIGUEZ, and does not include any statements made throughout the remaining portion of the interview.

job duties that can include administrative duties and physical care.

c. During this interview law enforcement showed RODRIGUEZ a still image of MV #1 which was taken from a file found in the SUBJECT ACCOUNT.[12] In response, RODRIGUEZ identified MV #1 by first and last name and stated she was 9 years old. In response to further questioning, RODRIGUEZ stated, "She is safe."

d. I believe RODRIGUEZ's statements identifying MV #1 and that "She is safe" is confirmation that RODRIGUEZ personally knew and victimized MV #1 as depicted in the video. These admissions demonstrate that the videos found in RODRIGUEZ's SUBJECT ACCOUNT that appear to depict RODRIGUEZ engaging in sexual conduct with MV #1, do in fact depict RODRIGUEZ engaged in sexual conduct with MV #1.

21. Subsequent to the interview, law enforcement searched RODRIGUEZ's car and found an LG G6 cellphone along with memory cards. These items were seized pursuant to the August 19th Search Warrants.

22. Subsequent to the interview, I was able to use the name provided by RODRIGUEZ to identify MV #1, among other things, to obtain a photo of MV #1 and compared that photograph to the child pornography depicting MV #1. I believe these photos depict the same person.

---

[12] I compared RODRIGUEZ's face in these videos with his DMV photo, images on the SUBJECT ACCOUNT, and from having seen him in person during this interview.

23. According to the identifying information I obtained for MV #1 and RODRIGUEZ, RODRIGUEZ was 33 years old, and MV #1 was approximately 8 years old at the suspected time of the sexual contact depicted in the child pornography. This information corroborates RODRIGUEZ's incriminating statements.

VII. CONCLUSION

24. For all the reasons described above, there is probable cause to believe that RODRIGUEZ committed the offense of production of child pornography in violation of 18 U.S.C. § 2251(a).

/s/
DEREK BAKER, Special Agent
Homeland Security
Investigations

Subscribed to and sworn before me by telephone pursuant to FRCP 4.1. this 26 day of August, 2021.

HONORABLE PEDRO V. CASTILLO
UNITED STATES MAGISTRATE JUDGE

EXHIBIT 1

UNITED STATES DISTRICT COURT

for the

Central District of California

FILED
CLERK, U.S. DISTRICT COURT
August 19, 2021
CENTRAL DISTRICT OF CALIFORNIA
BY: CD DEPUTY

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

Steve Jackson Rodriguez, Date of Birth: 03/25/1984, California driver's license: D2730390

Case No. 2:21-MJ-03867

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

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-2

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

See Attachment B

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

☒ evidence of a crime;

☒ contraband, fruits of crime, or other items illegally possessed;

☒ property designed for use, intended for use, or used in committing a crime;

☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C § 2251	Production and Attempted Production of Child Pornography
18 U.S.C. § 2252A(a)(2)	Distribution or Receipt of Child Pornography
18 U.S.C. § 2252A(a)(5)(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.

/s/
Applicant's signature

HSI Special Agent Derek R. Baker
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: August 19, 2021

Judge's signature

City and state: Los Angeles, CA

Honorable Alka Sagar, U.S. Magistrate Judge
Printed name and title

AUSA: Lara x0427

ATTACHMENT A-2

PERSON TO BE SEARCHED

The person to be searched, and the property that is on his person, is identified as Steve Jackson Rodriguez, date of birth 03/25/1984, California driver's license D2730390, and who is approximately 5 foot 8 inches tall. Steve Jackson Rodriguez's person includes any pockets in his clothing, and any bags or other containers carried or held by him or within his immediate control and includes the search of any digital devices found, provided that Steve Jackson Rodriguez is located within the Central District of California at the time of the search.

ATTACHMENT B

ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 2251 (production and/or attempted production of child pornography), 18 U.S.C. § 2252A(a)(2) (distribution or receipt of child pornography), and 18 U.S.C. § 2252A(a)(5)(B) (possession of child pornography) (the "SUBJECT OFFENSES"), namely:

a. Child pornography, as defined in 18 U.S.C. § 2256(8).

b. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that refer to child pornography, as defined in 18 U.S.C. § 2256(8), including but not limited to documents that refer to the possession, receipt, distribution, transmission, reproduction, viewing, sharing, purchase, or downloading, production, shipment, order, requesting, trade, or transaction of any kind, involving child pornography.

c. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, and also including but not limited to financial records, tending to identify persons involved in the possession, receipt, distribution, transmission, reproduction, viewing, sharing, purchase, or downloading, production, shipment, order, requesting, trade, or transaction of any kind, involving child pornography, as defined in 18 U.S.C. § 2256.

d. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that refer or relate to any production, receipt, shipment, order, request, trade, purchase, or transaction of any kind involving the transmission through interstate commerce by any means, including by computer, of any visual depiction of a minor engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

e. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, identifying persons transmitting in interstate commerce, including by computer, any visual depiction of a minor engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

f. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that identify any minor visually depicted while engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

g. Any and all records, documents, programs, applications, materials, items, depictions, images, or videos of children, even if not child pornography.

h. Any and all records, documents, programs, applications, materials, items, depictions, images, or videos of children, evidencing RODRIGUEZ's access to children.

i. Any and all records, documents, programs, applications, materials, items, depictions, images, or videos of a colostomy bag, the use of a colostomy bag, or of a child who

has any medical condition that may require the use of a colostomy bag.

j. Any and all records, documents, programs, applications, materials, items, depictions, images, videos, or other evidence of MV #1.

k. Any and all records, documents, programs, applications, or materials or items which are sexually arousing to individuals who are interested in minors, but which are not in and of themselves obscene or which do not necessarily depict minors involved in sexually explicit conduct. Such material is commonly known as "child erotica" and includes written materials dealing with child development, sex education, child pornography, sexual abuse of children, incest, child prostitution, missing children, investigative techniques of child exploitation, sexual disorders, pedophilia, nudist publications, diaries, and fantasy writings.

l. Any and all records, documents, programs, applications, materials, items, images, or depictions of underwear, lingerie, sex toys, or other items that are commonly used in the sexual abuse of children.

m. Any records, documents, programs, applications, or materials identifying possible minor victims depicted in child pornography and/or minor victims of sexual abuse.

n. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, which pertain to peer-to-peer file sharing software.

o. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, which pertain to accounts with any Internet Service Provider.

p. Any records, documents, programs, applications, materials, and files relating to IP addresses 47.149.10.108 and 47.149.20.114.

q. Records, documents, programs, applications, materials, and files relating to the deletion, uploading, and/or acquisition of victim files to include photographs, videos, e-mails, chat logs, or other files.

r. Any digital device bearing electronic serial number 089451725600202258.

s. Any digital device which is an LG G6.

t. Any records, documents, programs, applications, materials, items, files, or products related to or could be used in the production of images, videos, or other depictions of child pornography.

u. Any records, documents, programs, applications, materials, items, files, or products related to or could be used in the production of images, videos, or items depicted in any of the 18 images of child pornography found in the SUBJECT ACCOUNT.

v. Any digital device used to facilitate the above-listed violations and forensic copies thereof.

w. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the SUBJECT OFFENSES, and forensic copies thereof.

x. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence 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 of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's 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.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

SEARCH PROCEDURE FOR DIGITAL DEVICES

4. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as “EnCase” and “FTK” (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques, including to search for known images of child pornography.

c. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

6. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offenses listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

7. During the execution of this search warrant, with respect to RODRIGUEZ, who is located in the Central District of California during the execution of the search and who is reasonably believed by law enforcement to be a user of a biometric sensor-enabled device that falls within the scope of the warrant, law enforcement personnel are authorized to: (1)

depress the thumb- and/or fingerprints of RODRIGUEZ onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of the face of RODRIGUEZ with his eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing RODRIGUEZ's thumb or finger onto a device and in holding a device in front of RODRIGUEZ's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

8. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

AFFIDAVIT

I, Derek R. Baker, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the United States Department of Homeland Security ("DHS"), Immigration and Customs Enforcement ("ICE"), Homeland Security Investigations ("HSI"), and have been so employed since June 2018.

II. PURPOSE OF AFFIDAVIT

2. This affidavit is made in support of an application for warrants to search the following:

a. 1113 San Bernardino Avenue, Pomona, California 91767 (the "SUBJECT PREMISES"), as further described in Attachment A-1; and,

b. The person of Steve Jackson Rodriguez ("RODRIGUEZ") date of birth is 03/25/1984, who appears to be a Hispanic male, and is approximately 5 foot 8 inches tall, as further described in Attachment A-2; and,

c. A 2017 blue Honda Civic bearing California license plate 8TEA232 registered to RODRIGUEZ (the "SUBJECT VEHICLE"), as further described in Attachment A-3.

3. As described further in Attachment B, the requested warrants seek authorization to seize evidence, fruits, and instrumentalities, of violations of 18 U.S.C. § 2251 (production and/or attempted production of child pornography), 18 U.S.C. § 2252A(a)(2) (distribution or receipt of child pornography), and 18 U.S.C. § 2252A(a)(5)(B) (possession of child pornography)

(collectively, the "SUBJECT OFFENSES"). Attachments A-1, A-2, A-3, and B are attached hereto and incorporated herein by reference.

4. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

III. BACKGROUND OF SPECIAL AGENT DEREK R. BAKER

5. I am currently assigned to the HSI Los Angeles Child Exploitation Task Force, where I investigate criminal violations relating to child exploitation and child pornography, illegal production, distribution, receipt and possession of child pornography, in violation of 18 U.S.C. §§ 2252A and the SUBJECT OFFENSES. I have received training in the area of child pornography and child exploitation offenses and have observed and reviewed various examples of child pornography in all forms of media, including computer media.

6. I have participated in the execution of numerous search warrants, many of which involved child exploitation and/or child pornography offenses, including those relating to subjects who use the Internet and two-way communication devices, such as cellular telephones, to entice or coerce minors to

engage in sexually explicit conduct. I make this affidavit based upon my personal knowledge and experience, my review of pertinent documentation, and discussions with other law enforcement officers.

7. Through both my training and my experience, I have become familiar with the methods of operation used by people who commit offenses involving the sexual exploitation of children. I have attended training classes concerning computer crimes and the sexual exploitation of children on the Internet. This training has given me an understanding of how people involved with offenses relating to the sexual exploitation of children use the Internet to further those offenses. My experience in investigations in this regard has supplemented my understanding of how people involved in offenses related to the sexual exploitation of children use the Internet to further those offenses.

IV. BACKGROUND ON CHILD EXPLOITATION OFFENSES, COMPUTERS, THE INTERNET, AND DEFINITION OF TERMS

8. Based upon my training and experience in the investigation of child pornography offenses, and information related to me by other law enforcement officers involving the investigation of child pornography offenses, I know the following information about the use of computer with child pornography:

a. Computers and Child Pornography. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. Child

pornographers can now produce both still and moving images directly from a common video camera and can convert these images into computer-readable formats. The use of digital technology has enabled child pornographers to electronically receive, distribute, and possess large numbers of child exploitation images and videos with other Internet users worldwide.

b. File Storage. Computer users can choose their method of storing files: either on a computer's hard drive, an external hard drive, a memory card, a USB thumb drive, a smart phone or other digital media device, etc. (i.e., "locally") or on virtual servers accessible from any digital device with an Internet connection (i.e., "cloud storage"). Computer users frequently transfer files from one location to another, such as from a phone to a computer or from cloud storage to an external hard drive. Computer users also often create "backup," or duplicate, copies of their files. In this way, digital child pornography is extremely mobile and such digital files are easily reproduced and transported. For example, with the click of a button, images and videos containing child pornography can be put onto external hard drives small enough to fit onto a keychain. Just as easily, these files can be copied onto compact disks and/or stored on mobile digital devices, such as smart phones and tablets. Furthermore, even if the actual child pornography files are stored on a "cloud," files stored in this manner can only be accessed via a digital device. Therefore, viewing this child pornography would require a computer,

smartphone, tablet, or some other digital device that allows the user to access and view files on the Internet.

c. Internet. The term "Internet" is defined as the worldwide network of computers -- a noncommercial, self-governing network devoted mostly to communication and research with roughly 500 million users worldwide. The Internet is not an online service and has no real central hub. It is a collection of tens of thousands of computer networks, online services, and single user components. In order to access the Internet, an individual computer user must use an access provider, such as a university, employer, or commercial Internet Service Provider(s) ("ISP(s)"), which operates a host computer with direct access to the Internet.

d. Internet Service Providers. Individuals and businesses obtain access to the ISPs. ISPs provide their customers with access to the Internet using telephone or other telecommunications lines; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers; remotely store electronic files on their customer's behalf; and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or businesses that have subscriber accounts with them. Those records often include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application

information, and other information both in computer data and written record format.

e. IP Addresses. An Internet Protocol address ("IP Address") is a unique numeric address used to connect to the Internet. An IPv4 IP Address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). In simple terms, one computer in a home may connect directly to the Internet with an IP Address assigned by an ISP. What is now more typical is that one home may connect to the Internet using multiple digital devices simultaneously, including laptops, tablets, smart phones, smart televisions, and gaming systems, by way of example. Because the home subscriber typically only has one Internet connection and is only assigned one IP Address at a time by their ISP, multiple devices in a home are connected to the Internet via a router or hub. Internet activity from every device attached to the router or hub is utilizing the same external IP Address assigned by the ISP. The router or hub "routes" Internet traffic so that it reaches the proper device. Most ISPs control a range of IP Addresses. The IP Address for a user may be relatively static, meaning it is assigned to the same subscriber for long periods of time, or dynamic, meaning that the IP Address is only assigned for the duration of that online session. Most ISPs maintain records of which subscriber was assigned which IP Address during an online session.

f. IP Address – IPv6. Due to the limited number of available IPv4 IP addresses, a new protocol was established using the hexadecimal system to increase the number of unique IP

addresses. An IPv6 consists of eight sets of combination of four numbers 0-9 and/or letters A through F. An example of an IPv6 IP address is 2001:0db8:0000:0000:0000:ff00:0042:8329.

g. The following definitions:

i. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

ii. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where: (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

iii. "Cloud-based storage," as used herein, is a form of digital data storage in which the digital data is stored on remote servers hosted by a third party (as opposed to, for example, on a user's computer or other local storage device) and is made available to users over a network, typically the Internet. Users of such a service can share links and associated

passwords to their stored files with other traders of child pornography in order to grant access to their collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop and laptop computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to a file stored on a cloud-based service does not need to be a user of the service to access the file. Access is typically free and readily available to anyone who has an Internet connection.

iv. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

v. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including

keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

vi. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

vii. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

viii. "Encryption" is the process of converting data into a code in order to prevent unauthorized access to the data.

ix. 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.

x. "Log files" are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

xi. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

xii. "Mobile applications," as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a.

xiii. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

xiv. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

xv. A "storage medium" or "storage device" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, "thumb," "jump," or "flash" drives, CD-ROMs, and other magnetic or optical media.

xvi. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

xvii. A "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

V. SUMMARY OF PROBABLE CAUSE

9. On or about July 12, 2021, I received information from the National Center for Missing and Exploited Children ("NCMEC") regarding CyberTipline Report 94619315 (the "CyberTip") which identified a user who uploaded child pornography files using their Google account.

10. The CyberTip contained the IP addresses captured by Google at the time of login and during upload of the various child pornography files. The return of legal process show the IP addresses resolved to the SUBJECT PREMISES. Records show RODRIGUEZ currently resides at the SUBJECT PREMISES.

11. On or about August 6, 2021, I obtained a federal search warrant from the Honorable Maria A. Audero, in case number 2:21-mj-3616, for RODRIGUEZ's Google account primarily based on the information obtained from the CyberTip and Google's log information. Shortly thereafter, law enforcement executed the 2:21-mj-3616 search warrant on RODRIGUEZ's Google account which showed that several child pornography files were in his account and according to IP address information, those files were uploaded from the SUBJECT PREMISES. As set forth below in more detail, I believe there is probable cause to search the SUBJECT PREMISES, RODRIGUEZ's person (the registered owner of the SUBJECT ACCOUNT and the apparent resident of the SUBJECT PREMISES), and RODRIGUEZ's registered vehicle, the SUBJECT VEHICLE, for evidence related to the SUBJECT OFFENSES.

VI. STATEMENT OF PROBABLE CAUSE

12. I learned the following information from my review of the CyberTip and information found from publicly available and law enforcement databases:

A. Identification of the Account

13. On or about July 7, 2021, at approximately 3:32 a.m. Universal Coordinated Time ("UTC"), NCMEC received information from Google (the "PROVIDER") reporting that 18 files containing and/or associated with suspected child pornography were uploaded by an individual using the account stevoevil22@gmail.com (the "SUBJECT ACCOUNT"). The PROVIDER provided NCMEC with basic subscriber information for the SUBJECT ACCOUNT.

14. According to the PROVIDER, the subscriber of the SUBJECT ACCOUNT is registered to "Steve Rodriguez," registered with phone number (626) 392-8852 (the "-8852 Number"), verified[1] on January 25, 2016, at 7:30 a.m. UTC.

15. The PROVIDER also indicated they had captured EXIF[2] data from two (2) of the 18 files. The EXIF data captured by the PROVIDER indicated both of the files were captured using an LG Electronics device, model LG-LS993 (which is more commonly

---

[1] According to the PROVIDER, phone number(s) are provided by the account holder. "Verified" indicates the account holder responded to a request by the PROVIDER to confirm the phone number is valid/correct.

[2] EXIF is abbreviated for exchangeable image file format, which is data contained withing the file, and can contain specific information about that file, including, but not limited to, the camera make/model and date the file was created.

known as a "G6") and on the same date/time, which was January 1, 2018, at 4:09 a.m., however the exact time zone was not indicated. I know this information to mean the data contained within the file is providing information that potentially help in identifying the physical device which produced the child pornography files. This EXIF data for two of the files uploaded into the SUBJECT ACCOUNT appears to match data from RODRIGUEZ's registered cellphone at the time. These two still images appear to depict a Caucasian female, approximately 5-9 years old ("MV #1"). MV #1's face is clearly visible in the images, and she appears to have a colostomy bag attached to her abdomen.[3]

16. On or about August 17, 2021, I have reviewed at least eight (8) videos stored on the SUBJECT ACCOUNT as obtained from the PROVIDER, and they depict suspected child pornography as defined in 18 U.S.C. § 2256. During my review of the SUBJECT ACCOUNT, I saw at least three (3) videos involving MV #1. Two of these videos appear to depict RODRIGUEZ engaging in oral

[3] These two still images of MV #1 may contain child pornography; however, the government is not relying on these two images to establish probable cause that defendant possessed or produced child pornography in the instant search warrant. The government mentions these images and MV #1 to demonstrate that there is independent probable cause to search a LG G6 cellphone associated with RODRIGUEZ, which may have been used to capture and/or store images or videos of child pornography or of minor victims. These images will be referred to as ("IMAGE #1" and "IMAGE #2").

copulation with what appears to be MV #1.[4] During two of the videos of apparent child pornography, which I believe depicts RODRIGUEZ performing oral sex on MV #1, you can see MV #1's colostomy bag in the video.

17. The PROVIDER included information in the CyberTip, which showed the previous IP addresses captured at the time the uploads occurred using the SUBJECT ACCOUNT. I know this information can show me where the user was physically located, by address, when the user uploaded the child pornography files. I know through my training and experience that when a person engages in the SUBJECT OFFENSES, it typically occurs in a place where the person can conceal their actions or conduct.

18. A search of publicly available and law enforcement databases of "Steve Rodriguez" and the SUBJECT PREMISES indicates that a 37-year-old "Steve Jackson Rodriguez" is associated with the SUBJECT PERMISES.

B. Description of Additional Files Uploaded Using the Subject Account

19. In the CyberTip, the PROVIDER indicated 18 files containing or associated with child pornography were uploaded using the SUBJECT ACCOUNT. The CyberTip also specifically stated at least some of the uploaded child pornography files

[4] I identified RODRIGUEZ based on a comparison with other images contained in the SUBJECT ACCOUNT and his DMV photograph, and I identified MV #1 based on a comparison of the victim in IMAGE #1, IMAGE #2 and the two videos depicting RODRIGUEZ and MV #1 mentioned above.

"appear unfamiliar and may depict newly produced content," which can mean the files had not been previously identified to NCMEC.

20. I have reviewed the 15 files which had been previously viewed by the PROVIDER, among others later provided from the search of the SUBJECT ACCOUNT. The following are descriptions of two files that I have reviewed from the SUBJECT ACCOUNT which depict suspected child pornography as defined in 18 U.S.C. § 2256:

a. "report_11626601965411693084.jpg" ("IMAGE #3") which is an image file and appears to depict a Caucasian female, approximately 5-7 years old, laying on her back with her vagina exposed while engaging in what appears to be anal sex with what appears to be an adult male penis.

b. "report_14309050322603975612.jpg" ("IMAGE #4") which is an image file and appears to depict a Caucasian female, approximately 4-6 years old, with her hand holding what appears to be an adult male penis, which appears to be touching her face.

C. Identification of the User

21. On or about July 12, 2021, I searched for and located the following information using Accurint[5]:

a. A search of the -8852 Number produced a result for "Steve Rodriguez," a full social security number ending in -3105 ("RODRIGUEZ's SS NUMBER"), and information that this person

[5] A for-pay service which can help to identify people, addresses, relatives, businesses, vehicles and other information by providing a comprehensive database of public records.

was associated with the SUBJECT PREMISES from March 2020 through at least July 2020.

b. A search of RODRIGUEZ's SS NUMBER showed RODRIGUEZ's birth date as March 25, 1984, and records indicated that RODRIGUEZ's SS NUMBER was associated with the SUBJECT PREMISES from March 2020 through at least July 2021.

22. California Department of Motor Vehicles ("DMV") records for "Steve Rodriguez" with a birthdate March 25, 1984, showed RODRIGUEZ is registered with the DMV with a current registered address of the SUBJECT PREMISES since at least on or about April 24, 2021. DMV records also include an image of RODRIGUEZ, which I have viewed. RODGIRUGEZ appeared to be a Hispanic male whom according to the record, is approximately 5'08" tall and weighs 158 pounds. I and other law enforcement officers who execute this search warrant will be able to identify RODRIGUEZ in part based on this DMV photo which I and others have viewed before we execute the warrant.

23. Using the information provided in the CyberTip, I conducted further investigation into the SUBJECT ACCOUNT and discovered the following:

a. IP address 47.149.10.108 ("SUBJECT IP ADDRESS #1") was the IP address captured at login (approximately July 4, 2021, at 10:16 p.m. UTC) and when the user of the SUBJECT ACCOUNT uploaded IMAGE #1 (approximately December 6, 2020, at 9:07 p.m. UTC). Frontier Communications Corporation owns SUBJECT IP ADDRESS #1. On July 15, 2021, I received information from Frontier Communications for SUBJECT IP ADDRESS #1 which showed

that SUBJECT IP ADDRESS #1 was assigned to a Frontier Communications account in RODRIGUEZ's name on the relevant dates. The Frontier Communication account in RODRIGUEZ's name lists the SUBJECT PREMISES as the account address and the SUBJECT ACCOUNT as its contact email address.

b. IP address 2607:fb90:21cb:8952:dcaf:31a8:8c79:f31f was the IP address captured when the user uploaded IMAGE #2 (approximately June 21, 2020 at 6:15 p.m. UTC). T-Mobile owns this IP address; however, without certain identifying information not contained in the CyberTip, I would be unable to determine the subscriber for this IP address during the time of upload.

c. IP address 47.149.20.114 ("SUBJECT IP ADDRESS #2") was the IP address captured when the user uploaded IMAGE #3 (approximately May 28, 2020, at 7:56 p.m. UTC) and IMAGE #4 (approximately August 15, 2020, at 9:52 p.m. UTC). On or about July 22, 2021, I received information from Frontier Communications for SUBJECT IP ADDRESS #2, which showed SUBJECT IP ADDRESS #2 was assigned to a Frontier Communications account in RODRIGUEZ's name. The Frontier Communication account in RODRIGUEZ's name lists the SUBJECT PREMISES as the account address on the relevant dates.

d. According to a search of law enforcement and public databases, T-Mobile is the phone provider for the -8852 Number, which is the mobile phone number registered with the PROVIDER.

i. On or about July 22, 2021, I received information from T-Mobile, which showed RODRIGUEZ's billing address was the SUBJECT PREMISES. Additionally, T-Mobile provided device information for the period indicated in the captured EXIF data (January 1, 2018).

ii. According to T-Mobile records, RODRIGUEZ used a device with electronic serial number ("ESN") 089451725600202258, which was used from April 10, 2017, through May 5, 2019.

iii. I used a general Internet search for a website that allows the status check of any ESN and saw the ESN belonged to a LG G6. According to the EXIF data provided by NCMEC in the CyberTip, an LG G6 is make/model of device that appears to have been used to create two of the suspected child pornography files uploaded by the SUBJECT ACCOUNT.

e. On or about July 21, 2021, I received information from the California Employment Development Department which showed RODRIGUEZ had provided the SUBJECT PREMISES as his address since July 24, 2018, and provided the -8852 Number as his phone number.

24. On or about August 3, 2021, at approximately 12:00 p.m. local time, I arrived at the SUBJECT PREMISES and saw a blue Honda Civic bearing California license plate 8TEA232 (the "SUBJECT VEHICLE") parked on the street directly in front of the

SUBJECT PREMISES. According to DMV information, this vehicle is registered to RODRIGUEZ at the SUBJECT PREMSES.

25. On or about August 6, 2021, the Honorable Maria Audero, United States Magistrate Judge in the Central District of California signed the search warrant (21-mj-3616) for the SUBJECT ACCOUNT.

26. On or about the same date, I served the PROVIDER with the search warrant. On or about August 11, 2021, the PROVIDER produced files in response to the search warrant.

27. I reviewed some of the files produced by the PROVIDER. The files I reviewed included additional child pornography files uploaded to RODRIGUEZ's account. Additionally, I reviewed videos contained within the SUBJECT ACCOUNT that appeared to depict RODRIGUEZ, as I recognized him from the previously viewed photograph retained by the DMV, and at least one video which appeared to show a Hispanic male bearing a likeness to RODRIGUEZ, in/around a blue Honda vehicle that appeared to match the SUBJECT VEHICLE.

28. On or about August 18, 2021, from 6:00 a.m. through approximately 11:30 a.m. local time, SA Paul Radlinski and I conducted surveillance at the SUBJECT PREMISES and saw the SUBJECT VEHICLE park in front of the SUBJECT PREMISES at approximately 8:40 a.m. Shortly thereafter, a Hispanic male I recognized as RODRIGUEZ exited the driver's seat, and enter the front door after appearing to unlock it. At approximately 11:30 a.m., RODRIGUEZ exited the SUBJECT PREMISES through the front door, entered the SUBJECT VEHICLE, and left the area.

VII. TRAINING & EXPERIENCE ON INDIVIDUALS WITH A SEXUAL INTEREST IN CHILDREN

29. Based on my training and experience, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that individuals who view and possess multiple images of child pornography are often individuals who have a sexual interest in children and in images of children, and that there are certain characteristics common to such individuals:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or in other visual media, or from literature describing such activity. These individuals often maintain possession of these items for long periods of time and keep their collections in numerous places – in digital devices in their homes, in their cars, in their workplaces, or on their persons.

b. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials (including through digital distribution via the Internet); conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share

the same interests in child pornography. These individuals often maintain possession of these items for long periods of time.

30. If an individual produces an image of child pornography on a digital device, law enforcement can often obtain evidence of this production if they are to seize and search the digital device itself, even if the image is no longer stored on the digital device.

31. Digital child pornography on a digital device is easy to maintain for long periods of time. Modern digital devices often have extremely large storage capacities. Furthermore, cheap and readily available storage devices, such as thumb drives, external hard drives, and compact discs make it simple for individuals with a sexual interest in children to download child pornography from the Internet and save it – simply and securely – so it can be accessed or viewed indefinitely.

32. Furthermore, even if a person deleted any images of child pornography that may have been possessed or distributed, there is still probable cause to believe that there will be evidence of the illegal activities – that is, the possession, receipt, and/or distribution of child pornography – at the SUBJECT PREMISES, in the SUBJECT VEHICLE, or on RODRIGUEZ's person. Based on my training and experience, as well as my conversations with digital forensic experts, I know that remnants of such files can be recovered months or years after they have been deleted from a computer device. Evidence that child pornography files were downloaded and viewed can also be

recovered, even after the files themselves have been deleted, using forensic tools. Because remnants of the possession, distribution, and viewing of child pornography is recoverable after long periods of time, searching the SUBJECT PREMISES, SUBJECT VEHICLE, and RODRIGUEZ's person could lead to evidence of the child exploitation offenses.

VIII. BACKGROUND ON CYBERTIPS

33. CyberTipline Report. NCMEC was established in 1984 as a private, nonprofit 501(c)(3) organization. NCMEC provides services nationwide for families and professionals in the prevention of abducted, endangered, and sexually exploited children. Pursuant to its mission and its congressional authorization (see 42 U.S.C. § 5773), NCMEC operates the CyberTipline and the Child Victim Identification Program to assist law enforcement in identifying victims of child pornography and child sexual exploitation. NCMEC works with law enforcement, Internet service providers, electronic payment service providers, and others to reduce the distribution of child sexual exploitation images and videos over the Internet. NCMEC's CyberTipline is the nation's centralized reporting system for the online exploitation of children. The public and electronic service providers can make reports of suspected online enticement of children for sexual acts, extra-familial child sexual molestation, child pornography, child sex tourism, child sex trafficking, unsolicited obscene materials sent to a child, misleading domain names, and misleading words or digital images on the internet. NCMEC does not investigate and cannot

verify the accuracy of information reported to NCMEC. NCMEC forwards the reports of child sexual exploitation to law enforcement for purposes of investigation and disposition of potential criminal wrongdoing to be determined solely by the relevant law enforcement agency and prosecutor's office. As part of the CyberTipline program, internet service providers that identify suspected child exploitation material on their systems may send a report to NCMEC. The reports contain information such as the account name, name, telephone number, and ISP address associated with an individual who uploaded suspected child exploitation material. The CyberTipline reports also indicate whether the provider viewed the suspected child exploitation material.

IX. TRAINING & EXPERIENCE ON GOOGLE

34. Based on a review of information provided by Google regarding its services, information provided by other law enforcement officers, and/or my training and experience, I am aware of the following:

a. Google provides numerous free services to users with a Google account. These services include Gmail, Google Drive, and Google Photos. Gmail is a web-based email service. Google Drive is a file storage and synchronization service which provides users with cloud storage, file sharing, and collaborative editing. Google Photos is an image hosting and sharing web service that allows users with a Google account to

store and share images for free. The username for a Google account is the email address linked to the account.

b. In my training and experience, I have learned that providers of e-mail and/or social media services offer a variety of online services to the public. Subscribers obtain an account by registering with Google. In my training and experience, e-mail and social media providers generally ask their subscribers to provide certain personal identifying information when registering for an e-mail or social media account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, e-mail and social media providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of login (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account.

c. In addition, e-mail and social media providers often have records of the Internet Protocol ("IP") address used to register the account and the IP addresses associated with particular logins to the account. Google will send

verifications to a user in order to verify information the user lists on their Google account. The verification typically involves a process in which the Electronic Service Provider ("ESP") sends an email, text message, or voice verification to the phone number listed and verifies the information when the subscriber responds to the ESP's email, phone call or text message.

X. TRAINING & EXPERIENCE ON DIGITAL DEVICES[6]

35. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. A person who connects to the Internet must use a computer or mobile device, such as a tablet or wireless telephone, to facilitate that access. Furthermore, in my training and experience, these devices typically travel with a subject or remain in SUBJECT PREMISES or in the subject's vehicle. It is therefore reasonable to believe that computers, tablets, wireless telephones, and other electronic storage media may be present in SUBJECT PREMISES, on RODRIGUEZ's person, or in the SUBJECT VEHICLE. Further, because it is possible to store

[6] As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral input/output devices, such as keyboards, printers, scanners, monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

certain mobile devices, such as removable storage media and wireless telephones, in a pocket, it is reasonable to believe that mobile devices may be found on RODRIGUEZ's person or in any place a small item can fit.

b. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

c. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat

programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

d. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

e. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

36. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult

to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

37. The search warrant requests authorization to use the biometric unlock features of the devices seized, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the

opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. As noted above, I know that most homes with Internet capability use only one IP address. That IP address, in turn, is often shared by many devices that access the Internet using a wireless modem. Accordingly, if there are multiple digital devices discovered during a search of the SUBJECT PREMISES, any of those devices could have been used to access the Internet and download the files discussed above.

d. Thus, if while executing the warrant, law enforcement personnel encounter a digital device within the scope of the warrant that may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to, with respect to RODRIGUEZ, provided he is located in the Central District of California during the execution of the search: (1) depress the RODRIGUEZ's thumb- and/or fingers on the device(s); and (2) hold the device(s) in front of RODRIGUEZ's face with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

38. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

XI. CONCLUSION

39. For all the reasons described above, there is probable cause to believe to believe that evidence, fruits, and

instrumentalities of violations of 18 U.S.C. § 2252A(a)(2) (distribution or receipt of child pornography), and 18 U.S.C. § 2252A(a)(5)(B) (possession of child pornography) as described in Attachment B, will be found in a search of the SUBJECT PREMISES, RODGRIGUEZ, and the SUBJECT VEHICLE.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 19th day of August, 2021.

THE HONORABLE ALKA SAGAR
UNITED STATES MAGISTRATE JUDGE

AO 93C (Rev. 8/18) Warrant by Telephone of Other Reliable Electronic Means ☐ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Steve Jackson Rodriguez, Date of Birth: 03/25/1984, California driver's license: D2730390	)	Case No. 2:21-MJ-03867

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

See Attachment A-2

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

Such affidavit(s) or testimony are incorporated herein by reference.

YOU ARE COMMANDED to execute this warrant on or before 14 days from the date of its issuance *(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 the U.S. Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.

☐ 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: August 19, 2021 10:59 a.m.

Judge's signature

City and state: Los Angeles, CA

Honorable Alka Sagar, U.S. Magistrate Judge
Printed name and title

AUSA: Lara x0427

AO 93C (Rev. 8/18) Warrant by Telephone of Other Reliable Electronic Means (Page 2)

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

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A-2

PERSON TO BE SEARCHED

The person to be searched, and the property that is on his person, is identified as Steve Jackson Rodriguez, date of birth 03/25/1984, California driver's license D2730390, and who is approximately 5 foot 8 inches tall. Steve Jackson Rodriguez's person includes any pockets in his clothing, and any bags or other containers carried or held by him or within his immediate control and includes the search of any digital devices found, provided that Steve Jackson Rodriguez is located within the Central District of California at the time of the search.

ATTACHMENT B

ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 2251 (production and/or attempted production of child pornography), 18 U.S.C. § 2252A(a)(2) (distribution or receipt of child pornography), and 18 U.S.C. § 2252A(a)(5)(B) (possession of child pornography) (the "SUBJECT OFFENSES"), namely:

a. Child pornography, as defined in 18 U.S.C. § 2256(8).

b. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that refer to child pornography, as defined in 18 U.S.C. § 2256(8), including but not limited to documents that refer to the possession, receipt, distribution, transmission, reproduction, viewing, sharing, purchase, or downloading, production, shipment, order, requesting, trade, or transaction of any kind, involving child pornography.

c. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, and also including but not limited to financial records, tending to identify persons involved in the possession, receipt, distribution, transmission, reproduction, viewing, sharing, purchase, or downloading, production, shipment, order, requesting, trade, or transaction of any kind, involving child pornography, as defined in 18 U.S.C. § 2256.

d. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that refer or relate to any production, receipt, shipment, order, request, trade, purchase, or transaction of any kind involving the transmission through interstate commerce by any means, including by computer, of any visual depiction of a minor engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

e. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, identifying persons transmitting in interstate commerce, including by computer, any visual depiction of a minor engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

f. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, that identify any minor visually depicted while engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

g. Any and all records, documents, programs, applications, materials, items, depictions, images, or videos of children, even if not child pornography.

h. Any and all records, documents, programs, applications, materials, items, depictions, images, or videos of children, evidencing RODRIGUEZ's access to children.

i. Any and all records, documents, programs, applications, materials, items, depictions, images, or videos of a colostomy bag, the use of a colostomy bag, or of a child who

has any medical condition that may require the use of a colostomy bag.

j. Any and all records, documents, programs, applications, materials, items, depictions, images, videos, or other evidence of MV #1.

k. Any and all records, documents, programs, applications, or materials or items which are sexually arousing to individuals who are interested in minors, but which are not in and of themselves obscene or which do not necessarily depict minors involved in sexually explicit conduct. Such material is commonly known as "child erotica" and includes written materials dealing with child development, sex education, child pornography, sexual abuse of children, incest, child prostitution, missing children, investigative techniques of child exploitation, sexual disorders, pedophilia, nudist publications, diaries, and fantasy writings.

l. Any and all records, documents, programs, applications, materials, items, images, or depictions of underwear, lingerie, sex toys, or other items that are commonly used in the sexual abuse of children.

m. Any records, documents, programs, applications, or materials identifying possible minor victims depicted in child pornography and/or minor victims of sexual abuse.

n. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, which pertain to peer-to-peer file sharing software.

o. Any records, documents, programs, applications, or materials, including electronic mail and electronic messages, which pertain to accounts with any Internet Service Provider.

p. Any records, documents, programs, applications, materials, and files relating to IP addresses 47.149.10.108 and 47.149.20.114.

q. Records, documents, programs, applications, materials, and files relating to the deletion, uploading, and/or acquisition of victim files to include photographs, videos, e-mails, chat logs, or other files.

r. Any digital device bearing electronic serial number 089451725600202258.

s. Any digital device which is an LG G6.

t. Any records, documents, programs, applications, materials, items, files, or products related to or could be used in the production of images, videos, or other depictions of child pornography.

u. Any records, documents, programs, applications, materials, items, files, or products related to or could be used in the production of images, videos, or items depicted in any of the 18 images of child pornography found in the SUBJECT ACCOUNT.

v. Any digital device used to facilitate the above-listed violations and forensic copies thereof.

w. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the SUBJECT OFFENSES, and forensic copies thereof.

x. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence 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 of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's 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.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

SEARCH PROCEDURE FOR DIGITAL DEVICES

4. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques, including to search for known images of child pornography.

c. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

6. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offenses listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

7. During the execution of this search warrant, with respect to RODRIGUEZ, who is located in the Central District of California during the execution of the search and who is reasonably believed by law enforcement to be a user of a biometric sensor-enabled device that falls within the scope of the warrant, law enforcement personnel are authorized to: (1)

depress the thumb- and/or fingerprints of RODRIGUEZ onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of the face of RODRIGUEZ with his eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing RODRIGUEZ's thumb or finger onto a device and in holding a device in front of RODRIGUEZ's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

8. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.