AO 91 (Rev. 11/11) Criminal Complaint (Rev. by USAO on 3/12/20) ☐ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Central District of California

United States of America

v.

BRYANT NAJERA GONZALEZ,

Defendant

Case No. 2:26-mj-00861-DUTY

CRIMINAL COMPLAINT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

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

On or about the dates(s) of April 9, 2025, through May 22, 2025, in the County of Los Angeles in the Central District of California, and elsewhere, the defendant(s) violated:

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

This criminal complaint is based on these facts:

Please see attached affidavit.

/s/ Shane Andersen
Complainant's signature

Shane Andersen, FBI Special Agent
Printed name and title

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

Date: 2/17/26

Judge's signature

City and state: Los Angeles, California

Hon. Margo A. Rocconi, U.S. Magistrate Judge
Printed name and title

AUSA: Joseph Guzman - x2438

AFFIDAVIT

I, Shane Andersen, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") in Los Angeles, California and have been so employed since May 2018. I am currently assigned to a counter-terrorism squad, where I work international and domestic terrorism and weapons of mass destruction issues. I attended 20 weeks of New Agent Training at the FBI Academy in Quantico, Virginia. Prior to joining the FBI, I worked in the United States Intelligence Community, conducting counterterrorism and foreign intelligence operations for more than nine years. As an FBI Special Agent, I have participated in multiple investigations regarding domestic terrorism, riots, and crimes against children to include internet-based sexual crimes. Through my training and experience, I have learned and used a variety of investigative techniques and resources, including surveillance, subpoenas, search warrants, evidence seizures, and analysis of telephone and other digital records. As a federal agent, I am authorized to investigate violations of laws of the United States, and as a law enforcement officer I am authorized to execute warrants issued under the authority of the United States.

II. PURPOSE OF AFFIDAVIT

2. This affidavit is made in support of a criminal complaint against and arrest warrant for Bryant Najera GONZALEZ

("GONZALEZ"), for violations of 18 U.S.C. § 2251(a), (e) (Production of Child Pornography).

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

a. The premises located at 8402 5th Street, Townhouse D, Downey, California 90241 (the "SUBJECT PREMISES"), as described in Attachment A-1;

b. A 2014 black Chevrolet Camaro with California license plate 7ESM766 (the "SUBJECT VEHICLE"), as described in Attachment A-2; and

c. The person of Bryant Najera GONZALEZ ("GONZALEZ") as described in Attachment A-3.

4. The requested search warrants seek authorization to seize evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 371 (Conspiracy); 18 U.S.C. § 2251(a), (e) (Sexual Exploitation of Children and Attempted Sexual Exploitation of Children); 18 U.S.C. § 2422(b) (Enticement of a Minor and Attempted Enticement of a Minor); 18 U.S.C. § 2252A(a)(2) (Distribution and Receipt of Child Pornography); 18 U.S.C. § 2252A(a)(5)(B) (Access with Intent to View and Possession of Child Pornography); and 18 U.S.C. § 875(b) (Interstate Threats) (the "Subject Offenses"), as described more fully in Attachment B. Attachments A-1 through A-3 and B are incorporated herein by reference.

5. The facts set forth in this affidavit are based on 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 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, and all dates and times are on or about those indicated.

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

6. In this affidavit, the terms "minor," "sexually explicit conduct," "visual depiction," "producing," and "child pornography" are defined as set forth in 18 U.S.C. § 2256. The term "computer" is defined as set forth in 18 U.S.C. § 1030(e)(1).

7. Based upon my training and experience in the investigation of child pornography, and information related to me by other law enforcement officers involved in the investigation of child pornography, I know the following information about the use of computers 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 ("ISP"), which operates a host computer with direct access to the Internet.

d. Internet Service Providers. Individuals and businesses obtain access to the Internet through 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 customers' 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. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in

real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

ii. "Chat room," as used herein, refers to the ability of individuals to meet in one location on the Internet in order to communicate electronically in real-time to other individuals. Individuals may also have the ability to transmit links to electronic files to other individuals within the chat room.

iii. "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.

iv. "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.

v. "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.

vi. "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).

vii. "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).

viii. "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.

ix. "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.

x. "File Transfer Protocol" ("FTP"), as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.

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

xii. 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.

xiii. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote

storage, and co-location of computers and other communications equipment.

xiv. An "Internet Protocol address" or "IP address," as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers ("ISPs") control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

xv. "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.

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

xvii. "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 game.

xviii. "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.

xix. "Remote computing service," as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

xx. "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.

xxi. 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.

xxii. "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.

xxiii. 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).

IV. Background on Nihilistic Violent Extremism ("NVE") and the "764" Network

8. Based on my training and experience and discussions with other FBI special agents, I understand the following about NVE and 764:

a. NVEs are individuals who engage in criminal conduct within the United States and abroad, in furtherance of political, social, or religious goals that derive primarily from a hatred of society at large and a desire to bring about its collapse by sowing indiscriminate chaos, destruction, and social instability. NVEs work individually or as part of a network with these goals of destroying civilized society through the

corruption and exploitation of vulnerable populations, which often include minors.

b. NVEs, both individually and as a network, systematically and methodically target vulnerable populations across the United States and the globe. NVEs frequently use social media communication platforms to connect with individuals and desensitize them to violence by, among other things, breaking down societal norms regarding engaging in violence, normalizing the possession, production, and sharing of Child Sexual Abuse Material ("CSAM") and gore material, and otherwise corrupting and grooming those individuals towards committing future acts of violence.

c. Those individuals are targeted online, often through synchronized group chats. NVEs frequently conduct coordinated extortions of individuals by blackmailing them so they comply with the demands of the network. These demands vary and include, but are not limited to, self-mutilation, online and in-person sexual acts, harm to animals, sexual exploitation of siblings and others, acts of violence, threats of violence, suicide, and murder.

d. Historically, NVEs systematically targeted vulnerable individuals by grooming, extorting, coercing, and otherwise compelling through force, or the threat of force, the victims to mutilate themselves or do violence, or threaten violence, to others, and either film or photograph such activity. The members of the network have edited compilation photographs or videos of targeted individuals and shared the

photographs and videos on social media platforms for several reasons, including to gain notoriety amongst members of the network, and spread fear among those targeted individuals for the purpose of accelerating the downfall of society and otherwise achieving the goals of the NVEs.

e. NVEs have adopted various monikers to identify themselves. The networks have changed names over time, which has led to the creation of related networks. Although the networks change names and use a variety of different social media platforms, the core members and goals remain consistent and align with the overarching threat of NVE.

f. 764 and related groups are NVEs who engage in criminal conduct within the United States and engage with other extremists abroad. The 764 network's accelerationist goals include social unrest and the downfall of the current world order, including the United States Government. Members of 764 work in concert with one another towards a common purpose of destroying civilized society through the corruption and exploitation of vulnerable populations, including minors.

V. SUMMARY OF PROBABLE CAUSE

9. Between approximately April 2025 and continuing through at least June 2025, through social media platforms, direct messaging, and other means of communication, GONZALEZ coerced, induced, and enticed minor children to create and send

to him CSAM. For example, at GONZALEZ's urging, Minor Victim 1[1] ("MV1"), a then-11-year-old girl, produced and sent to GONZALEZ at least one CSAM video. GONZALEZ possessed at least six CSAM videos and one CSAM image of MV1. After obtaining the sexually explicit videos and images of MV1, GONZALEZ then shared the CSAM with other users via the Internet on multiple occasions. At GONZALEZ's urging, Minor Victim 2 ("MV2"), a then-15-year-old girl, produced and sent to GONZALEZ at least four images of child erotica and several videos in which MV2 engaged in self-harm and self-humiliation. In communications with other online users, GONZALEZ has also discussed extorting minor victims, including by sending sexually explicit images to the victims' family members. Based on GONZALEZ's online activities, his coercion and enticement of minors to create CSAM and self-harm videos, and my training and experience, I believe GONZALEZ is associated with the nihilistic violent extremist ideology. As set forth below, GONZALEZ lives as the SUBJECT PREMISES and drives the SUBJECT VEHICLE.

VI. STATEMENT OF PROBABLE CAUSE

10. Based on my review of law enforcement reports, conversations with other law enforcement agents, and my own knowledge of the investigation, I am aware of the following:

A. A Tipster Informs the FBI that GONZALEZ Is Extorting Minors

[1] MV1 was listed as "VICTIM 3" in prior affidavits submitted for federal warrants to search digital devices, as discussed below. However, hereinafter they will be referred to as MV1.

to Produce CSAM and Self-Harm Videos and Images.

11. In May 2025, the FBI received a tip from an individual (the "Tipster")[2] who reported that the user of a social media account with the Discord display name[3] "netcat" ("NETCAT") was extorting minors to produce CSAM and self-harm images or videos and distributing those images to others on Discord. The Tipster provided information regarding NETCAT that allowed the FBI to identify GONZALEZ as the user of the display name NETCAT, including the following:

a. A screenshot that displayed one of NETCAT's accounts for what I refer to as "Discord Account 6."[4] As discussed below, through review of Discord records, the FBI concluded that GONZALEZ is the user of NETCAT's Discord Account 6.

b. A screenshot of a Discord chat that depicted a user with the display name "netcat" who attempted to entice

[2] The Tipster contacted the FBI on their own accord. The Tipster's identity is known to the FBI.

[3] A display name is how users primarily appear across Discord. Users can change their display name whenever they want. "Usernames," by contrast, are unique to each user and primarily serve as unique identifiers.

[4] As discussed below, law enforcement identified at least six Discord accounts operated by GONZALEZ.

Minor Victim 3 ("MV3")[5] to carve the cutsign[6] "netcat" into their leg. The chat included a photograph of a pair of thighs and a hand. The left thigh had over thirty lateral cuts that were bleeding. The right thigh had approximately ten smaller lateral cuts. The left hand was depicted with the palm up and blood visible on the fingers. Under the photograph was the following chat message:

GONZALEZ: still?!

MV3: yep

MV3: I'll do it later

GONZALEZ: yeah netcat in big letters mmm

c. A photograph depicting a female victim believed to be MV3, who appeared to be a minor, with the fansign "NETCAT" written in marker multiple times on her neck, chest, and shoulders.

d. A screenshot from commercial messaging application Telegram that appears to be a Telegram channel

[5] The female was previously listed as "VICTIM 1" and "VICTIM 2" in prior affidavits submitted for federal warrants to search digital devices, as discussed below. However, through additional investigation, I have concluded that VICTIMS 1 and 2 are the same person and hereinafter will be referred to as MV3.

[6] Based on my training and experience, I know that a "fansign" is a photograph of a person with an inscription written on the body, wall, or a piece of paper, used on the internet as an autograph or as a means to show acquiescence towards a specific individual. Similarly, a "cutsign" is a fansign that is carved into the skin as opposed to being written on the body, wall, or piece of paper. Lorebook victims are often extorted into creating fansigns for their abusers, who are often members of NVE groups.

titled "NETCAT LOREBOOK."[7] The screenshot contains two photographs of an individual that the Tipster reported to be named "Bryant" (the true first name of GONZALEZ). The FBI compared the photographs of "Bryant" to DMV photographs of GONZALEZ and concluded that GONZALEZ is the individual in the photographs in the NETCAT LOREBOOK. The screenshot additionally contained text that read:

> Netcat/Sypebf is an ugly, disgusting, degenerate, brown, pedophilic e-boy who is notoriously known for being a grotesque femboy, cp spreader, sex pest, making girls cut themselves on cam and wasting money on e-whores. (when he should be saving it to get surgery for his disgusting kike nose) /Here's proof of him literally ADMITTING to extorting said 12 year old girl. / In the first photo, he's showing another equally weird ass person CP of the 12 year old to sell it. In the second photo, he's sending the same video to another weirdo to eventually extort her.
>
> (Errors in original.)[8]

e. Personal identifying information for "Bryant," including his name, age, location, and phone number that they attributed to "Bryant." The FBI compared the information for "Bryant" to known information for GONZALEZ and determined that the information matched.

B. The FBI Identifies And Executes Search Warrants On Additional Social Media Accounts Used By GONZALEZ That Are

---

[7] Based on my training and experience, I know that a "lorebook" is a collection of materials of "lore" about a perpetrator or victim stored in one location, such as a Telegram channel or Discord server. A lorebook is typically made exclusively to store information, photographs, videos, social media accounts, or other information about an individual as compromising or embarrassing leverage against that individual.

[8] Throughout this affidavit, all quotations from messages contain the errors as made in the original messages.

Engaged In The Enticement, Production, Receipt, And/Or Distribution Of CSAM.

12. As discussed below, through analysis of subscriber records, IP addresses, National Center for Missing and Exploited Children ("NCMEC") records, and other records, the FBI concluded that GONZALEZ operated at least six Discord accounts and an Instagram account (the "Instagram Account").

13. I obtained and reviewed subscriber records for Discord Account 1. The subscriber records for Discord Account 1 identified the SUBJECT PREMISES as the billing address and listed "netcat" as an associated display name. The subscriber records also showed that the user of Discord Account 1 regularly connected to Discord through IP address 47.154.241.150 (the ".150 IP Address").

a. I obtained and reviewed subscriber records for the .150 IP Address and learned that the subscriber for the .150 IP Address was a male located at the SUBJECT PREMISES. Based on the above, as well as my training and experience and knowledge of this investigation, I believe that the male is GONZALEZ's father or another male relative.

14. I obtained and reviewed subscriber records for Discord Account 2. The subscriber records for Discord Account 2 listed "netcat" as an associated display name and showed that the user of Discord Account 2 regularly connected to Discord through the .150 IP Address.

15. I obtained and reviewed subscriber records for Discord Account 3. The subscriber records for Discord Account 3

identified the SUBJECT PREMISES as the billing address and listed "netcat" as an associated display name. The subscriber records showed that the user of Discord Account 3 regularly connected to Discord through the .150 IP Address.

a. The subscriber records also showed that the user of Discord Account 3 at times connected to Discord using IP address 174.227.66.239 (the ".239 IP Address"), including at one time when the user of Discord Account 3 uploaded a suspected CSAM video to Discord.

b. I reviewed Verizon records from the .239 IP Address and learned that the .239 IP Address was used by the phone number 562-632-6871 (the "6871 Number") during the time the CSAM video referenced in the immediately preceding paragraph was uploaded.

c. I reviewed Verizon subscriber records for the 6781 Number and observed that the subscriber of the 6871 Number was a female located at the SUBJECT PREMISES. Based on my training and experience and knowledge of this investigation, I believe that the female is GONZALEZ's mother or female relative and that GONZALEZ used the 6871 Number.

16. I reviewed subscriber records for Discord Account 4. The subscriber records for Discord Account 4 identified the SUBJECT PREMISES as the billing address and listed "netcat" as an associated display name. The subscriber records also showed that the user of Discord Account 4 regularly accessed the internet via the .150 IP Address.

17. I reviewed subscriber records for Discord Account 5. The subscriber records for Discord Account 5 identified the SUBJECT PREMISES as the billing address and listed "netcat" as an associated display name.

18. I reviewed subscriber records for Discord Account 6. The subscriber records for Discord Account 6 identified the SUBJECT PREMISES as the billing address and listed "netcat" as an associated display name. The subscriber records showed that the user of Discord Account 6 regularly connected to Discord through the .150 IP Address.

19. I reviewed subscriber records for the Instagram Account. The subscriber records for the Instagram account listed the 6871 Number and a Gmail account (the "Gmail Account") as account identifiers.

a. I reviewed subscriber records for the Gmail account. The Gmail subscriber records revealed that GONZALEZ was the subscriber of the Gmail Account and listed the 6871 Number on the account.

20. On November 10, 2025, the Honorable Steve Kim, United States Magistrate Judge for the Central District of California, in Case Nos. 2:25-mj-6992 and 2:25-mj-6993, issued federal warrants to search Discord Accounts 1-6 and the Instagram Account. As discussed further below, during my review of the contents of GONZALEZ's Discord Accounts and the Instagram Account, I observed multiple instances of GONZALEZ's accounts receiving, uploading, and distributing CSAM, as well as evidence

that GONZALEZ coerced minors into producing CSAM and related self-harm material.

C. FBI Receives NCMEC Reports Regarding GONZALEZ's Receipt and Distribution of CSAM on Several of GONZALEZ's Social Media Accounts.

21. Based on my training and experience, I know that the NCMEC functions as a national clearinghouse for information on missing and exploited children and the sexual exploitation of children. ESPs and members of the public can report suspected child exploitation to NCMEC through its CyberTipline. ESPs include companies such as Discord and Meta Platforms, which provide free and paid services online. These services may include email, instant messaging, social networking, and online file transfer or storage. NCMEC provides information to law enforcement agencies through CyberTipline Reports. I also know ESPs may discover suspected child exploitation files through user reports, automated scanning of a hash value[9] associated with a particular file depicting child pornography, and other methods.

22. During the course of this investigation, as discussed below, FBI received several NCMEC reports related to several of

[9] A "hash value" is a numerical identifier for digital data, such as a particular file. It is obtained by using a mathematical function, often called an algorithm. When a hash value is generated for an image file, any other identical image file will have the same hash value. However, if the data is changed, even very slightly (such as the addition or deletion of a single pixel in an image), the hash value will change. Thus, a hash value can be thought of as a "digital fingerprint" for data -- if two images have the same hash value, there is an extremely high likelihood that the images are the same.

GONZALEZ's Discord Accounts and the Instagram Account. These reports showed that GONZALEZ's social media accounts were used to receive, upload, and distribute CSAM, and to coerce minors into producing CSAM and related self-harm material.

D. GONZALEZ Produced, Possessed, and Distributed Videos of MV1 Using Discord Account 1.

23. On April 9, 2025, NCMEC received Cyber Tip ("CT") Report 208901166 from Discord, which the FBI received and reviewed in September 2025. CT Report 208901166 shows that GONZALEZ, using Discord Account 1, uploaded the following videos to a Discord Server on April 9, 2025, at 04:13:40 UTC:

a. A video titled "SPOILER_20250407_161518.mov" and identified with hash value 3e66ca1fb9e8c91553016823eb152c98 ("CSAM Video 1"). CSAM Video 1 is a 34-second video that appeared to depict a prepubescent female with blonde hair between the approximate ages of 9-11 years old (i.e., MV1). MV1 was nude and seated on the floor facing the camera. She is naked and visible from her head down to her vagina. Her legs were bent at the knees and spread to expose her vagina. She licked the fingers of one hand then proceeded to masturbate by rubbing and inserting her fingers inside her vagina. At 29 seconds, she used her fingers to spread her labia and expose her vagina to the camera. At 31 seconds, she removed her fingers from her vaginal area, licked them, leaned forward, and reached for the camera. The video ended immediately thereafter. The video contained sound, but no words were spoken or heard.

b. A video titled "SPOILER_20250407_161309.mov" and identified with hash value 646f2ecdeb5136aaf629ccf4fb3542c4 ("CSAM Video 2"). CSAM Video 2 is a 29-second video that also appeared to depict MV1. MV1 was nude and stood facing the camera with her head down to her knees in the frame. At 1 second, she turned around, placed her hands on her buttocks and exposed her anus and vagina directly toward the camera. At 6 seconds, she turned back around, got on her hands and knees, and crawled toward the camera. At 13 seconds, she came to her knees, centered her bare breasts toward the camera, and used both hands to touch her breasts. She stood and, at 23 seconds, she lifted one of her legs to expose her vagina. At 27 seconds, she lowered her leg, leaned toward the camera and made a heart shape with her fingers, before she reached toward the camera; the video ended immediately after. The video contained sound, but no words were spoken or heard. Several red lateral scratches and/or healed cuts appeared visible on both thighs.

c. A video titled "SPOILER_20250407_135021.mov" and identified with hash value a942c874e370cb80f9c7bd866708a1a0 ("CSAM Video 3"). CSAM Video 3 is a 22-second video that also appeared to depict MV1. She stood facing the camera, and the frame showed her body from head to mid-calf area. She wore a black and white striped, long-sleeved top and black shorts with white piping and a white drawstring. At 1 second, she waved at the camera and began to remove her top, shorts, and underwear; she was not wearing a bra. She stood nude with her breasts and pubic area exposed, and turned twice to expose her buttock.

Several red lateral scratches and/or healed cuts were visible on both thighs. At 20 seconds, she leaned forward toward the camera and said, "Hey, NETCAT" before the video ended.

24. I also reviewed Discord records obtained pursuant to the Discord search warrant described above. My review of those records showed that on April 9, 2025, between 03:13:07 UTC and 03:48:53 UTC, GONZALEZ engaged in a direct message chat with MV1, directing MV1 to produce another video:

25. For example, on April 9, 2025, GONZALEZ, using Discord Account 1, engaged in a direct message chat with MV1 on Discord, stating the following at 03:34:44 UTC:

> i wanna see you on yr back.. with your legs up also flat on ur belly ass up.. just show yourself off.. I like when you do it freely its so cute watching you do that and just say my name or something youd look so cute in so many poses I have in mind , youre gonna turn me into a perv..

26. On April 9, 2025, at 03:40:14 UTC, MV1 sent a video that contained suspected CSAM material ("CSAM Video 4"). The video, titled 5668909086_1359380719356350674_20250409_133819, was 27 seconds in length and depicted MV1. MV1 was naked and laid on her back on a bathroom floor. She lifted her legs up then rolled onto her stomach and arched her back. MV1 then faced the camera and posed on her side. She walked her hands forward toward the camera and laid her head on the floor close to the camera lens. The focal point of the video was MV1's naked body; to include her breasts and pubic area. Several red lateral scratches and/or healed cuts appeared visible on her thigh.

27. Eight minutes later, at 03:48:06 UTC, GONZALEZ wrote: "I feel like a perv fuck asking you this lolz/you are a cute lil fuck doll look at you./you are beaut."

28. Also on April 9, 2025, shortly after receiving CSAM Video 4, GONZALEZ engaged in a direct message chat with Discord User 1. At 04:13:41 UTC, in a single direct message GONZALEZ sent eight videos and two images to Discord User 1. The videos included CSAM Videos 1-4 and the following:

a. A video titled 1351811093047152726_1359380725668909086_1359380721084399638_SPOILER_20250407_161715 ("CSAM Video 5") that was 26 seconds in length and depicted MV1. MV1 was naked, on her knees, and centered in frame. She moved her face close to the camera and opened her mouth. She then squeezed her exposed breast before she moved closer to the camera and kissed the lens. MV1 moved back on her knees and centered her bare breasts and pubic area in frame. She again placed her hands on her exposed breasts before the video ended. The focal point of the video was MV1's exposed breasts and pubic area.

b. An image titled _1359380720195469333_rn_image_picker_lib_temp_6ca3e24c-a4b4-4600-8762-76562ffd1846 that depicted a prepubescent female with blonde hair between the approximate ages of 9-11 years old and assessed to be MV1. MV1 stood naked and covered her breast with her hand. Her bare pubic area was visible in the image.

c. A video titled 1351811093047152726_1359380725668909086_1359380723546722314_809C

C8E1-6368-4862-9210-0FD2EE05DA72 that was two seconds in length and depicted a Hispanic or Asian female between the approximate ages of 14-16. She was centered in the camera frame with her breasts exposed. She held a piece of notebook paper that contained a fansign which read, "netcat owns me." The paper had three hearts drawn around the words.

29. Also, on April 9, 2025, GONZALEZ engaged in a direct message chat with Discord User 2. In that chat, at 02:16:02 UTC, GONZALEZ sent a one-second video that appeared to be the final second of CSAM Video 3, in which MV1 says, "Hey, NETCAT". Immediately after the video was sent, the following chat occurred:

> GONZALEZ (02:16:34 UTC): hold on I cropped the video Ill send the full idk why its not sending nga
>
> Discord User 2 (02:16:57 UTC): nigga ure retarded if u think shes 14…
>
> Discord User 2 (02:30:58 UTC): and u think shes 14/shes obv 10-11

30. On April 16, 2025, GONZALEZ engaged in a direct message chat with Discord User 3, stating the following:

> GONZALEZ (10:53:39 UTC): this is that girl/wait til the end
>
> [GONZALEZ attached CSAM Video 3, i.e, the video in which MV1 says, "Hey, NETCAT", to the above message.]
>
> Discord User 3 (10:57:25 UTC): brooo she looks 9/im hard
>
> Discord User 3 (11:02:37 UTC): do you have more of her

GONZALEZ (11:03:40 UTC): Yeah I do/I got some good videos here/shes such a whore/she told me shell do anything I want/Fuck I could've gotten her on cam too but then I got banned

31. During the same chat with Discord User 3, on April 16, 2025, at 11:04:52 UTC, GONZALEZ sent a video titled 1361992805987254493_1362020921812062288_1362020921371656242_20250407_121107 ("CSAM Video 6") that was 9 seconds in length and depicted MV1 standing center frame. She wore a striped black and white long sleeve shirt and black shorts with white piping. MV1 undressed and stood nude in front to the camera. MV1's breasts and pubic area were visible.

32. After GONZALEZ sent CSAM Videos 3 and 6, the chat continued:

GONZALEZ (11:05:09 UTC): See her tits/there like fucking/Not tits theyre just nips

GONZALEZ (11:06:06 UTC): shes aussie

Discord User 3 (11:06:21 UTC): do u have vids of her playing with her pussy

GONZALEZ (11:06:29 UTC): Yeah here lmao

GONZALEZ (11:06:57 UTC): shes such a whore its insane/ Like she knows toooo much for anfucking eleven year old

33. GONZALEZ attached to the above message a video titled, 1361992805987254493_1362020921812062288_1362020920591519834_SPOILER_20250407_161715. That video was 26 seconds in length and

appeared to be CSAM Video 5. He then exchanged the following messages:

GONZALEZ (11:06:58 UTC): She has a nice cunt

GONZALEZ (11:11:11 UTC): But yeah this bitch is insnsNe for an 11 bro

34. On April 16, 2025, NCMEC received CT Report 209468984 from Discord, which the FBI received and reviewed in September 2025. Per the report, on April 9, 2025, at 11:06:57 UTC, GONZALEZ, using Discord Account 2 and the .150 IP Address from the SUBJECT PREMISES, uploaded CSAM Video 1 (hash value 056645381ee4dc7432fcd0cc4e681d55) and CSAM Video 3 (hash value b38d2deda744f8550efad7980dc3b365) to a Discord server. GONZALEZ sent these videos at the same time he sent CSAM Video 5 to Discord User 3, as described in paragraph 33. CSAM Video 1 and 3 do not appear in the chat message sent at 11:06:57 UTC, and it is assessed that Discord prevented their transfer due to the videos' hash values being identified as suspected CSAM.

35. On April 19, 2025, Discord sent NCMEC CT Report 209627216, which the FBI received and reviewed in September 2025. The FBI's review of the CT Report and attached video file revealed that on April 16, 2025, at 14:06:02 UTC, GONZALEZ used the .239 IP Address to upload what appeared to be the final second of suspected CSAM Video 3 (in which MV1 says, "Hey, NETCAT"). That video was titled, SPOILER_20250407_135021.mov (hash: 648fb4638fb77d84187a4f816769f988). This was confirmed through a Discord conversation designated 1362371487666798603, which had 95 participants, and that I obtained from the November

10 Warrant. In that chat, at 14:06:02 UTC, GONZALEZ sent a one second video titled, 1362371487666798603_1363153676880969788_1363153676524589066_SPOILER_20250407_135021 that appeared to be the same video clip of CSAM Video 3 (in which MV1 says "Hey, NETCAT"), as referenced above in NCMEC CT Report 209627216.

36. In November 2025, Australian law enforcement authorities reported to the FBI that they identified MV1 as a female born in 2013. According to those reports, MV1 was 11 years old when CSAM Video 4 was produced.

E. GONZALEZ Enticed MV2 to Produce CSAM and Engage in Self-Harm.

37. On June 4, 2025, NCMEC received CT Report 213266429 from Discord, which the FBI received and reviewed in September 2025. According to the NCMEC report, MV2, a 15-year-old female, reported to Discord that she met "Bryant" (later determined to be GONZALEZ) on Discord when she was fourteen and he was twenty-two. MV2 described that "Bryant" was a Hispanic male from California, and that they became online friends but never met in person. MV2 considered "Bryant" her "online partner/boyfriend" and told him about her life and the problems she faced. MV2 told "Bryant" she was fifteen years old, to which "Bryant" responded that he liked the age gap and how "young and little" MV2 was. Using his knowledge of MV's personal and emotional details, "Bryant" used "emotional manipulation" to get MV2 to send him "inappropriate sexual videos and pictures" of MV2 and made MV2 engage in self-harm. MV2 reported that "Bryant" used

the 6871 Number and the usernames for Discord Account 6 and the Instagram account.

38. In January 2026, Italian law enforcement authorities reported to the FBI that they spoke to the father of MV2, and confirmed the accuracy of the information MV2 reported to NCMEC.

39. I reviewed the November 10 warrant information for Discord Account 6, and noted in a Direct Message conversation on May 22, 2025, GONZALEZ and MV2 engaged in the following conversation:

> GONZALEZ (07:50 UTC): go grab/a pair of white underwear and write my name on it okkay? And, ut it over your face. Thnk
>
> MV2 (07:51 UTC): il write/BRYANT
>
> GONZALEZ (07:51 UTC) perma marker/LMAO NO/Fuck it…/Yes actually yeah do/that 'on the back, and netcat on the front. There's two sides ;x
>
> GONZALEZ (07:52 UTC): Bryant will be on yr butt side.
>
> MV2 (07:55 UTC): Oki I did it/But had to hide it/Il take the pic when my mom lesved me alone for a sec
>
> GONZALEZ (07:56 UTC) lmfao. Imagine she saw you doing it/who tf is Bryant netcat
>
> GONZALEZ (08:16 UTC): Grr..take a pic and video w the underwear and paci in yr mouth w no top on
>
> MV2 (08:36 UTC): I took some

40. At 08:41 UTC, on May 22, 2025, MV2 sent three photographs in the chat as described and directed by GONZALEZ: the first photograph depicted a close-up of a female's face from

her nose to below her chin. She had curly brown hair and had a My Little Pony pacifier in her mouth; the second photograph depicted a topless female 12-15 years old. She wore light-colored underwear with "Nectcat" and a heart written in ink on the pubic area of the underwear. Her breasts were exposed, and one nipple was covered with a Hello Kitty sticker. Her face was not visible; the third photograph depicted a close-up of a female's face from below her nose to her exposed cleavage. She had curly brown hair and had a My Little Pony pacifier in her mouth.

41. The chat continued after MV2 sent the three pictures described in paragraph 40. At 08:48 UTC, GONZALEZ wrote: "Ugh remove the hellow kitty u lil tease."

42. At 08:51 UTC, MV2 sent a photograph similar to the second photograph described above; however, the Hello Kitty sticker was removed and exposed both breasts and nipples.

43. Later on May 22, 2025, the chat continued:

> MV2 (11:22 UTC): IM SDILL NOT OVER THIS PICFURE
>
> [an attachment was sent but did not appear in chat]
>
> MV2 (11:33 UTC): WHY DID UR EYES LOOK SO BIG
>
> GONZALEZ (11:34 UTC): yeah yeah be lucky. 99% of groomies don't get to see their groomers cause that's bad opsec, and FEDDEDDD[10]. when I leave you you won't have much pics of me heh. THE OFFICERS WONT Know who I am. I will shave my hair off by then. LMAO"

[10] "Fedded" is a term commonly used to refer to an individual subject to federal law enforcement action.

GONZALEZ (11:34 UTC): I kinda opened them wide/on purpose to mock you/Don't post this ee/Ew

MV2 (11:46 UTC): ALSO BRUH U LOOKED LIKE A GIRL

GONZALEZ (11:46 UTC): groomers don't, it's a liability it's a risk, It's FEDD VILE/it's JAIL CENTRAL/LMAO

MV2 (11:47 UTC): sometimes thyed get doxxed[11] tho/by other people

GONZALEZ (11:48 UTC): Some yeah tbh most just yeah don't wanna get fedded LMAO. Like it's just true no groomer or pedo will willingly do that unless they're extrmely in love or infactuated w their "victim" 😭 Cause it's literally jail tiken LMAO

44. The chat continued later that day as follows:

GONZALEZ(13:07 UTC): paci in yr pussy./nowput the paci inf your kid pussy

GONZALEZ (13:08 UTC): I wanna see the pacifier you had as a lil baby in your child cunt/put it in your mouth after"

GONZALEZ (13:09 UTC): A video btw

MV2 (13:09 UTC): Yeah holdon il use the insta[12] cam/play once

GONZALEZ (13:09 UTC): FUCK/you/[MV2's display name]

MV2 (13:10 UTC): Yeah rape me/pls

---

[11] Doxxed is a when an individual's private or identifying information is published on the Internet, typically with malicious intent.

[12] "Insta" is a term commonly used to refer to Instagram.

GONZALEZ (13:10 UTC): Stupid slut/Well I have yr address/okay wait/So listen on

GONZALEZ (13:11 UTC): Paci in yr mouth first..so there's a lot of saliva being collected..

GONZALEZ (13:13 UTC): stick it out. And slide it in you. <3 and say netcats kid cunny/ no that's too far mmm LMAO/netcatttts princess no that's corny UGH/Nyways then stuff it in your mouth c; and move it around..

45. In the same chat on June 1, 2025, at 11:09 UTC, GONZALEZ provided MV2 with the 6871 Number to "FT" them.[13]

46. Additionally, GONZALEZ directed MV2 to produce videos and images of self-harm and self-humiliation. On May 19, 2025, GONZALEZ engaged in a direct message chat with MV2 on Discord. During the chat, GONZALEZ directed MV2 to video record herself lick a toilet bowl and slap herself in the face. GONZALEZ and MV2 exchanged the following messages:

GONZALEZ (15:32:35 UTC): [MV2's display name] i wantyou to lick yr toilet seat

MV2 (15:36:20 UTC): How is this hot/id it cu sim doing something disgusting for u

GONZALEZ (15:36:49 UTC): bc i love to see you be cute and humiliate yrself

[13] Based on the context of the conversation, I believe GONZALEZ and MV2 were conducting a video chat outside of the Discord application.

MV2 (15:41:14 UTC): Do u still want me to lick da toilet

GONZALEZ (15:41:50 UTC): the actual toilet btw. not the seat/lift up the seat

GONZALEZ (15:42:23 UTC) bro how do italian toilets look like

GONZALEZ (15:44:55 UTC): good little girl, just prop yr phone up ig. oh and take your top and bottoms off okay [MV2's first name].

GONZALEZ (15:44:56 UTC): don't do it yet, tell me before u do it

MV2 (15:45:19 UTC): CLOTHES OFF?

GONZALEZ (15:45:25 UTC): obviously/youll need it off for the other video anyway

47. At this point, for several minutes GONZALEZ directed MV2 on how to hold the phone and record the video. GONZALEZ then wrote:

GONZALEZ (16:00:47 UTC): don't be super zoomed in/I want to see your tiny body

MV2 (16:11:22 UTC): I took the vid

GONZALEZ (16:11:55 UTC): mmm send it

48. At 16:24:00 UTC, MV2 sent GONZALEZ three videos of her licking a toilet bowl. The first video, titled 1372615424390463511_1374060031858708593_1374060030420324352_IMG_0267, was one second in length and depicted MV2 licking a toilet. The frame was focused on her face and toilet. She wore dark makeup around her eyes. The second video, titled

1372615424390463511_1374060031858708593_1374060031527620698_IMG_0259, was also one second in length and depicted MV2 licking a toilet, as described above. The third video, titled 1372615424390463511_1374060031858708593_1374060031019847681_IMG_0260 was a half-second video that depicted MV2 licking a toilet, as described above.

49. The chat continued after MV2 sent GONZALEZ the three above-described videos:

MV2 (16:24:19 UTC): Never doing again sybau

GONZALEZ (16:24:27 UTC): Did it wrong/Again

GONZALEZ (16:25:06 UTC): Like dont put it so close to your face

MV2 (16:25:55 UTC): IL make a vid with my body/I dont wanna lick the oitlet again

GONZALEZ (16:25:59 UTC): No/grr/Youll wash yr mouth after anyway, get it out of the way

MV2 (16:26:27 UTC): Ok waif

GONZALEZ (16:26:47 UTC): Take everything off

GONZALEZ (16:28:56 UTC): oh and when you lick it. Say im sorry netcat

50. At 16:35:05 UTC, MV2 sent GONZALEZ two videos of her licking a toilet bowl. The first video titled, 372615424390463511_1374062821037441088_1374062820697833573_IMG_0270 was three seconds in length and depicted MV2 with her head close to a toilet bowl. MV2 was topless, and her breasts were centered in frame. She leaned forward and licked the toilet bowl as she looked directly into the camera. The second video,

titled 1372615424390463511_1374062821037441088_1374062821184114688_IMG_0275, was one second in length and depicted MV2 licking a toilet. The frame was focused on her face and toilet. She wore dark makeup around her eyes.

51. At 16:50:24 UTC, GONZALEZ, told MV2 to "oh and give yrself a lil slap on the face/love tap/from me." At 16:59:14 UTC, MV2 sent two videos of her engaged in self-harm. The first video titled, 1372615424390463511_1374068900857253918_1374068900173447308_IMG_0279, was 3 seconds in length and depicted MV2 with black makeup on her nose, around her mouth, and diamond shapes around her eyes; like a clown. MV2 said, "I'm sorry Netcat" and slapped herself in the face. The second video, titled, 1372615424390463511_1374068900857253918_1374068900572037322_IMG_0283, was 1 second in length and depicted MV2 with the same makeup as described above. In that video, MV2 delivered three forceful punches to her face.

F. GONZALEZ Discusses Extorting Victims

52. As discussed in detail below, during my review of some of GONZALEZ's Discord Accounts, I observed GONZALEZ discussing the extortion of several victims, including minor victims. Based on these conversations, I believe GONZALEZ may be extorting victims.

53. For example, based on my review of the November 10 warrant information for Discord Account 1, I observed a Direct

Message conversation on April 6, 2025, in which GONZALEZ and Discord User 2 engaged in the following conversation:

GONZALEZ (20:16 UTC): potential / uhh / extort victim lmfaoo / her names [Minor Victim 4's ("MV4") display name] / vids of her being ate by her dog out LMAOO / and like look

Discord User 2 (20:16 UTC): SHOW ME

GONZALEZ: shes actually terrified

a. At 20:16 UTC, GONZALEZ sent a 40-second video of a Discord chat screen recording between MV4 and Discord User 4. In the recording, a female voice that I believe belongs to MV4 was heard confronting Discord User 4. MV4 cried and said, "I'm getting fucking fedded, they found my school, I'm going to fucking kill myself this week, I have no choice…this is all your fucking fault, you're an asshole." Discord User 4, a male voice with an English accent responded, "I'd say its Matt's fault as well, not just my fault." MV4 then said, "You literally just ruined my fucking life…by the way it's child porn."

b. GONZALEZ and Discord User 2 then exchanged the following messages:

GONZALEZ (20:16 UTC):

lmfaooooooooooooooooooooooooooooooo / someone found her school / kiwiland, [display name] / lmfaooooo / ate out by her dog / n now shes fuckign scared / LMAO

GONZALEZ (20:17 UTC): now tht her shit got found out though

Discord User 2 (20:17 UTC): what she look like

GONZALEZ (20:17 UTC): her school / she so scared/she looks like a white girl w glasses / I gotta find a pic uh

Discord User 2 (20:17 UTC): ok / idc / lets extort

c. At 20:18 UTC, GONZALEZ sent a nine-second video titled, 1355202083971797063/1358536248355979314/0Ou9Ip7.mp4. The video depicted a small black and white dog licking the vagina of a female. GONZALEZ then sent a second video, titled, 1355202083971797063/1358536275170168852/axbCDiZ.mp4. That video was nine seconds in length and depicted a female on a bed. Her bare pubic area was centered in frame, and her legs were spread and bent at the knees. The small black and white dog in the previous video was down by MV4's feet. Also on the bed was a similar sized tan dog. The black and white dog got up and walked to MV4 and proceeded to lick her exposed vagina.

d. GONZALEZ and Discord User 2 then exchanged the following messages:

GONZALEZ (20:18 UTC): the way the doog comes to her BRO / lmaoooo

Discord User 2 (20:21 UTC): how old is ss he

GONZALEZ (20:21 UTC): 17 I think / lmao when shes like / "that's child porn idc"

54. Based on my review of the November 10 warrant information for Discord Account 4, I observed a Direct Message conversation on April 26, 2025, in which GONZALEZ and Discord User 5 engaged in the following conversation:

Discord User 5 (17:17 UTC): some egirl / I have their doxx / [Minor Victim 5's ("MV5") display name]

GONZALEZ (17:18 UTC): how she look like

Discord User 5 (18:25 UTC): On ig / Their doxx is priv

GONZALEZ (17:18 UTC): im down / lmao / ddi the guy extort her

Discord User 5 (17:19 UTC): Nb extortrd her yet

GONZALEZ (17:19 UTC): damn

Discord User 5 (17:19 UTC): we the first

GONZALEZ (17:19 UTC): if she had a nude leak it would be sm easier too / cus look / her friend / lmao

a. At 17:19 UTC, GONZALEZ sent an image from Instagram that depicted two females between the approximate ages of 14 and 16 years old. The females were in an arcade and sat on a motorcycle that was part of a video game. GONZALEZ and Discord User 5 then exchanged the following messages:

Discord User 5 (17:19 UTC): We have her full info

GONZALEZ (17:19 UTC): can say "we;ll send it to yr friends" / blah blah

Discord User 5 (17:20 UTC): I have her addy n name n shit

GONZALEZ (18:28 UTC): lmfao / make a gc / w my alt / when yr down to do it

55. Based on my review of the November 10 warrant information for Discord Account 4, I also observed a Direct Message conversation on April 27, 2025, in which GONZALEZ and Discord User 6 engaged in the following conversation:

GONZALEZ (08:37 UTC): Did [Discord User Name] disappear

Discord User 6 (08:37 UTC): I mede her quit / every server / she fears me so much / that it make sm hard / LMFAO

GONZALEZ (08:38 UTC): What did you get from her lmao

Discord User 6 (08:38 UTC): some vids / but now its getting boring / I could literally spam all her shit

GONZALEZ (08:38 UTC): send it

Discord User 6 (08:38 UTC): to the whole family

GONZALEZ (08:38 UTC): ll extort her w someone

Discord User 6 (08:39 UTC): shes on twitter and insta

Discord User 6 (08:41 UTC): her face?

a. At 08:41 UTC, Discord User 6 sent an image in the chat that depicted a female between the approximate ages of 14 and 17 years old. GONZALEZ and Discord User 6 then exchanged the following messages:

GONZALEZ (09:05 UTC): Send the stuff..;p / On tele? / also / have you extorted her like gotten her on cam / do yk her friends social

Discord User 6 (09:13 UTC): everything / she shows only her body / or pussy / shes ashamed of her face / I sell that shit

G. GONZALEZ's Activities Are Consistent with NVE Ideology

56. Based on my training, experience, and conversation with other law enforcement officers, I believe there is probable cause to establish that GONZALEZ's activities are consistent

with NVE ideology. Namely, GONZALEZ groomed at least two minor victims to produce self-harm, self-humiliation videos, fansigns, and/or CSAM videos and images. GONZALEZ shared those CSAM videos with others in online chatrooms. GONZALEZ participated in chats where 764 promotional materials were sent and NVE topics were discussed (e.g., extortion, grooming, CSAM, fansigns, cutsigns, doxxing, self-harm, self-humiliation, and known NVE victims and subjects). GONZALEZ possessed fansigns of multiple victims with his Discord display name and encouraged another to produce a cutsign with this Discord display name.

H. GONZALEZ Lives at the SUBJECT PRESMISES and Drives the SUBJECT VEHICLE.

57. Between May 2025 and January 2026, I reviewed records from the California Department of Motor Vehicles, as well as bank records, United States Postal Service records, police reports, phone records, and internet subscriber records for GONZALEZ, all of which list the SUBJECT PREMISES, and only the SUBJECT PREMISES, as GONZALEZ's current residence.

58. I reviewed video surveillance and surveillance reports from November 2025 and January 2026 that documented GONZALEZ was consistently at the SUBJECT PREMISES and in operation of the SUBJECT VEHICLE (7ESM766).

59. I reviewed California Department of Motor Vehicles information for the SUBJECT VEHICLE. California Department of Motor Vehicle records listed the registered owner as a female at the SUBJECT PREMISES, with a name similar to the phone subscriber and believed to be GONZALEZ's mother.

60. I spoke to an Agent who had access to locational data from GONZALEZ's cellular phone, and determined the following: between January 9 and February 13, 2026, GONZALEZ's cellular phone consistently pinged around the SUBJECT PREMISES. GONZALEZ's movements away from the SUBJECT PREMISES were corroborated by comparing surveillance reports and his cellular phone ping data.

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

61. 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.

62. 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.

63. 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 or on his 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 could lead to evidence of child exploitation offenses.

VIII. TRAINING AND EXPERIENCE ON DIGITAL DEVICES[14]

64. 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. 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

[14] 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.

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.

b. 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.

c. 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.

d. 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.

65. 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.

66. The search warrant requests authorization to use the biometric unlock features of a device, 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. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress the SUBJECT PERSON's thumb and/or fingers on the device(s); and (2) hold the device(s) in front of the SUBJECT PERSON's face with his eyes open to activate the facial-, iris-, and/or retina-recognition feature.

IX. REQUEST FOR SEALING

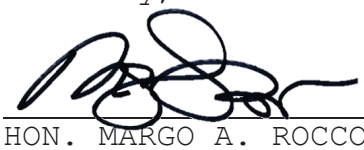
67. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant affidavit. I believe that sealing is necessary because the items and information to be seized is relevant to an ongoing investigation into criminal conduct involving minor victims and as far as I am aware, the target of this investigation remains unaware that he is being investigated. Disclosure of the search warrant affidavit at this time would be likely to seriously jeopardize the investigation. Such disclosure may provide an opportunity to destroy evidence, change patterns of behavior, or allow flight from prosecution. Further, based upon my training and experience, I have learned that criminals who engage in the Subject Offenses often search for criminal affidavits and search warrants via the Internet, and disseminate them to other criminals as they deem appropriate, i.e., post them publicly online through forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on this continuing investigation and may severely jeopardize its effectiveness.

X. CONCLUSION

68. For all the reasons described above, there is probable cause to believe that GONZALEZ has committed a violation of 18 U.S.C. § 2251(a), (e) (Production of Child Pornography).

69. Further, for all the reasons described above, there is probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 371 (Conspiracy); 18 U.S.C. § 2251(a), (e) (Sexual Exploitation of Children and Attempted Sexual Exploitation of Children); 18 U.S.C. § 2422(b) (Enticement of a Minor and Attempted Enticement of a Minor); 18 U.S.C. § 2252A(a)(2) (Distribution and Receipt of Child Pornography); 18 U.S.C. § 2252A(a)(5)(B) (Access with Intent to View and Possession of Child Pornography); and 18 U.S.C. § 875(b) (Interstate Threats), as described more fully in Attachment B, will be found in a search of the SUBJECT PREMISES, SUBJECT VEHICLE, and the SUBJECT PERSON described in Attachments A-1, A-2, and A-3.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 17th day of February, 2026.



HON. MARGO A. ROCCONI
UNITED STATES MAGISTRATE JUDGE