AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Middle District of Florida

United States of America
v.
MARIE-JO GORDO

Case No. 6:23-mj-2213

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 June 17, June 26, and July 8, 2023 in the county of Seminole/Orange/Osceola in the Middle District of Florida, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. §§ 2251(a)	Sexual Exploitation of Children Producing Child Pornography

This criminal complaint is based on these facts:

See Attached Affidavit

☑ Continued on the attached sheet.

Complainant's signature

Eric Phillips, Task Force Officer, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 10/25/2023

Judge's signature

City and state: Orlando, Florida

LESLIE HOFFMAN PRICE, U.S. Magistrate Judge
Printed name and title

STATE OF FLORIDA **Case No. 6:23-mj-**2213 thru 2214

COUNTY OF ORANGE

MASTER AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT AND APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Eric Phillips, being duly sworn, depose and state the following:

1. I am a Task Force Officer ("TFO") with the Federal Bureau of Investigation ("FBI") and have been since October 2019. I have been employed by the Seminole County Sheriff's Office as a Deputy Sheriff since March 2005. In February 2013, I was assigned to the Seminole County Sheriff's Office, Crimes Against Children Unit, as a Detective investigating cases involving child death, child abuse, child neglect, and internet crimes against children. I have received specialized training in the investigation of sex crimes, child exploitation, child pornography, and computer crimes. I have participated in investigations of persons suspected of violating federal child pornography laws, including 18 U.S.C. §§ 2251 and 2252A. I have also participated in investigations of persons suspected of enticing and coercing minors to engage in sexual activity in violation of 18 U.S.C. § 2422.

2. I have participated in various training courses for the investigation and enforcement of federal child pornography laws in which computers are used as the means for producing, receiving, transmitting, and storing child pornography. Additionally, I have been involved in authoring search warrants as well as

participated in the execution of search warrants involving searches and seizures of computers, computer equipment, software, and electronically stored information.

3. I make this affidavit based on my training, experience, and background as a law enforcement officer, including my experience with the FBI, my personal participation in the investigation, and information provided by other law enforcement officers and agency personnel. As set forth in greater detail below, I have probable cause to believe that a crime has taken place, specifically that Marie-Jo GORDO ("GORDO") produced child pornography in violation of 18 U.S.C. § 2251(a), possessed child pornography in violation of 18 U.S.C. § 2252A(a)(5), received and distributed child pornography in violation of 18 U.S.C. § 2252(a)(2), and coerced and enticed a minor to engage in sexual activity in violation of 18 U.S.C. § 2422(b). Furthermore, I have probable cause to believe that the person of GORDO will have instrumentalities, contraband, and evidence of the crimes being investigated, as set forth in Attachment B.

4. This affidavit is submitted in support of a criminal complaint against GORDO specifically for a violation of 18 U.S.C. § 2251(a) (producing of child pornography). This affidavit in also submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search GORDO's person and any electronic devices located on GORDO'S person for the things described in Attachment B.

5. I make this affidavit from personal knowledge based on my participation in this investigation, information from other criminal investigators,

information from other law enforcement officers, information from agency reports, and a review of documents provided to me by these witnesses and law enforcement officers. Because this affidavit is being submitted for the limited purpose of establishing probable cause in support of a criminal complaint and search warrant, I have not set forth each and every fact learned during the course of this investigation.

INVESTIGATION

6. On September 22, 2023, a parent reported to the Orange County Sheriff's Office ("OCSO") that her minor son and child-victim ("CV"), who has not attained 18 years of age, was engaged in a sexual relationship with his former teacher, GORDO. The parent provided the OCSO with CV's Apple iPhone 14 belonging to CV and provided consent to search the phone. GORDO had been a teacher at a school located in Orange County, Florida ("School 1"), but resigned in June 2023. Based on a review of open sources, it is believed that GORDO is now an art teacher at a second school located in Orange County, Florida ("School 2"), which has students ranging from kindergarten through 8th grade.

FORENSIC REVIEW OF CV's CELLUAR DEVICE

7. On September 25, 2023, the OCSO Digital Forensic Unit conducted a forensic examination of CV's Apple iPhone 14. On October 23, 2023, I reviewed the forensic report which stated that approximately 28 videos were located on CV's Apple iPhone 14 that depicted GORDO and CV engaged in sexual activity. The following is a brief description of three video files that were located on CV's Apple iPhone 14:

A: Title: IMG_8444.MOV

Date: June 17, 2023

Description: A 13 minute, 13 second, video file that depicted GORDO and CV engaging in mutual oral sexual activity and penile/vaginal sexual activity between them both. Based on GORDO's location and the location of the cellular device when the video recording started, it is likely GORDO was the person who set up the cellular device and started the recording prior to her sexual activity with CV in order to video record their sexual activity. The location appeared to be in a hotel room.

Metadata on the file showed it was produced with an Apple iPhone 14 and showed a location of Springs Colony Circle near I-4, in Altamonte Springs, Seminole County, Florida.

B: Title: IMG_8537.MOV

Date: June 26, 2023

Description: A 4 minute, 13 second, video file that depicted GORDO performing oral sex on CV and penile/vaginal sexual activity between them. Based on GORDO's location and the location of the cellular device when the video recording started, it is likely GORDO was the person who set up the cellular device and started the recording prior to her sexual activity with CV in order to video record their sexual activity. The location appeared to be in a hotel room.

Metadata on the file showed it was produced with an Apple iPhone 14 and showed a location of Universal Boulevard and International Drive, in Orlando, Orange County, Florida.

C: Title: IMG_8651.MOV

Date: July 8, 2023

Description: A 4 minute, 17 second, video file that depicted GORDO and CV engaging in digital penetration, CV performing oral sexual activity on GORDO and penile/vaginal sexual activity between them both. Based on GORDO's location and the location of the cellular device when the video recording started, it is likely GORDO was the person who set up the cellular device and started the recording prior to her sexual activity with CV in order to video record their sexual activity. The location appeared to be inside of a vehicle.

Metadata on the file showed it was produced with an Apple iPhone 14 and showed a location of US-192 and Black Lake Road, in Kissimmee, Osceola County, Florida.

8. There were also multiple video files recovered from CV's Apple iPhone 14 that depicted GORDO and CV engaged in sexual activity and that were created by a different cellular device, namely an Apple iPhone 11. For example, in one video recovered from CV's Apple iPhone 14 that was not filmed using CV's phone, GORDO and CV are near and/or before a mirror engaging in sexual activity, and an Apple iPhone 11 can be seen recording the encounter due to the mirror reflection. I believe based on this evidence that several videos of GORDO and CV engaged in sexual activity were recorded with GORDO's Apple iPhone 11 and later sent to CV's Apple iPhone 14.

9. On October 12, 2023, Seminole County Sheriff's Office Crimes Against Children Detective Patrick Rigaud-Colon conducted a recorded interview with CV who confirmed his sexual relationship with GORDO and stated the sexual activity occurred between June 2023 and September 2023. CV confirmed that the sexual activity took place inside a vehicle and multiple different hotels throughout Orange, Osceola, and Seminole Counties. CV stated GORDO was his teacher in 8th grade in 2019 at School 1 as well as his religious ambassador through School 1.

TECHNICAL TERMS

10. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This

storage media can contain any digital data, including data unrelated to photographs or videos.

c. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

d. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

11. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, material that has been viewed via the Internet is typically stored for a long period of time on the device. This information can often be recovered with forensics tools.

12. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the GORDO's electronic device(s) was used, the purpose of its use, who used it, and when they used it. There is probable cause to believe that this forensic electronic evidence might be on the device(s) because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

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

and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

13. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device(s) consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

USE OF BIOMETRICS

14. I request that the warrants permit law enforcement to compel GORDO to unlock any and all devices on her person requiring biometric access subject to seizure pursuant to the warrant. The grounds for this request are as follows:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices (like smartphones) and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password (hereinafter, "Biometric Access"). These biometric features include fingerprint scanners, facial

recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes, and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. In my training and experience, users of electronic devices often enable the biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. Based on my training and experience, I know that the majority of commercially available phones contain at least one form of biometric access. The passcode or password that would unlock the devices subject to search under the warrants currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the devices,

making the use of biometric features necessary to the execution of the search authorized by the warrants.

g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

h. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user of that device at

all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. I also know that, in some cases, a search may uncover circumstantial or direct evidence to support the conclusion about the identity of the user of given devices.

i. Due to the foregoing, if law enforcement personnel encounter a device that is subject to search and seizure pursuant to the warrant, and the device may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of GORDO to the fingerprint scanner of the device; and (2) hold the device in front of GORDO'S face and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search its contents as authorized by the warrants.

CONCLUSION

15. Based on the above information, there is probable cause that between June 2023 and September 2023, in the Middle District of Florida, GORDO knowingly produced child pornography in violation of 18 U.S.C. § 2251(a). I also submit that this affidavit supports probable cause for a warrant authorizing the search of GORDO to seek the items described in Attachment B for evidence of the following offenses: production of child pornography in violation of 18 U.S.C. § 2251(a), possession of child pornography in violation of 18 U.S.C. § 2252A(a)(5),

receiving and distributing child pornography in violation of 18 U.S.C. § 2252(a)(2), and coercion and enticement of a minor to engage in sexual activity in violation of 18 U.S.C. § 2422(b).

Eric Phillips, Task Force Officer
Federal Bureau of Investigation

Affidavit submitted by email and attested to me as true and accurate by telephone or videoconference consistent with Fed.R.Crim. P. 41(d)(3) this 25th day of October 2023.

HON. LESLIE HOFFMAN PRICE
United States Magistrate Judge