AFFIDAVIT IN SUPPORT OF APPLICATION FOR COMPLAINT & ARREST WARRANT

I, Rachel Corn, a Special Agent with the Federal Bureau of Investigation (FBI), Baltimore Division, Baltimore, Maryland, being duly sworn, depose and state as follows:

PURPOSE OF THE AFFIDAVIT

1. This affidavit is submitted in support of a criminal complaint and arrest warrant for Erik Lee Madison ("Madison"), born in 2005, for violations of Title 18 United States Code, Section 2251(a) (sexual exploitation of a child), Title 18 United States Code, Section 2422(b) (online coercion and enticement), and Title 18, United States Code, Section 2261A(2) (Cyberstalking) (the "TARGET OFFENSES").

2. The statements in this affidavit are based in part on information and reports provided by the Anne Arundel County Police Department, the Baltimore County Police Department, the training and experience of other law enforcement officers with whom I have had discussions, on my investigation of this matter, and on my experience and background as a Special Agent of the FBI. Since this affidavit is being submitted for the limited purpose of securing a complaint and arrest warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that Madison has committed the TARGET OFFENSES.

AGENT BACKGROUND

3. I have been a SA with the FBI since May 2006. Since September 2006, I have primarily investigated federal violations concerning child pornography and the sexual exploitation of children. I have gained experience through training in seminars, classes, and daily work related to conducting these types of investigations. Specifically, I have received FBI Crimes Against Children training, FBI Innocent Images Online Undercover training, and FBI Peer to Peer Network

Online Investigation training. I have participated in the execution of numerous search warrants, of which the majority have involved child exploitation and/or child pornography offenses. Many of the child exploitation and/or child pornography search warrants resulted in the seizure of computers, cell phones, magnetic storage media for computers, other electronic media, and other items evidencing violations of federal laws, including various sections of Title 18, United States Code § 2252A involving child exploitation offenses. I have also participated in the execution of numerous search warrants for online accounts, such as email accounts, online storage accounts and other online communication accounts related to child exploitation and/or child pornography. In the course of my employment with the FBI, I have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media and within online accounts.

4. As a federal agent, I am authorized to investigate violations of laws of the United States and am a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

PROBABLE CAUSE

5. On November 6, 2025, Madison's person and residence were searched, pursuant to warrants issued by the Honorable Douglas R. Miller (Case Nos. 25-mj-02892-DRM, 25-mj-02893-DRM). The redacted affidavit in support of those search warrant applications is attached to this affidavit as Exhibit 1, and incorporated by reference.

6. During the execution of the search warrant of Madison's person, an iPhone was seized. The phone was password protected. The password for the phone was provided by Madison's mother. The phone was manually reviewed at the residence. Eleven Google accounts were located on the phone to include kinishroxy@gmail.com and johngotii25@gmail.com. The

Google Voice number 469-389-1708, the number provided by Minor Victim 2 as being a "burner phone number" used by Leo, was also logged into the phone. Within the Password application of the phone the Roblox account Departed49 (the Roblox username that Minor Victim 2 and Minor Victim 3 identified as Leo's) was listed. Also located in the Password application of the phone was an Amazon account associated with the phone number 667-415-6879. Several applications, such as Chime, MartinsFood, and MyWorkDaysite.com were associated with the email address emadison519@icloud.com.

7. During the search of the bedroom identified as Madison's bedroom several pieces of paper were located. Some of the pieces of paper stated, "Horror House Leo Heil Satan" and "NMK LEO."

CONCLUSION

8. Based upon all of the information set forth in this application, I respectfully submit that there is probably cause to believe that **Erik Lee Madison** violated Title 18 United States Code, Section 2251(a) (sexual exploitation of a child), Title 18 United States Code, Section 2422(b) (online coercion and enticement), and Title 18, United States Code, Section 2261A(2) (Cyberstalking).

Rachel S C

Special Agent Rachel Corn
Federal Bureau of Investigation

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4.1 and Fed. R. Crim. P. 4(d) this 6th day of November, 2025.

Honorable Douglas R. Miller
United States Magistrate Judge
District of Maryland

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Rachel S. Corn, a Special Agent with the Federal Bureau of Investigation (FBI), Baltimore Division, Baltimore, Maryland, being duly sworn, depose and state as follows:

1. I have been a Special Agent with the FBI since May 2006. Since September 2006, I have primarily investigated federal violations concerning child pornography and the sexual exploitation of children. I have gained experience through training in seminars, classes, and daily work related to conducting these types of investigations. Specifically, I have received FBI Crimes Against Children training, FBI Innocent Images Online Undercover training, and FBI Peer-to-Peer Network Online Investigation training. I have participated in the execution of numerous search warrants, of which the majority have involved child exploitation and/or child pornography offenses. Many of the child exploitation and/or child pornography search warrants resulted in the seizure of computers, cell phones, magnetic storage media for computers, other electronic media, and other items evidencing violations of federal laws, including various sections of Title 18, United States Code § 2252A involving child exploitation offenses. I have also participated in the execution of numerous search warrants for online accounts, such as email accounts, online storage accounts and other online communication accounts related to child exploitation and/or child pornography. In the course of my employment with the FBI, I have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media and within online accounts.

2. As a federal agent, I am authorized to investigate violations of laws of the United States and am a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

[redacted]

6. The statements in this affidavit are based in part on information and reports provided by the Anne Arundel County Police Department, the Baltimore County Police Department, the training and experience of other law enforcement officers with whom I have had

[redacted]

discussions, on my investigation of this matter, and on my experience and background as a Special Agent of the FBI. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violations of the TARGET OFFENSES are located in the TARGET ACCOUNTS and TARGET LOCATIONS.

SUMMARY CONCERNING CHILD PORNOGRAPHY, PERSONS WHO POSSESS AND COLLECT CHILD PORNOGRAPHY AND HOW USE OF COMPUTERS AND THE INTERNET RELATES TO THE POSSESSION, RECEIPT AND DISTRIBUTION OF CHILD PORNOGRAPHY

7. Based on my investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that individuals who utilize the internet to view and receive 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, including the following:

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 other visual media, or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children or images of children frequently maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location.

Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer or cellphone, and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, or in online storage, email accounts or other online communication accounts, to enable the individual to view the collection, which is valued highly.

e. 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, rarely destroy correspondence from other child pornography distributors/collectors, 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. This data is typically in digital format, and often maintained on computers, cell phones and in online storage, email accounts or other online communication accounts.

f. Individuals who would have knowledge on how to distribute and receive digital images of child pornography through the use of Peer to Peer networks and other online methods would have gained knowledge of its location through online communication with others of similar interest. Other forums, such as bulletin boards, newsgroups, IRC chat or chat rooms have forums dedicated to the trafficking of child pornography images. Individuals who utilize these types of forums are considered more advanced users and therefore more experienced in acquiring a collection of child pornography images.

g. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior has been consistently documented by law enforcement officers involved in the investigation of child pornography.

8. Based on my investigative experience related to computer and internet related child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned the following:

a. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies.) The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The

distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

b. The development of computers, smartphones and the internet have added to the methods used by child pornography collectors to interact with and sexually exploit children. Computers, smartphones and the internet serve four functions in connection with child pornography. These are production, communication, distribution, and storage.

c. Mobile devices such as laptop computers, smartphones, iPods, iPads and digital media storage devices are known to be used and stored in vehicles, on persons or other areas outside of the residence.

d. Smartphones have the capability to access the Internet and store information, such as videos and images. As a result, an individual using a smartphone can send, receive, and store files, including child pornography, without accessing a personal computer or laptop. An individual using a smartphone can also easily plug the device into a computer, via a USB cable, and transfer data files from one digital device to another. Many people generally carry their smartphone on their person.

e. Child pornographers can now transfer photographs from a camera onto a computer-readable format. With the advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography.

f. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), easy access to the Internet, and online file sharing and storage, the computer is a preferred method of distribution and receipt of child pornographic materials.

g. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion. Collectors and distributors of child pornography use online resources to retrieve and store child pornography, including services offered by Internet Portals such as AOL Inc., Yahoo, and Google, Inc., Facebook, Dropbox, Instagram, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services, file exchange services, messaging services, as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Email accounts, online storage accounts, and other online communication accounts allow users to save significant amounts of data, including email, images, videos, and other files. The data is maintained on the servers of the providers, and is occasionally retained by the providers after the user deletes the data from their account. Typically, when

individuals search for and obtain files on the internet that depict the sexual abuse of minors, using cell phone, and other computer to visit internet websites, the electronic communications travel in and affecting interstate and even foreign commerce.

h. In my recent investigative experience, as well as recent discussions with law enforcement officers, I know that individuals who collect child pornography are using email accounts, online storage accounts, and other online communications accounts to obtain, store, maintain, and trade child pornography with growing frequency, in addition to, or as an alternative to, the use of personal devices.

i. Based on traits shared by collectors, the use of email, online storage accounts, and other online communication accounts, and the increased storage capacity of computers and server space over time, there exists a fair probability that evidence regarding the distribution, receipt and possession of child pornography will be found in the TARGET LOCATIONS notwithstanding the passage of time.

j. In addition, computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily available forensic tools.

k. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space for long periods of time before they are overwritten.

l. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages.

m. The storage capacity of personal computers has increased dramatically over the last few years. Common and commercially available hard drives are now capable of storing over 500 GB of data. With that amount of storage space, an individual could store thousands of video files and/or hundreds of thousands of image files.

n. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Since the storage capacity of hard drives has increased dramatically over the last several years, it is more likely that the above-described information will be recovered during forensic analysis.

NCMEC CYBERTIPLINE REPORTS

9. The National Center for Missing and Exploited Children (NCMEC) receives complaints via their Cybertipline from Internet Service Providers (ISPs), Electronic Service Providers (ESPs), and others. These Cybertipline reports are reviewed by a NCMEC analyst and forwarded to law enforcement for further investigation on the information provided in the Cybertipline report.

DISCORD

10. Discord is a free voice, video, and text chat application. Users can access Discord via desktop and mobile applications. The service can also be accessed from its website. Once a user has created their account, users can create a server, and invite their friends to join it with an invite link, or they can join an existing server. Users can also communicate through direct messages. Direct messages allow users to send messages, share files, live stream their screen, and call others privately outside of servers.

11. Discord retains certain information regarding the users of their communications platforms, in addition to certain information pertaining to the communication itself. Among that data is the following: the unique User ID number of the account that is assigned by Discord; the registration date and time for the account; the registration IP address of the account; email addresses provided by a user; a user's current username and tag number; if the user is a paid subscriber, limited billing information; IP addresses; session start-timestamps for the last 90 days; whether the email address is verified; friends-list for users; and stored messages and attachments that users have send to each other in text channels, whether in a server or in direct messages, unless it has been deleted by the user.

BACKGROUND ON NIHILISTIC VIOLENT EXTREMISM AND 764

12. Nihilistic Violent Extremists (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 advancing their goal of destroying civilized society through the corruption and exploitation of vulnerable populations, which often includes minors.

13. 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.

14. 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.

15. 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, 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.

16. NVEs networks 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.

17. One such NVE group is known as "764." Members of 764 use known online social media communications platforms, as mediums to support the possession, production, and sharing of extreme gore media and CSAM with vulnerable, juvenile populations. These individuals often conduct coordinated extortions of teenagers, blackmailing the victims to comply with the demands of the group.

18. Members of 764 are often required to procure photos or videos of their victims containing CSAM and self-mutilation content to maintain or improve their standing in 764 online networks. It is common for 764 members to extort minor victims into producing CSAM via recorded video calls, which are made available to other 764 members. The self-mutilation content sought by 764 members often includes what is referred to as "blood signs," "fan signs," or "cut signs."[2] These terms generally refer to victims being extorted into using a sharp object to either (1) cut a symbol or word such as an online moniker into the victim's skin; or, (2) cut the body to obtain blood which the victim uses to draw words or symbols, usually on a wall or other flat surface. 764 members often distribute photographs and/or video recordings of the cutting and

[2] The words "fan signs" and "cut signs" are often abbreviated "fs" and "cs," respectively.

subsequent designs created with the victim's blood. 764 members often store photographs and videos of the CSAM or self-mutilation content among one or more digital devices such as their cellular telephones, computers, or other digital storage media.

19. To extort victims into producing CSAM or self-mutilation content, 764 members often threaten to release naked pictures of the victim or to "swat" the victim or the victim's family. Swatting describes the reporting of a false emergency to law enforcement with the intent to cause an armed police response to a particular location. Swattings sometimes result in serious physical injury or death as responding officers are often made to believe they are responding to a mass shooting or other life or death situation. There are several groups the FBI assesses are offshoots of 764. These groups exhibit the same or similar characteristics and modus operandi as 764. These groups include but are not limited to "30," "44," and "6996."

BACKGROUND ON TELEGRAM

20. As described by Telegram on their public-facing website,[3] as well as based on my training and experience, I am aware that Telegram is a mobile and desktop messaging application. It can be used on smartphones, such as Apple iOS and Google Android devices, and on desktop computers by users to send messages and media to each other. Telegram has reported that it has approximately one billion active users.

21. To sign up for a Telegram account, a user must provide a phone number. Telegram users can select a username, but they are not required to do so. Usernames are unique, meaning only one Telegram user can have a particular username. Telegram users can find other users by

[3] Much of the information in this section can be found on Telegram's website, including Telegram's Privacy Policy (https://telegram.org/privacy?setln=en), Terms of Service (https://telegram.org/tos?setln=en), and FAQ page (https://telegram.org/faq?setln=en).

searching for the username or by using the known phone number of a user. Users can also select a display name, such as a first and last name. Display names are not unique.

22. Telegram offers a variety of communication methods for its users, including:

a. **One-on-one chats.** Users on Telegram can communicate directly with another user through a one-on-one chat. The participants can send each other text messages, photos, videos, any files, and make voice calls.

b. **Groups.** Telegram users can join a group with up to 200,000 "members." The members of a group can share messages, photos, videos, and files. A group can be public (i.e., anyone can view and post messages in the group) or private (i.e., an individual must be added to the group to see its content and/or members). Members of a group can designate "administrators," who are members of the group that control group membership and information.

c. **Channels.** The "owner" or "administrator" of the channel to broadcast messages to an unlimited number of "subscribers." Subscribers cannot post messages in the channel. A channel can be either public or private.

d. **Secret chats.** Secret chats are a type of group in which messages are end-to-end encrypted, meaning that only the sender and recipient can view the contents of the chats on their respective devices. A user can modify the settings of a secret chat to prevent the forwarding of messages and to automatically delete messages.

23. Telegram is a cloud service that stores information and media from chats, groups, and channels on servers owned, maintained, controlled, or operated by Telegram. However, Telegram does not store information or media related to secret chats on its servers.

24. If a user logs in to Telegram from a new device using their phone number, information and media stored in Telegram's cloud will sync instantly to the new device. A Telegram account can be used on multiple devices at the same time.

25. According to Telegram's privacy policy, Telegram stores basic user account data, including mobile number, username, display name, profile picture, and e-mail address, to the extent a user has provided this information.

26. I am aware that Telegram represents on its website that it is "based in Dubai," while Telegram has also reported that it is incorporated in the British Virgin Islands. However, based on information relayed to by members of the Department of Justice, I am aware that efforts to obtain information by serving mutual legal assistance requests on either the United Arab Emirates or the British Virgin Islands for information from Telegram have been unsuccessful.

27. Until approximately September 2024, Telegram refused to respond to legal process from the United States. Starting in approximately September 2024, Telegram updated its privacy policy and began to respond to law enforcement requests for subscriber information, typically consisting of a user's phone number and the Internet Protocol (IP) address of the user's most recent login.

28. I am unaware of any successful attempts by U.S. law enforcement to obtain additional information—including the contents of messages—from Telegram.

29. Telegram's website describes how the company intentionally distributes its servers to prevent governments from obtaining communications content:

> To protect the data that is not covered by end-to-end encryption, Telegram uses a distributed infrastructure. Cloud chat data is stored in multiple data centers around the globe that are controlled by different legal entities spread across different jurisdictions. The relevant decryption keys are split into parts and are never kept in the same place as the data they protect. As a result, several court orders from different jurisdictions are required to force us to give up any data.

Thanks to this structure, we can ensure that no single government or block of like-minded countries can intrude on people's privacy and freedom of expression. Telegram can be forced to give up data only if an issue is grave and universal enough to pass the scrutiny of several different legal systems around the world.

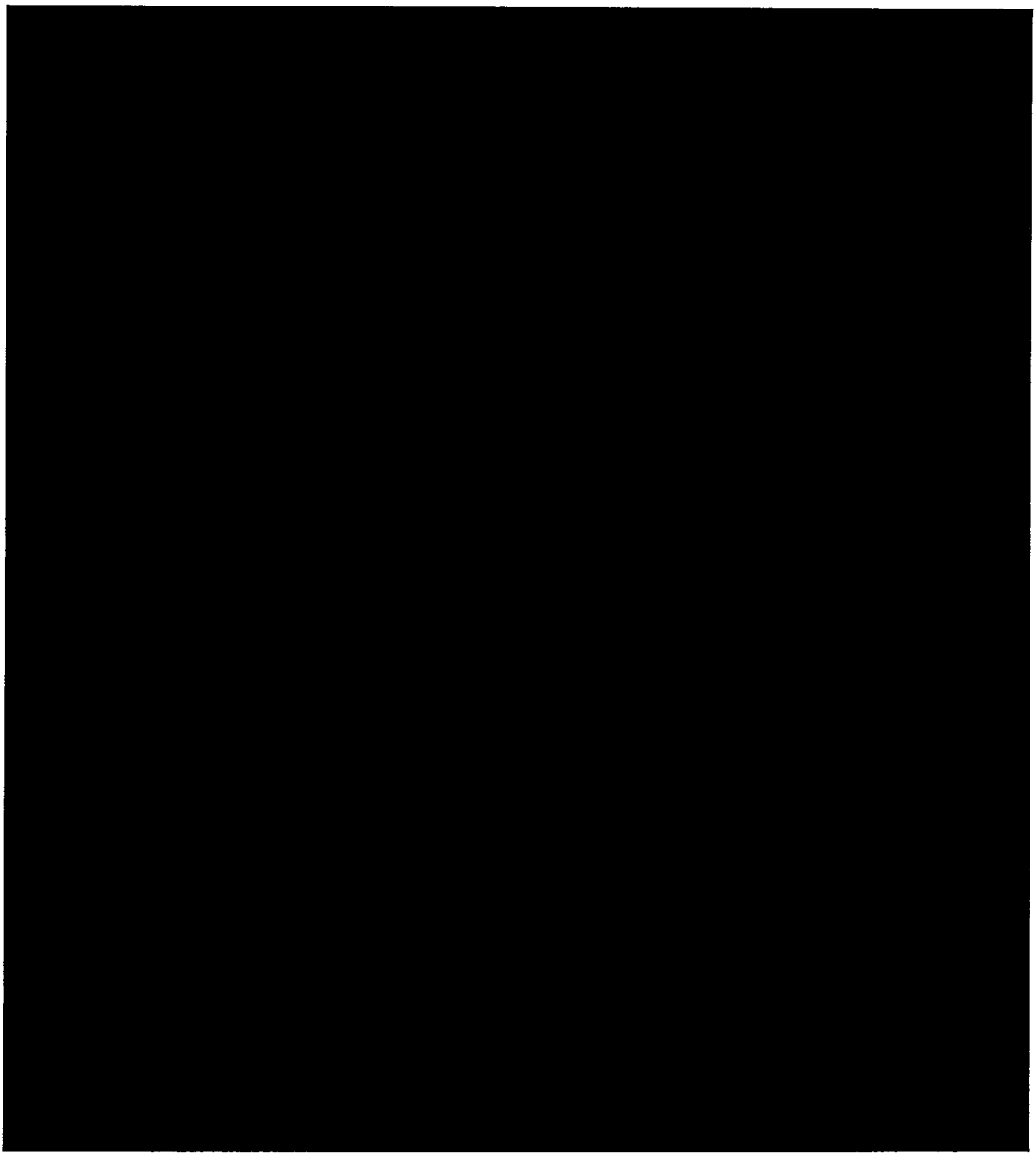
To this day, we have disclosed 0 bytes of user messages to third parties, including governments.

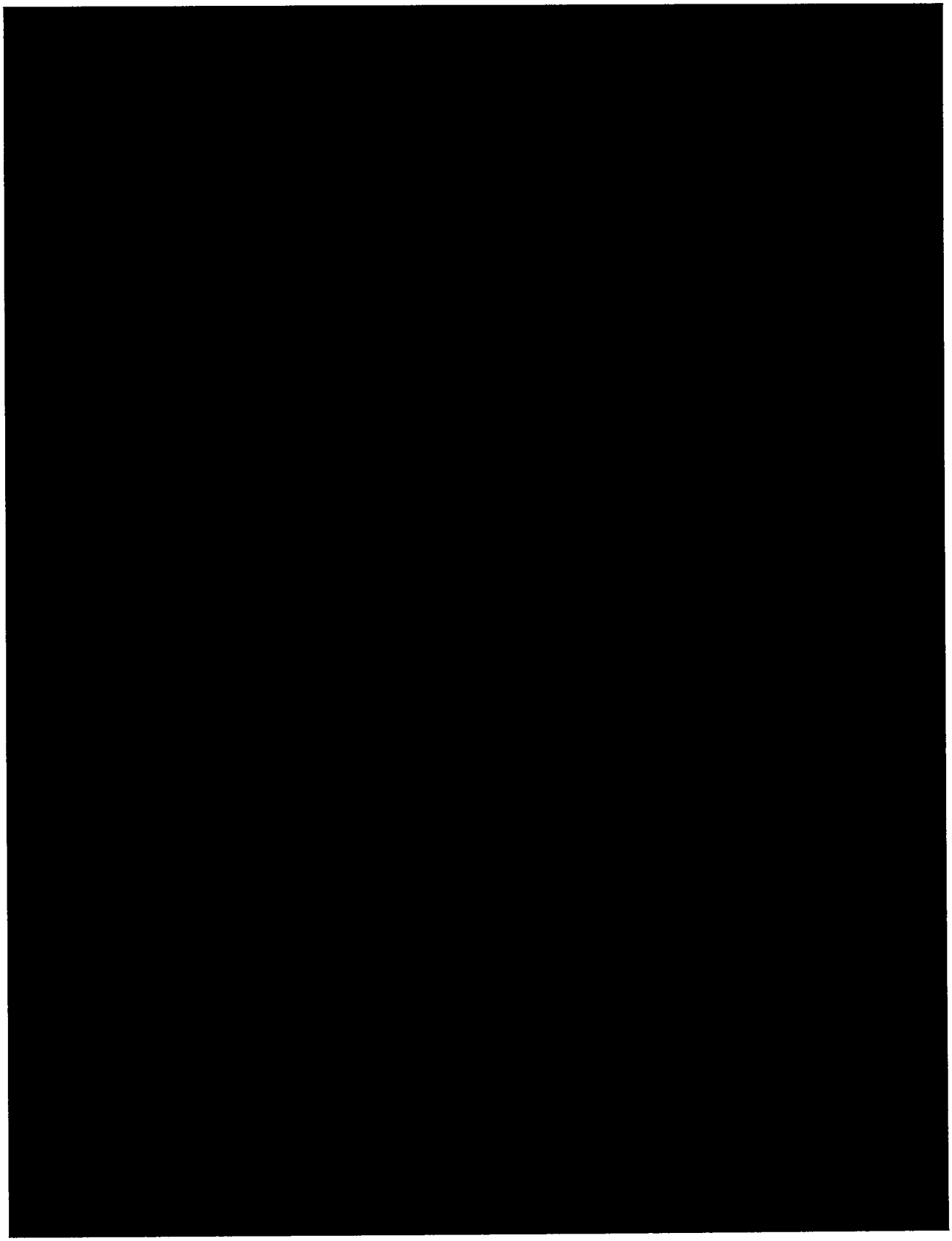
[redacted]

PROBABLE CAUSE

[redacted]

[4] The location of City A is known to law enforcement. However, because of the sensitive nature of this information, it will only be referred to as City A in this affidavit.

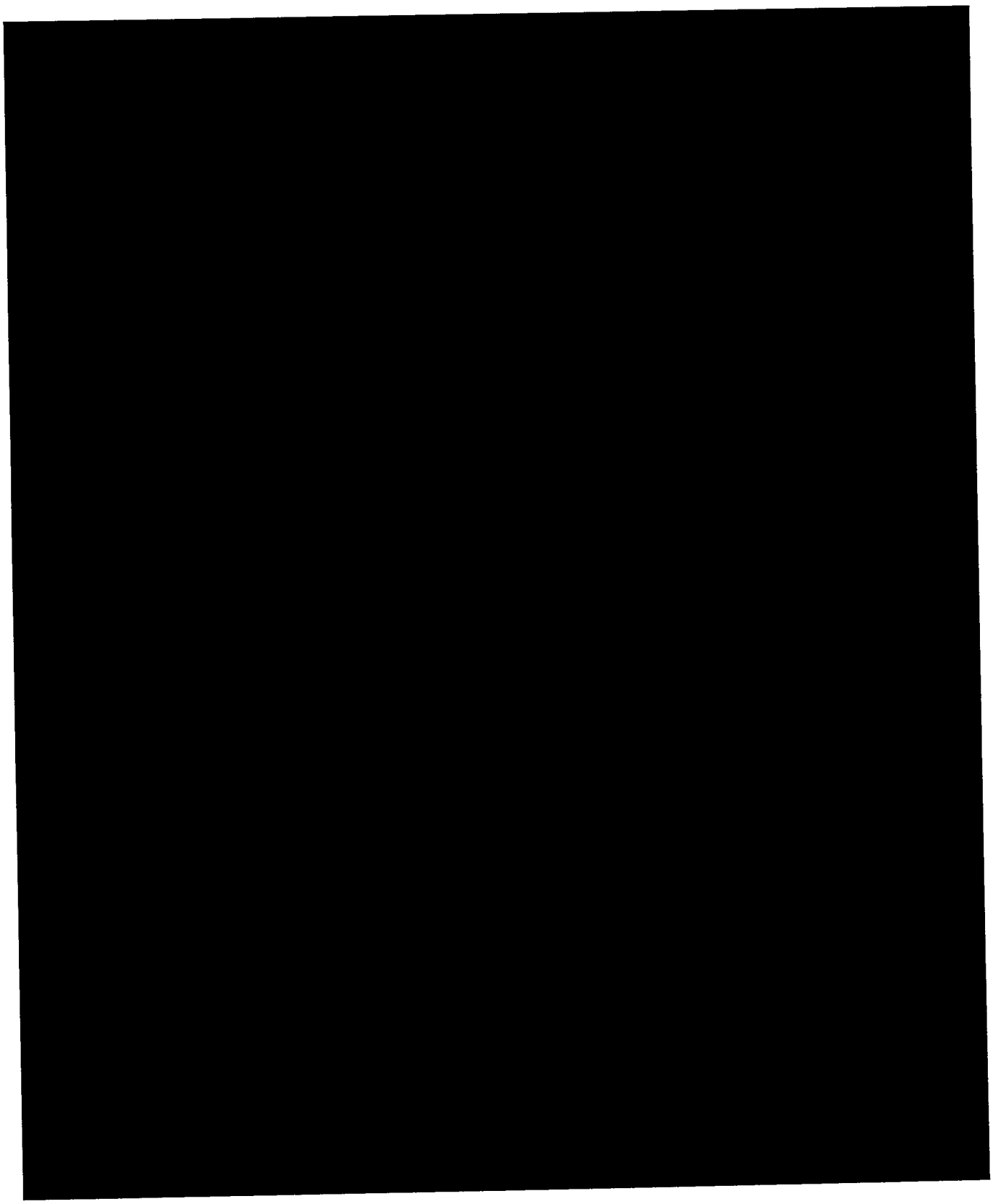


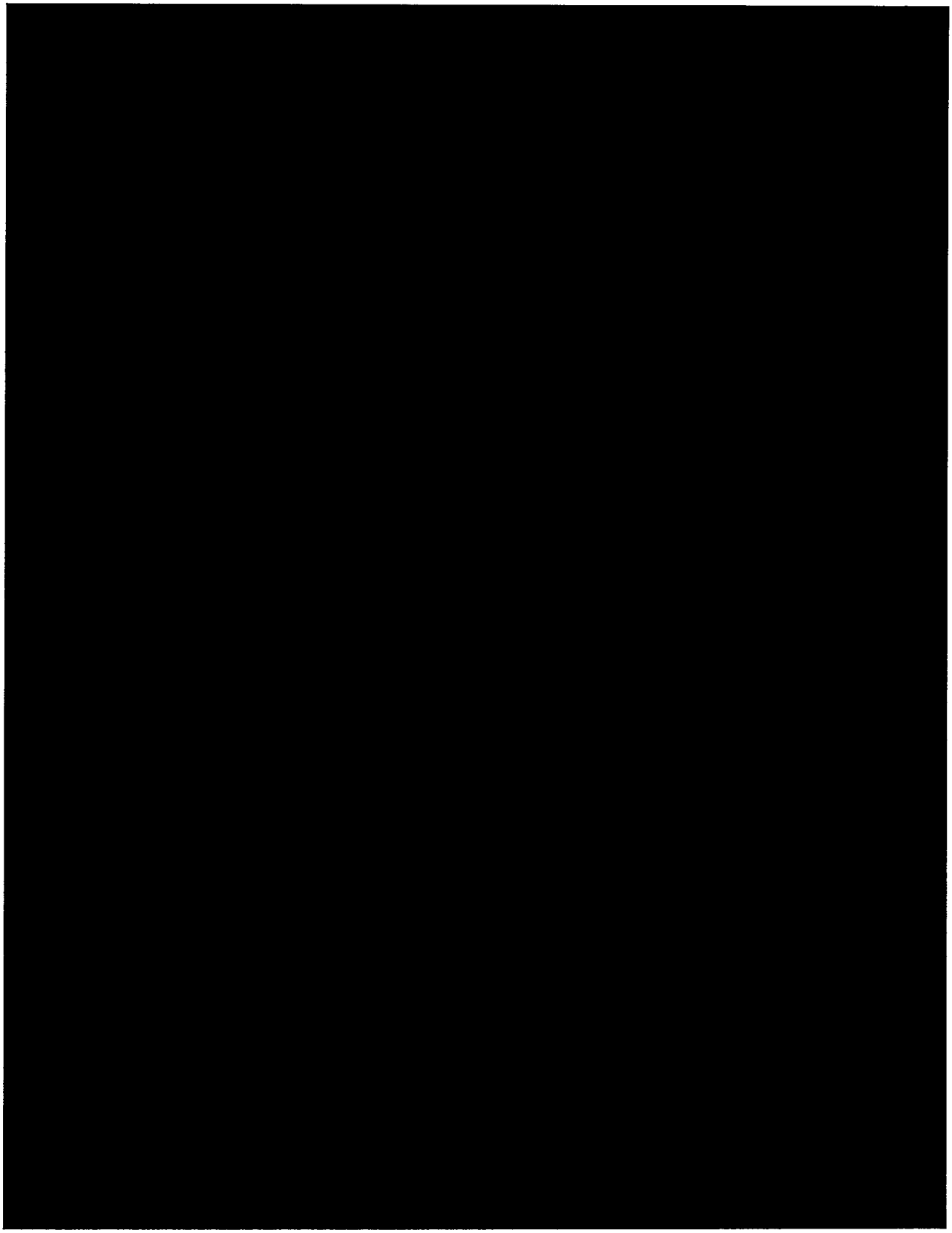


[redacted]

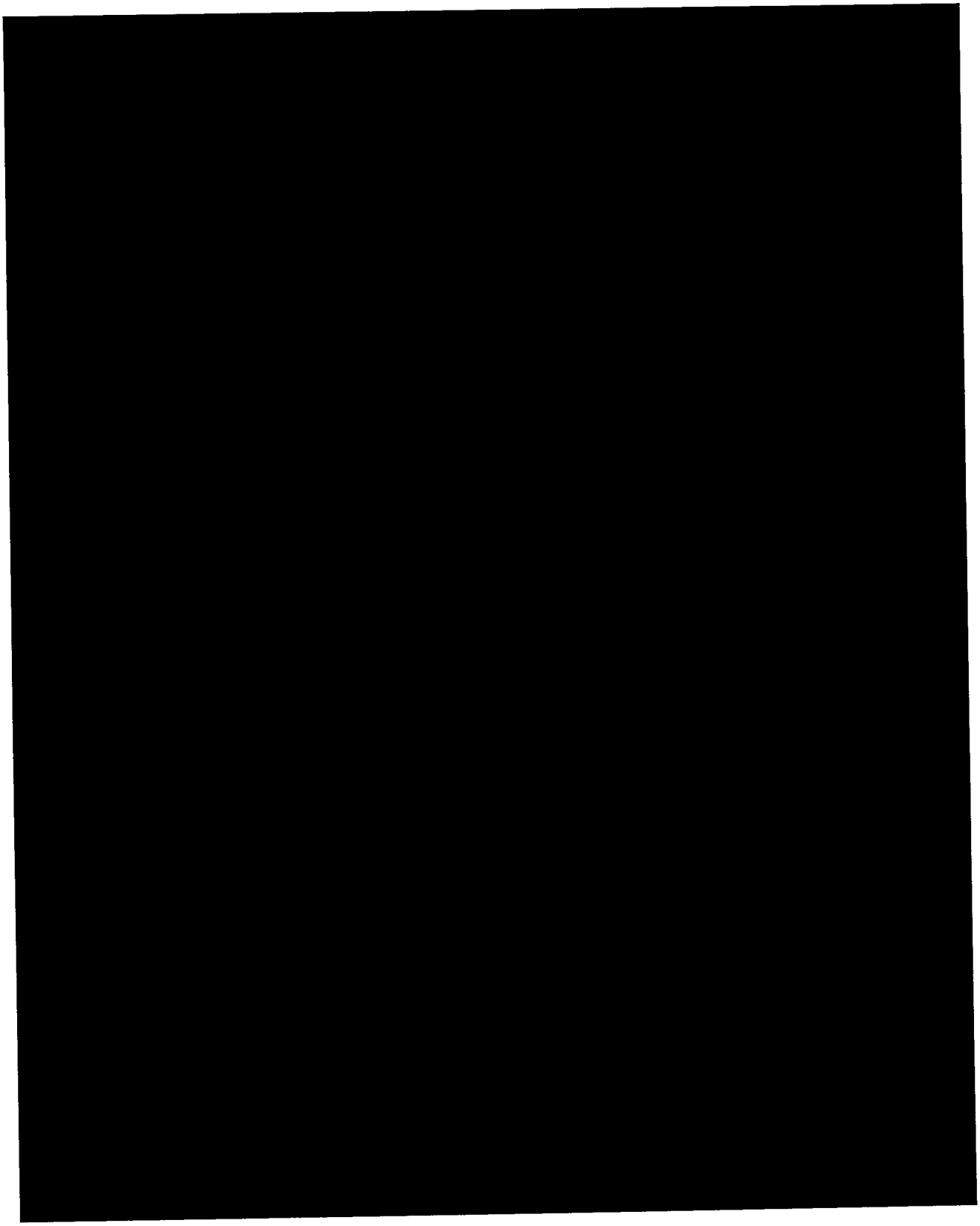
[8] A Discord server is a dedicated space within the Discord platform where communities can gather, communicate, and share content. Similar to a virtual meeting place organized into channels, allowing for text-based conversations, voice and video chats, and media sharing. Servers are customizable and can be tailored to various group sizes and interests, from small friend groups to large communities.

[redacted]





[10] According to Maryland Motor Vehicle Records, **Erik Madison** has a State Identification Card but not a driver's license. The address listed on the identification card is **2716 Daisy Avenue, Baltimore, Maryland 21227**.



1:25-mj-02891-DRM 1:25-mj-02892-DRM 1:25-mj-02893-DRM
1:25-mj-02907-DRM

[redacted]

53. Pinger provided the following information in response to administrative subpoena for the following account associated with phone number 469-963-5840 [redacted]

[redacted]

Account ID:	2134994590
Account Created:	03/26/2025
Application:	TextFree
Third Party Email:	emadison519@icloud.com
Email Verified:	Yes

54. Discord provided the following information in response to an administrative subpoena for the account 1350195743838830764:

Registration Date:	2025-03-14
Last Login Date:	2025-04-06
Old Username:	whatsyourproblemkid
Old Display Name:	Lucious

At least one login IP address resolved back to a Virtual Private Network.[11] Another login IP address resolved back to **2716 Daisy Avenue, Halethorpe, Maryland.**

55. Instagram provided the following information in response to an administrative subpoena for the account:

User ID:	71887328813
Vanity Name:	trackmeguys
Registered Email Address:	watchoutman@tutamail.com[12] (Verified)
Registered Date:	2025-01-15

At least one login IP address resolved back to a VPN. Another IP address that logged into the account on June 7, 2025 resolved back to **2716 Daisy Avenue, Halethorpe, Maryland.**

56. On August 12, 2025, United States Magistrate Judge Chelsea Crawford, of the District of Maryland, issued search warrants (Case Nos. 25-mj-02015, 25-mj-02016, 25-mj-02017, 25-mj-02018) for the following below listed accounts. The review of the search warrant results for the accounts is ongoing.

a. Discord accounts:

1. User ID: 1296273751880765461;
2. User ID: 1350195743838830764 ;
3. User ID: 735991317586509834;
4. User ID: 1264041778290491442; and
5. User ID: 1310771024777711691;

b. Roblox accounts:

1. User ID: 3195130829; and

[11] A Virtual Private Network ("VPN") creates a secure connection between a user and the internet, while the user remains anonymous by hiding their location, making it difficult to be tracked.

[12] Tuta is a secure and private email service that focuses on encrypting all data, including emails, contacts, and calendars. It's known for its commitment to user privacy and security, using end-to-end encryption and offering a free tier wit h no message limits. Tuta offers free and paid accounts. Tuta is based out of Germany.

2. User ID: 154156516;

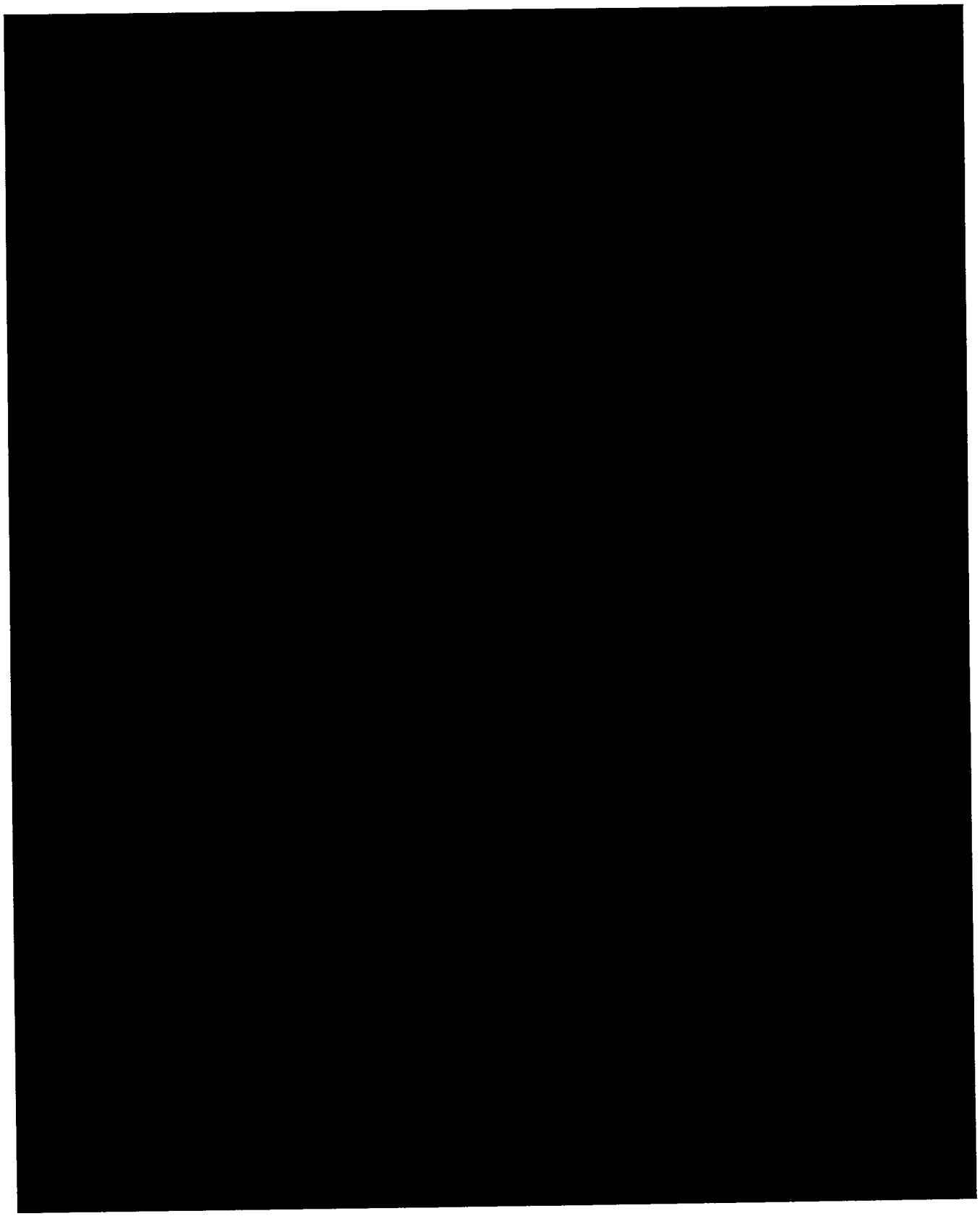
c. Instagram accounts:

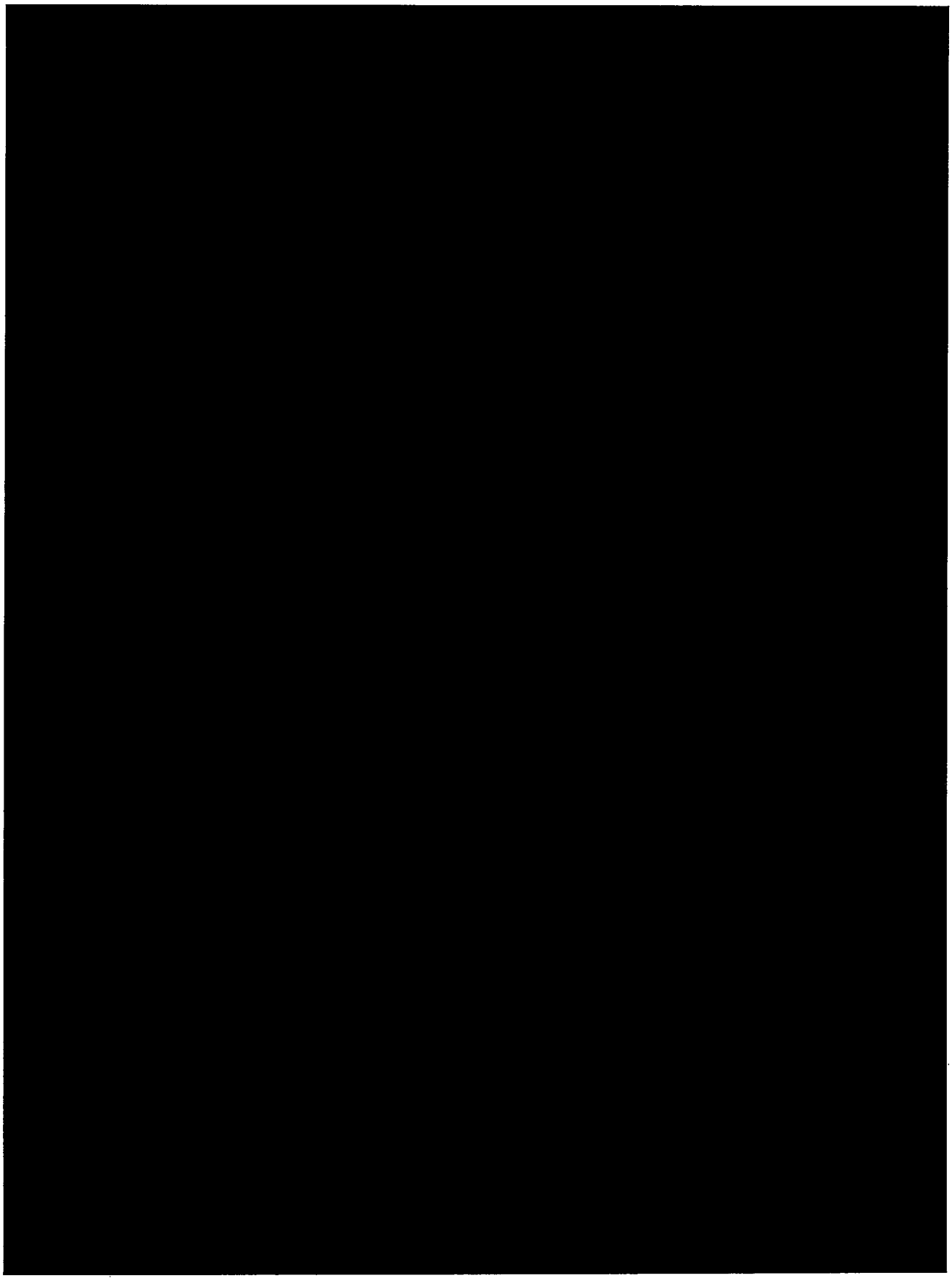
1. [redacted]
2. User ID: 71887328813 and Vanity Name: trackmeguys; and
3. User ID: 67820402061 and Vanity Name: inosatru;

d. Snap accounts:

1. Username: Reallyyoulnowme; and
2. [redacted].

[redacted]





[redacted]

iCloud Search Warrant

64. On September 17, 2025, United States Magistrate Judge Douglas R. Miller, of the District of Maryland, issued a search warrant (Case No. 25-mj-02386-DRM) for the following below listed iCloud accounts, the results of which are still being reviewed:

[redacted]

c. samuelpscarselli@icloud.com and DS ID: 8340670725;
d. emadison519@icloud.com and DS ID: 21141624151; and
e. emadison2005@icloud.com and DS ID: 17707599507.

Search Warrant Review of Apple Account emadison2005@icloud.com

65. The review of the search warrant results for the account associated with emadison519@icloud.com revealed the following account details:

Apple ID:	emadison519@icloud.com
DS ID:	21141624151

Account Type:	Full iCloud (iCloud+)
Name:	**Erik Madison**
Address:	**2716 Daisy Avenue, Halethorpe, Maryland**
Daytime Phone:	443-683-7786
Facetime/iMessage:	667-415-6879
Account Status:	Active
Creation Date:	10/06/2023

[redacted]

67. Also located in the deleted folder were five videos and two images that appear to be of the same female. In the videos, the female is observed naked from the waist down with her vaginal area mostly covered by a pillow. In at least two of the videos, a female's name is observed at the top. In the images, the female is naked from the waist down, facing the camera, with her genitalia exposed. The female's face is not observed in the images or videos. In some the videos and images, cuts are observed on the female's legs and arms. The titles of the six videos all begin, "ScreenRecording_09-05-2025."

68. Located in the cloudphotolibrary folder of the Apple search warrant results for the account emadison519@icloud.com was an image titled, IMG_7581.png, which appears to be a screen capture of a **Telegram** chat with a user's name, which is a nickname for the name that was displayed during the two videos mentioned in the previous paragraph. In the chat, the user of the account in the nickname says she is 14 years old. It is not known when the chat occurred.

69. Additional review of the Apple search warrant results for the account associated with emadison519@icloud.com revealed several images and videos where the name "Leo" was observed. For example, the video titled, 9202854341222041349.mp4 depicts red colored writing on a wall that says, "Leo 764 skin creep bleach dawn" and "I gave my soul to Leo." There are

pictures of several females, whose faces are not depicted, with the word "Leo" written on their bodies in red.

70. Also located in the Apple search warrant results for the account associated with emadison519@icloud.com were two videos that appear to be screen recordings of the same female. The recordings appear to be of a live Discord video chat involving two users. The videos are titled "-1223292174282966172.mp4" and "-3146014577452858084.mp4." During both recordings, the display names of the two users in the live video chat are observed. One of the display names is "leo." In both videos, a naked female is sitting on what appears to be a bed with her knees bent and her genitalia exposed to the camera. The female's face is not seen in the recordings. A voice is heard and appears to be instructing the female. In the first video, the voice is heard saying the following,

> Now listen, I want you to spread your legs again. Place your hand down onto your pussy. I want you to rub your clit for me. Very good. Keep going. Good. Good. You're doing so good for me.

The female is observed following the instructions and touches her genitalia with her hand. During the second recording, the female digitally penetrates her genitalia as the same voice continues to speak to her.

71. Also located in the Apple search warrant results for the account associated with emadison519@icloud.com are several images and videos of the same male. Based on my review of **Erik Madison's** MVA photograph and recent surveillance conducted at Madison's residence, I believe the images and videos are of **Erik Madison**. Also observed in the account associated with emadison519@icloud.com are several screenshots of what appears to be telegram chats.

Cybertipline Reports Received in September 2025

72. On September 17 and 18, 2025, NCMEC received 3 Cybertipline reports listing the same suspect account[13] and three separate suspected minor victims. All 3 Cybertipline Reports listed the Primary Incident Type as "Online Enticement of Children for Sexual Acts," and are detailed immediately below.

Cybertipline Report 220150889

73. On September 17, 2025, Discord sent Cybertipline Report 220150889 to NCMEC and listed the Primary Incident Type as "Online Enticement of Children for Sexual Acts." The incident time was listed as September 6, 2025. The report was processed by NCMEC and provided to law enforcement. Cybertipline Report 220150889 listed the suspect account username was baphome1. Also provided with the Cybertipline Report were chat logs between the Discord accounts baphome1 and an account that has been identified as being used by Minor Victim 2, born in 2010. Below is an excerpt from the chat logs, which took place between September 6, 2025, and September 8, 2025, with my comments in brackets:

Minor Victim 2:	Sooo what do yoh look likeee^^
	***
baphome1:	ill send a picture
Minor Victim 2:	AWW UR HANDSOME
baphome1:	thanks you are such a sweet girl
Minor Victim 2:	Noproblem!! And thxx^^
Minor Victim 2:	What's ur namee!!

[13] As detailed below, the suspect account in all 3 Cybertipline reports has the same User ID and email address, and the User Name in each includes "baphome1." Thus, I believe that all 3 are the same account.

baphome1: atlas

***

baphome1: i have something to ask

Minor Victim 2: Mhm!

baphome1: do you self harm [victim's first name]

Minor Victim 2: Well like I stopped for a while but this year I relapsed so yeah

***

baphome1: could you send me another pic?

***

baphome1: i will call in 15 minutes

***

baphome1: jvc[14]

***

[At this point in the conversation, it appears the two users may be communicating on Discord via live voice or video call based on the following messages sent by baphome1: "spell LEO big," "leave and rejoin i cant hear you," and "call when you are out the tub."]

***

Minor Victim 2: Is it oki for my cuts to puff up so much they usually dont :p or is it just cuz I repeatedly went over them

***

baphome1: would you like to call sweet girl

***

[14] JVC a term commonly found on Discord and other communication platforms meaning "join voice chat."

baphome1:	i want you to fuck yourself for me again
Minor Victim 2:	I cannot right now my parents are awake
Minor Victim 2:	I hear them because there in the room next to me
baphome1:	hm ok did you shave?
Minor Victim 2:	Not yet but ill make sure to shave later when I get back from my aunts house

***

baphome1:	i loved how soaked your bed was
Minor Victim 2:	It was messy :3
baphome1:	yeah and i will use you whenever i fucking want
baphome1:	yeah change your name to leos whore on discord now
Minor Victim 2:	That good??
baphome1:	yeah
baphome1:	goodlsut
baphome1:	slut
baphome1:	make sure you shave today
baphome1:	i love you slut
Minor Victim 2:	I gotta go now because my parents are mad im on my phone

***

Minor Victim 2:	But there i shaved!!^^
baphome1:	awww
baphome1:	look at that cute little pussy

Cybertipline Report 220215082

74. On September 18, 2025, Discord sent Cybertipline Report 220215082 to NCMEC and listed the Primary Incident Type as "Online Enticement of Children for Sexual Acts." The incident time was listed as September 5, 2025. The report was processed by NCMEC and provided to law enforcement. Cybertipline Report 220215082 listed the suspect account as baphome1#0000. Also provided with the Cybertipline Report were chat logs between the Discord accounts baphome1 and an account that has been identified as being used by Minor Victim 3, born in 2010. Below is an excerpt from the chat logs, which took place between September 5, 2025, and September 18, 2025, with my comments in brackets:

baphome1: can you fuck your little pussy for me?

***

Minor Victim 3: Ok ik ur talking other little kids but you can at least reply

***

Minor Victim 3: You can ask me to play with my clih but not reply

***

baphome1: wanna esex?

Minor Victim 3: how do u esex vro

***

baphome1: you want me to ext you but you cant even cut properly

Minor Victim 3: I told you my razors aren't sharp fag

Minor Victim 3: Oops didn't mean to say that!

baphome1: so then cam up and play with your pussy

***

baphome1: can you cut today

***

baphome1: i need you to use your blood to draw on a wall

Cybertipline Report 220241510

75. On September 18, 2025, Discord sent Cybertipline Report 220241510 to NCMEC and listed the Primary Incident Type as "Online Enticement of Children for Sexual Acts." The incident time was listed as September 12, 2025. The report was processed by NCMEC and provided to law enforcement. Cybertipline Report 220241510 listed one of the recipient accounts as baphome1#0000. Also provided with the Cybertipline Report were chat logs between the Discord accounts baphome1, and an account that has been identified as being used by Minor Victim 4, born in 2012, and other unidentified recipients and subject accounts. During the chat, which took place between September 12, 2025, and September 14, 2025, most of the communication comes from other users. Baphome1 said the following during the chat: "im going to make sure your mom knows what you do" and "bitch if you dont start slitting your thighs i promise."

76. A subpoena was sent to Comcast to obtain the subscriber information regarding the IP address 73.133.203.14, which logged into the account on 09/17/2025 at 05:53:50 UTC and was listed in all three Cybertipline Reports for the account Baphome1. Comcast provided the following subscriber information:

Name:	Alton Horne
Service Address:	**2716 Daisy Avenue, Halethorpe, Maryland 21227**
Status:	Active

77. On September 29, 2025, United States Magistrate Judge Chelsea J. Crawford, of the District of Maryland, issued a search warrant (Case No. 25-mj-02466) for the Discord account associated with the Username baphome1. The search warrant results are still being reviewed.

Search Warrant Review of Discord Account baphome1

78. During the review of the search warrant results of the Discord account baphome1, a chat conversation between baphome1 and another user was located. On September 15, 2025, during the chat, baphome1 sent the following messages:

baphome1: **@bloodovmen**

baphome1: add me on **tele**[15]

79. During the review of the search warrant results of the Discord account baphome1, another chat conversation between baphome1 and another user was located. On September 15, 2025, during the chat, baphome1 sent the following messages:

baphome1: my **tele** just got frozen

***

baphome1: https://**t.me/LEOh3ll**[16]

baphome1: new **tele**

80. During the review of the search warrant results of the Discord account baphome1, a chat conversation between baphome1 and the Discord account believed to used by Minor Victim

[15] Through my training and experience, "tele" is believed to be an abbreviation for Telegram.

[16] "T.me" is the short link domain for Telegram, used to create links for user profiles, groups, channels, and bots. When clicked, a t.me link opens the respective Telegram content directly in the app or, if the app isn't installed, through a web browser for preview.

5 was also located.[17] Below is an excerpt from the chat logs, which took place between September 4, 2025, and September 17, 2025, with my comments in brackets:

baphome1#0:	is your father home?
Minor Victim 5:	Yes unfortunately
baphome1#0:	ah i see
Minor Victim 5:	Leo I should give you his schedule
	***
baphome1#0:	hi [Minor Victim 5's online name]
	***
Minor Victim 5:	Why u leak me 2 melt
	***
Minor Victim 5:	also why ru sending shit 2 abuse
Minor Victim 5:	He has stuff to leak mr now
Minor Victim 5:	Thanks for putting me in bad positions

Interviews of Minor Victims 2, 3, and 4

81. On September 30, 2025, Minor Victim 3 was interviewed and confirmed she was 14 years old and was born in 2010. Minor Victim 3 confirmed her Discord username was account listed in Cybertipline Report 220215082 and that she communicated with baphome1 on Discord recently after first meeting him on Roblox. Baphome1's Roblox username was Departed49. Minor Victim 3 stated that baphome1 told her that he lived in Germany and that his name was or he goes by the name "Leo." Baphome1 told Minor Victim 3 that baphome1 associates himself with the extortion group "764" or "Slit Town" or "ST." Minor Victim 3 explained these are groups

[17] Follow up investigation has revealed that Minor Victim 5 is believed to have been born in 2011. Confirmation of Minor Victim 5's identity and date of birth are pending.

that extort people on Roblox. While on a call, baphone1 showed Minor Victim 3 that he had made another person cut themselves. Minor Victim 3 said she was "trolling" baphome1 and wanted to see how far she could take their conversation until he blocked her. Minor Victim 3 stated that baphome1 added people he was going to try to make into victims. Baphome1 asked Minor Victim 3 to use her blood to write "stuff" on the wall. Minor Victim 3 said she pretended to cut herself and used red makeup instead of blood to write on the wall. Baphome1 gave her Robux[18] in exchange for her cutting herself. Baphome1 also wanted Minor Victim 3 to turn on her "cam and touch herself." Minor Victim 3 denied doing this and denied sending baphome1 naked pictures. Minor Victim 3 did not recall telling baphome1 her age but said that she thought she sounded 15 years old when they talked. While on a call, Baphome1 showed Minor Victim 3 a compilation video of males and females, approximately 20 to 30 people total, that he convinced to cut for "them" and write on the wall for "them." Minor Victim 3 thought that a majority of the people depicted in the compilation video were minors. Minor Victim 3 thought the compilation video baphome1 showed her was saved on baphome1's "PC" because she thought he shared his screen with her when he showed it to her. The video was 31 seconds long. Baphome1 said he lived in a single-family home and was between 125 to140 pounds and over 6 feet tall. Baphome1 asked Minor Victim 3 to kill her sister's dog which she said she would not do. Baphome1 told her he would hit a dog. Minor Victim 3 said that baphome1 said the "lowest age he would go" is 8 or 10 years old.

82. In September 2025, Minor Victim 4 was interviewed by law enforcement. Minor Victim 4 initially denied that she was the person communicating on Discord and that multiple

[18] Rubux is the virtual currency for the Roblox platform. Users can buy Rubux with real money, receive a monthly stipend from a Roblox Premium Subscription, or earn it by creating and selling games or items within the Roblox community.

unknown people had access to her Discord account. Later in the interview, Minor Victim 4 admitted to communicating with the people listed in the Cybertipline report on Discord. Minor Victim 4 denied harming herself and/or animals, as detailed in the Discord chat. According to Minor Victim 4, she did not know who the people she was talking to were; they were just people online.

83. On October 10, 2025, Minor Victim 2 was interviewed by law enforcement. Minor Victim 2 met "Leo" on Roblox through another user. Minor Victim 2 stated that Leo's Roblox username was "Departed49." Minor Victim 2 and Leo moved their conversation to Discord. Leo's Discord username was Baphome1. Leo introduced Minor Victim 2 to other Discord users. Leo told Minor Victim 2 that he was from Germany. Leo used the "burner phone number 469-389-1708." Minor Victim 2 described Leo as being a part of the group "764." Minor Victim 2 stated she was used by Leo and his online "friends" for self-harming content and sexually explicit images and videos. Minor Victim 2 advised that most of the sexually explicit videos she participated in were done over live video chat. Minor Victim 2 was told that if she did not do exactly what the individuals said, they threatened to harm her and her family, to "swat" her residence, and to send her videos and images out to her family and friends. Minor Victim 2 used the Discord account listed in Cybertipline Report 220150889 but she deleted it on September 20, 2025. Minor Victim 2 created a new Discord account, which she created on September 13, 2025. Minor Victim 2 stated that one of Leo's friends has tried to contact her on her new Discord account.

84. Telegram provided the following information in response to an administrative subpoena for the account @bloodovmen (provided by baphome1 to another user, mentioned above), the first Telegram username provided in the baphome1 chat on September 15, 2025:

@bloodovmen
User #: 7585434245

+18023481149[19] [LƐ·ȡ/rival NMK]
Last Login IP: 47.229.117.141[20] on 10/02/2025 21:43:27

85. Third party collection of Telegram messages sent by LEOh3ll, the Telegram user name provided in the baphome1 chat on September 15, 2025, revealed that the User ID for LEOh3ll is 8214631606.

86. Some of the third party collected chats sent by User ID 8214631606 include the following:

Date	Message
9/16/25	The last true owner of 764 was Riley
9/16/25	I will murder you
9/16/25	Sure I can kill you and rape your dead body
9/18/25	You have to se your members and groom people into doing irl now
9/20/25	Arson tonight in NMK ANNC
9/21/25	Literally rage baited her into leaking her own pussy
9/21/25	Abuse dm me Iâ€™ll send you her leaks
9/21/25	Nah we got more last night I se her into leaking more
9/21/25	This nat bitch will look back one day and realize her life was a joke and hopefully she becomes suicidal
9/22/25	tell them to poll me and him OG rival/leo 764
9/22/25	Iâ€™ll just go back to editing com and remain untouched yet again
9/25/25	I also want to fuck 3 year olds do you feel special?
9/26/25	Because I quit com to preach to young children (I rape them)
9/26/25	So you donâ€™t think I still have the clips?
9/26/25	I was 764 RIVAL/XV
10/3/25	Join my discord server
10/6/25	this is literal fed bait no clue why niggas wanna be 764 so bad in 2025
10/6/25	extortion com is dead

[19] This phone number is owned by Google. An administrative subpoena was sent requesting the subscriber information for the account. As of November 2, 2025, a response to the subpoena request has not been received.

[20] The IP address geolocates to California. An administrative subpoena was sent requesting the subscriber information for the account. As of November 2, 2025, a response to the subpoena request has not been received.

Date	Message
10/6/25	if you have me saved as leo or rival as a contact change the name to "..' now
10/8/25	Is this to store images videos and so on or could I also use this to communicate with people
10/8/25	Ok and last thing are you sure the data is encrypted and canâ€™t be accessed by outside sources
10/9/25	Slitowns ass
10/9/25	I leaked the roster too

87. Telegram provided the following information in response to an administrative subpoena for the following account:

User # 8214631606
@bloodovgirls
+14695604252[21] [O9A cunt]
Last Login IP: 38.83.114.20[22] on 10/16/2025 3:11:27

88. Roblox provided the following information in response to an administrative subpoena for the following account:

User ID:	8454497422
Roblox Username:	departed49
Email Accounts:	o6800917@gmail.com, kinishroxy@gmail.com
Telephone Number:	469-560-4252[23]
Creation Date:	05/11/2025

Several login IP addresses resolved back to a VPN. Another login IP address resolved back to **2716 Daisy Avenue, Halethorpe, Maryland**.

89. Google provided the following information in response to administrative subpoenas for the following accounts:

[21] The subscriber for this phone number has been obtained and is believed to belong to a separate witness or victim that has not been detailed in this affidavit.

[22] This IP address resolves back to a VPN company.

[23] This is the same phone number that was provided by Telegram and associated with the account @bloodovgirls and believed to belong to a separate witness or victim that has not been detailed in this affidavit.

a.

Email:	kinishroxy@gmail.com
Name:	Kinish Roxy
Created Date:	05/18/2024
Recovery SMS:	667-415-6879

Several login IP addresses resolved back to a VPN. Several login IP addresses resolved back to **2716 Daisy Avenue, Halethorpe, Maryland.**

b.

Google Voice:	469-389-1708[24]
Name:	John Gotii
Email:	johngotii25@gmail.com
Start Time:	01/10/2025
Subscriber Status:	Active
Subscriber Type:	Free

Several login IP addresses for the account johngotii25@gmail.com resolved back to a VPN. Several login IP addresses also resolved back to **2716 Daisy Avenue, Halethorpe, Maryland.**

90. AT&T provided the following information in response to an administrative subpoena associated for the phone number 667-415-6879, the recovery SMS for the email account kinishroxy@gmail.com and a phone number provided in the iCloud account details for emadison519@icloud.com:

Phone Number:	667-415-6879
Name:	Tiffany Lanahan
Address:	**2716 Daisy Avenue, Baltimore, MD 21227**
MSISDN Active:	03/04/2025 – Current (as of 07/07/2025)

91. On October 16, 2025, United States Magistrate Judge J. Mark Coulson, of the District of Maryland, issued search warrants (Case Nos. 25-mj-02679-JMC, 25-mj-02680-JMC, 25-mj-02681-JMC, 25-mj-02682-JMC) for the Discord account rwaping#0, the Google account associated with kinishroxy@gmail.com, and other online accounts and devices. As of October 29, 2025, the search warrant results have not been received from Discord. On November 2, 2025, United States Magistrate Judge Charles D. Austin, of the District of Maryland, issued search

[24] This phone number was provided by Minor Victim 2 as being used by "Leo".

warrant (Case No. 25-mj-2713-CDA) for the Discord account violentcore#0 and several other Discord accounts. As of November 2, 2025, the search warrant results have not been received from Discord.

92. A review of the search warrant results provided by Google for the account kinishroxy@gmail.com revealed the following emails:

a. On October 14, 2024, and May 31, 2025, kinishroxy@gmail.com received two emails from Discord with the subject line "Welcome to Discord."

b. On May 9, 2025, kinishroxy@gmail.com received an email with the subject line "Begin Your Career at Dollar Tree and Family Dollar." The body of the email stated, "Dear **Erik Madison**: Congratulations and welcome to the Dollar Tree and Family Dollar Team as PT SALES FLOOR ASSOCIATE."

c. On May 11, 2025, kinishroxy@gmail.com received an email with the subject line "Roblox Email Verification: Departed49." The body of the email stated, "Thanks for choosing to secure your Roblox account Departed49 by providing an email address."

d. On June 2, 2025, kinishroxy@gmail.com received an email with the subject line "Your order BBY01-807062310094 has been picked up." The body of the email indicated it was from Best Buy and stated "Thanks for shopping with us, Erik. This email is to confirm that your order was picked up on 06/02/2025 at the GLEN BURNIE MD Best Buy location." The item picked up was listed as a CyberPowerPC, Gamer Master Gaming Desktop.

e. On June 3, 2025, kinishroxy@gmail.com received three emails from Proton Mail. The first email had the subject line "Welcome to Proton VPN." The second email had the subject line "Verify your email to continue to Proton." The third email's subject line was "Discover all the features of your Proton account." The following was stated within the body of the third email "Your Proton Account gives you access to all Proton products for free: password manager, cloud storage, email, and Bitcoin wallet…," "Proton Pass saves all your passwords in one place and automates logins…," "Proton Drive is an end-to-end encrypted vault for all your files….," and "Proton Mail protects your emails with end-to-end and zero-access encryption so that no one – not even Proton – can read your emails but you."

f. On October 1, 2025, kinishroxy@gmail.com received an email with the subject line "Action Required: Return Your Breezeline Equipment to Avoid Charges." The body of the email stated, "Dear **Erik Madison**, We are reaching out on behalf of Breezeline regarding your past service. Our records indicate that your service was disconnected on 2025-06-21 at the address listed below: 416 Maryland Ave Apt 2, Cumberland, MD 21502."

93. On October 21, 2025, October 22, 2025, October 23, 2025, October 28, 2025, and October 30, 2025, surveillance was conducted at **2716 Daisy Avenue, Baltimore, MD 21227**. On those days, Madison was observed leaving and returning to the residence on foot or in a red vehicle as a passenger. The vehicle was believed to be driven by Madison's stepfather.

PRIOR INVESTIGATIONS INTO ERIK MADISON

May 2020 Distribution of Child Pornography Investigation

94. According to a May 2020 Baltimore County Police report, a detective was assigned to investigate a Cybertipline Report submitted by Instagram. The Cybertipline Report detailed that a specific account sent a file of child pornography to another user. Through his investigation, which included a search warrant of the Instagram account in question, the detective determined the user of the Instagram account was **Erik Madison** ("Madison"), born in 2005 and who was a minor at the time. Madison resided at **2716 Daisy Avenue, Halethorpe, Maryland**. In June 2020, the detective spoke to both Erik and his mother about the Cybertipline Report. Madison admitted the account in the Cybertipline Report was his and that he sent the image. The detective explained Maryland child pornography laws, appropriate internet behavior and the proper supervision of teenagers on the internet. The case was closed.

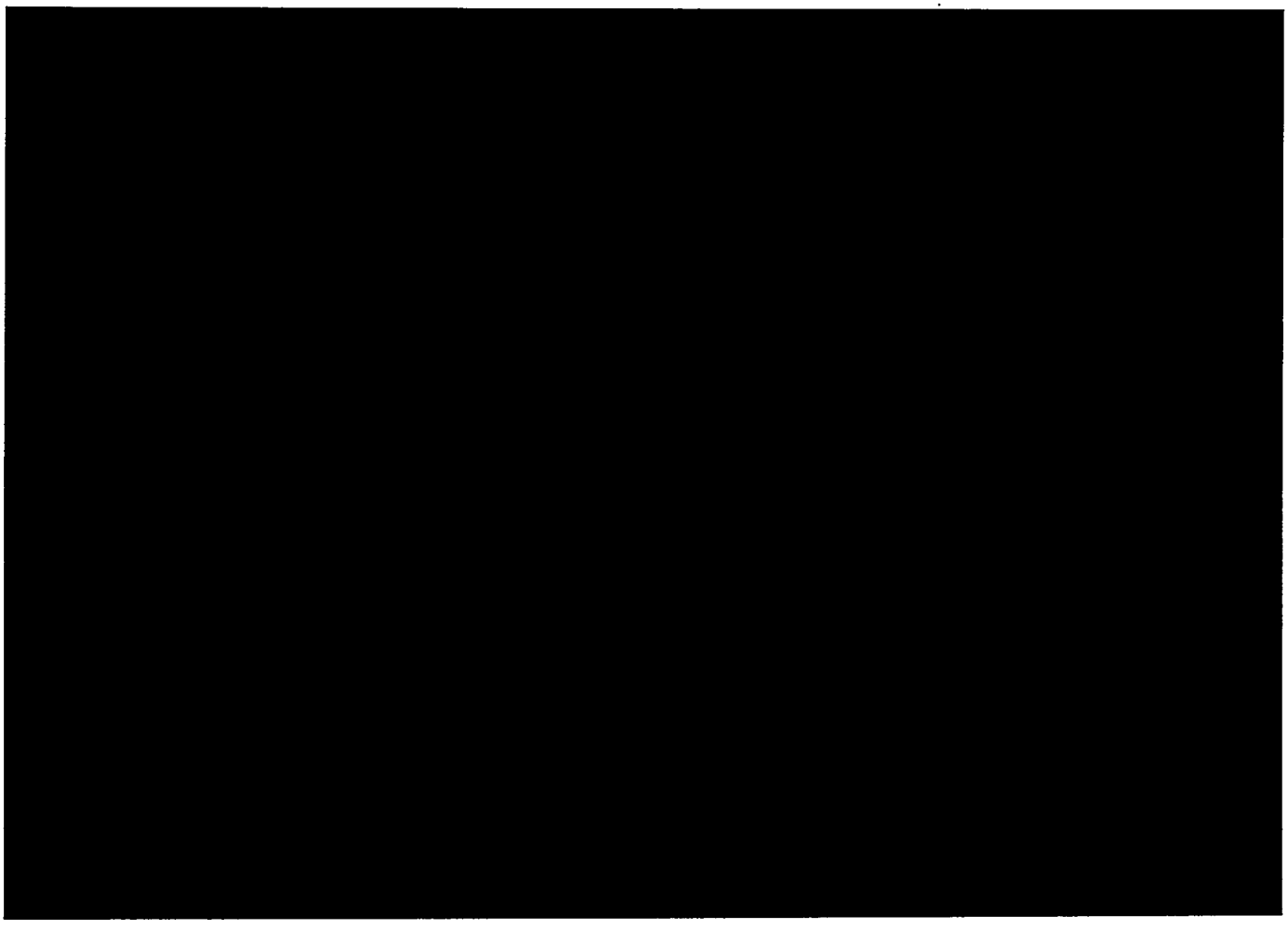
February 2022 Online Child Exploitation Investigation

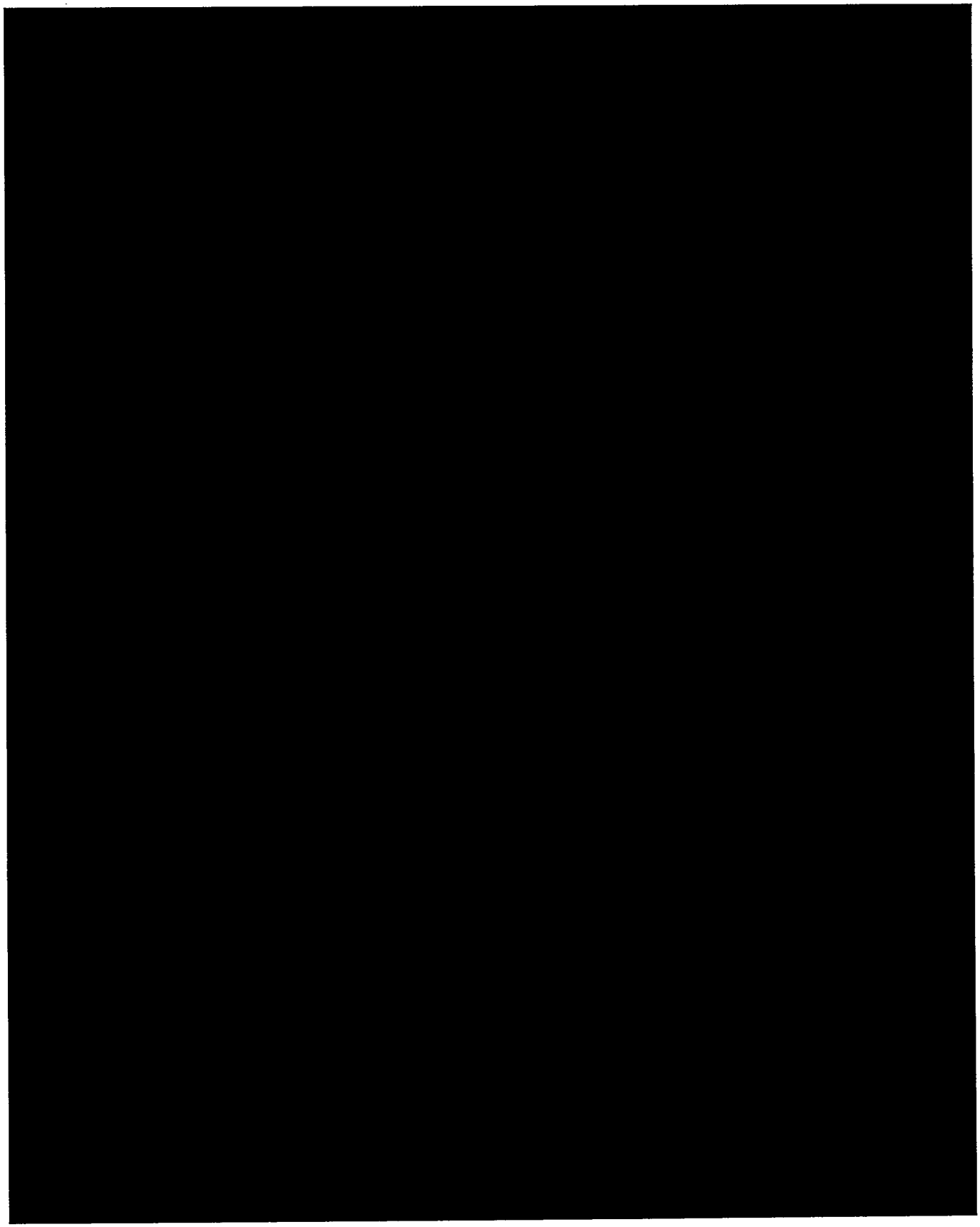
95. According to a February 2022 Baltimore FBI interview report, Madison, a minor at the time, was interviewed at his residence at **2716 Daisy Avenue, Halethorpe, Maryland** by an FBI Agent and Baltimore County Task Force Officer, with his mother's consent. Madison admitted to communicating with a minor female on Instagram and Snapchat who had sent him naked pictures. The victim then later blocked Madison's accounts and Madison created new accounts to continue to attempt to communicate with her. The victim's parents reported to law

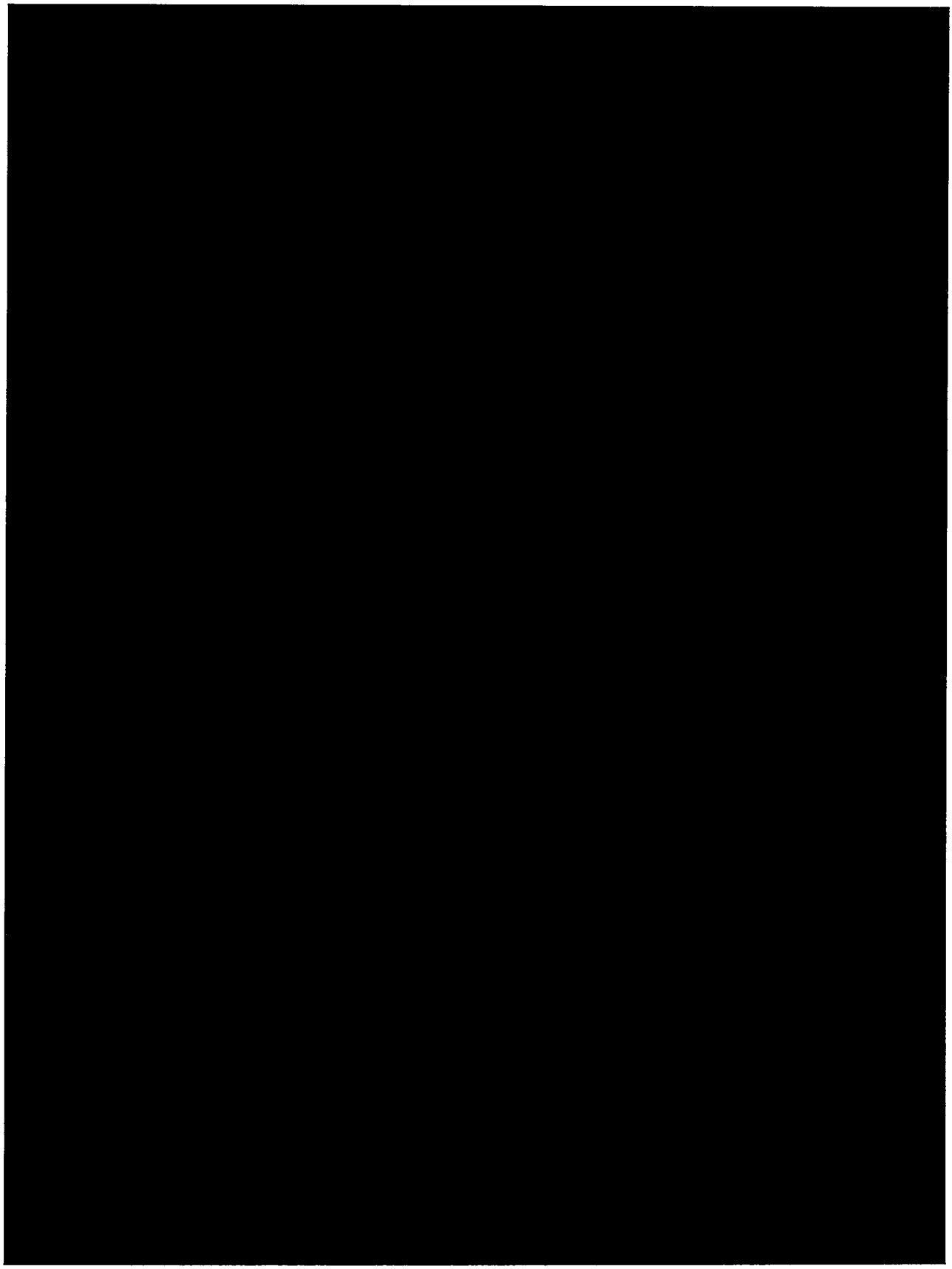
enforcement that Madison possessed child pornography and was "stalking" the minor female. Madison was advised to cease the online communications with the minor female and was advised about the legal consequences of his actions.

February 2022 Online Bestiality Investigation

96. According to a June 2022 Baltimore County Police report, while a minor, Madison posted a video online of him sexually abusing his dog. During the investigation, law enforcement seized Madison's phone and obtained a warrant to search the phone. The cell phone was associated with the phone number 240-360-3496. During the forensic examination of the cell phone, files of child pornography were located. Erik was charged as a juvenile with animal abuse and possession of child pornography.







SUMMARY

103. Based on the facts detailed above, as well as my training and experience, Madison appears to have a sexual interest in children that includes engaging in sex acts with minor females, producing through live streaming images and/or videos of such conduct, producing through live streaming images of minor females cutting themselves, often while engaging in sexually explicit conduct, and saving videos of such conduct and distributing the videos to others. Madison also uses various social media platforms to exploit minors. Further, Madison maintains and controls numerous social networking and email that appear to be used to commit the TARGET OFFENSES.

104. Based on my training and experience, as well as the activity detailed above, I believe that Madison displays characteristics common to individuals who have a sexual interest in children, and who access with the intent to view and/or, possess, collect, receive, produce, and distribute child pornography as discussed in paragraphs 6 and 7 above. I also believe that Madison displays the characteristics common to individuals who are involved in nihilistic violent extremism groups such as "764," as discussed in paragraphs 11 through 19 above

105. Based on these characteristics, and because the TARGET ACCOUNTS and TARGET LOCATIONS that are the subject of this affidavit appear to be accessed, controlled, and/or created by Madison, I respectfully submit there is probable cause that the TARGET LOCATIONS (1) contain evidence of the TARGET OFFENSES, and (2) are relevant to determine the ownership and control of the various accounts used to committed the TARGET OFFENSES. Based on my training and experience, such information may constitute evidence of the TARGET OFFENSES because the information can be used to identify the account's user or users.

CONCLUSION

106. Based on the foregoing information, I have probable cause to believe that contraband, and evidence, fruits, and instrumentalities of violations of the TARGET OFFENSES as set forth herein and in Attachments B1, B2, and B3 are currently contained in the TARGET ACCOUNTS and TARGET LOCATIONS, more fully described in Attachments A1, A2, and A3. I therefore respectfully request that the search warrant be issued authorizing the search of the TARGET ACCOUNTS and TARGET LOCATIONS for the items described above and in Attachments B1, B2, and B3, and authorizing the seizure and examination of any such items found therein.

Rachel S. Corn
Special Agent Rachel S. Corn
Federal Bureau of Investigation

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4.1 and Fed. R. Crim. P. 41(d)(3) this 4th day of November, 2025.

Honorable Douglas R. Miller
United States Magistrate Judge
District of Maryland