IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH THE DISCORD ACCOUNTS IDENTIFIED IN ATTACHMENT A-1	**Case No.** 22-mj-1930-TJS
IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH THE GOOGLE ACCOUNTS IDENTIFIED IN ATTACHMENT A-2	**Case No.** 22-mj-1931-TJS
IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH THE REDDIT ACCOUNTS IDENTIFIED IN ATTACHMENT A-3	**Case No.** 22-mj-1932-TJS

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Ian Montijo, being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"). As such, I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a Government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. I have been employed by the FBI since January 2020. I am currently assigned to the FBI's Baltimore Division with the Joint Terrorism Task Force ("JTTF"). Previously, I spent four years in the United States Marine Corps serving as an Intelligence Officer. During my tenure with the FBI, I have gained knowledge in the use of various investigative techniques including the utilization of location data, physical surveillance, investigative interviews, the service of Grand Jury Subpoenas, and

the execution of search and arrest warrants primarily in domestic terrorism investigations. From these experiences, I have become familiar with the ways in which persons plan and conduct criminal activities, to include but not limited to, the efforts persons involved in such activity take to disguise operations and avoid detection by law enforcement. Through training, education, and experience, I have become familiar with the lengths to which anti-government and anti-authority extremists will go to conceal their illegal activity. I have also become familiar with their particular techniques, such as using cryptic language, family resources, false identities, encrypted technology and the like to thwart law enforcement investigations.

2. I make this affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703 for the following electronic and telecommunications services accounts (collectively the "**TARGET ACCOUNTS**"):

a. **Discord Accounts**: records and information stored and premises owned, maintained, controlled, or operated by Discord, a company located at 444 De Haro Street, San Francisco, California 94107, and associated with the following Discord account usernames and e-mail addresses, further identified in Attachment A-1, to search for information further described in Attachment B-1:

1) The Discord account associated with **roskenicholas@gmail.com**, and with the username "Sophie42#6535" ("**TARGET DISCORD-1**"). Information specific to this account is set forth in paragraphs 9–11 and 13-14 below;

2) The Discord account associated with **pyronick7@gmail.com**, and with the username "AmericanSophie#1595" ("**TARGET DISCORD-2**"). Information specific to this account is set forth in paragraph 11 below;

b. **Google Accounts:** records and information stored at premises owned, maintained, controlled, or operated by Google LLC, a business headquartered at 1600 Amphitheater Parkway, Mountain View, CA 94043, and associated with the following Google accounts, further described in Attachment A-2, to search for information further described in Attachment B-2:

1) **roskenicholas@gmail.com** ("**TARGET EMAIL-1**"). Information specific to this account is set forth in paragraphs 8-11 below;

2) **pyronick7@gmail.com ("TARGET EMAIL-2").** Information specific to this account is set forth in paragraphs 8-9 below;

3) **JotunnJotnar@gmail.com** ("**TARGET EMAIL-3**"). Information specific to this account is set forth in paragraph 9 below;

4) **helenkiller1969@gmail.com** ("**TARGET EMAIL-4**"). Information specific to this account is set forth in paragraph 9-10 below;

c. **Reddit Accounts**: records and information stored at premises owned, maintained, controlled, or operated by Reddit, a company located at 2710 Gateway Oaks Drive, Suite 150N, Sacramento, California 95833, and associated with following Reddit accounts, further described in Attachment A-3, to search for information further described in Attachment B-3:

1) The Reddit account associated with e-mail address r**oskenicholas@gmail.com**, username "AmericanNick" and UserID "th12v" ("**TARGET REDDIT-1**"). Information specific to this account is set forth in paragraph 9 below;

2) The Reddit account associated with e-mail address **pyronick7@gmail.com**, username "AmericanNick7" and UserID "97h5ic" ("**TARGET REDDIT-2**"). Information specific to this account is set forth in paragraphs 8-9 below;

3) The Reddit account associated with username "AmericanPyro" ("**TARGET REDDIT-3**"). Information specific to this account is set forth in paragraph 9 below; and

4) The Reddit account associated with e-mail address **helenkiller1969@gmail.com**, username "Narrow_Frosting_1539" and UserID "c9dqz5I2" ("**TARGET REDDIT-4**"). Information specific to this account is set forth in paragraphs 9-10 below.

3. Based on the facts set forth in this Affidavit, I respectfully submit that there is probable cause to believe that the **TARGET ACCOUNTS** contain evidence of the following criminal offenses: 18 U.S.C. § 115(a)(1)(B) (threatening to murder a United States Judge) and 18 U.S.C § 351(c) (Attempt to Assassinate Justice of United States).

PROBABLE CAUSE

4. On June 8, 2022, at approximately 1:05 a.m., two United States Deputy Marshals saw an individual dressed in dark clothing and carrying a backpack and a suitcase, get out of a taxicab that had stopped in front of the Montgomery County, Maryland residence of a current Justice of the United States Supreme Court. The individual looked at the two Deputy U.S. Marshals, who were standing next to their parked vehicle, and then turned to walk down the street.

5. Shortly thereafter, Montgomery County Emergency Communications Center fielded a call from an individual who identified himself as NICHOLAS ROSKE. ROSKE informed the call taker that he was having suicidal and homicidal thoughts and that he had a firearm in his suitcase. ROSKE also told the call taker he came from California to kill a specific United States Supreme Court Justice. Montgomery County Police Department officers were dispatched to the location near the Supreme Court Justice's residence where they encountered ROSKE, who was still on the telephone with the Montgomery County Emergency Communications Center. ROSKE was taken into custody without incident and law enforcement officers seized ROSKE's possessions, including ROSKE's cell phone, backpack, and suitcase.

6. A search of the seized suitcase and backpack revealed a black tactical chest rig and tactical knife, a Glock 17 pistol with two magazines and ammunition, pepper spray, zip ties, a hammer, screwdriver, nail punch, crowbar, pistol light, duct tape, hiking boots with padding on the outside of the soles, and other items.

7. After being transported to the Montgomery County Police Department Second District Precinct, a detective advised ROSKE of his constitutional rights. ROSKE indicated that he understood his rights, agreed to speak with the detective, and signed a written waiver to that effect. ROSKE then told the detective that he was upset about the leak of a recent Supreme Court draft decision regarding the right to abortion as well as the recent school shooting in Uvalde, Texas. ROSKE indicated that he believed the Justice who he intended to kill would side with Second Amendment decisions that would loosen gun control laws. ROSKE stated that he began thinking about how to give his life a purpose and decided that he would kill the Supreme Court Justice. ROSKE identified the Justice's Montgomery County address by researching the topic on the Internet. ROSKE further indicated that he had purchased the Glock pistol and other items for

the purpose of breaking into the Justice's residence and killing the Justice as well as himself. ROSKE told the detective that the telephone seized from his person was his cell phone, and he provided the telephone number associated with it.

8. FBI Agents conducted a second interview of ROSKE at approximately 9:54 a.m. on June 8, 2022. ROSKE was advised for a second time of his constitutional rights and waived those rights in writing. Among other things, ROSKE admitted again that he had traveled to the Montgomery County residence with the intent to break into the Justice's house and to kill the Justice and then himself. ROSKE stated that he had researched the location of the Justice's house and how to carry out his plan on an Acer laptop. ROSKE also stated that he used Reddit, Google, and other online forums to learn the skills he thought were necessary to complete his plan. ROSKE identified two Google accounts that he used to conduct that research as **roskenicholas@gmail.com** (**TARGET EMAIL-1**) and **pyronick7@gmail.com** (**TARGET EMAIL-2**). ROSKE further stated he had a Discord account but that he deleted the account on Sunday, June 5, 2022. ROSKE said that he used his Reddit account to ask individuals, who were unknown to him, questions in order to refine his plan to kill the Justice. ROSKE also stated that on Monday, June 6, 2022, he attempted to use the settings menu on the Acer laptop to conduct a data wipe of the device because ROSKE did not want anyone he conversed with to be implicated as a result of his actions.

9. The FBI took custody of ROSKE's cell phone from the Montgomery County Police Department on June 8, 2022, at approximately 8:45 am. On June 9, 2022, pursuant to a federal search warrant authorized earlier that day by United States Magistrate Judge Timothy J. Sullivan (*see* Case No. 22-mj-1856-TJS), FBI Agents conducted an extraction of ROSKE's cell phone. An initial inspection of that extraction revealed the following accounts were accessed

through or otherwise associated with ROSKE's cell phone:

Account Type	Account Identifier(s)
Google	Email: roskenicholas@gmail.com (**TARGET EMAIL-1**)
Google	Email: pyronick7@gmail.com **(TARGET EMAIL-2)**
Google	Email: JotunnJotnar@gmail.com **(TARGET EMAIL- 3)**
Google	Email: helenkiller1969@gmail.com **(TARGET EMAIL-4)**
Reddit	Username: AmericanNick (**TARGET REDDIT-1**) User ID: thl2v Associated Email: roskenicholas@gmail.com
Reddit	Username: AmericanNick7 **(TARGET REDDIT-2)** User ID: 97h5ic Associated Email: pyronick7@gmail.com
Reddit	Username: AmericanPyro[1] **(TARGET REDDIT-3)**
Reddit	Username: Narrow_Frosting_1539 **(TARGET REDDIT-4)** User ID: c9dqz5I2 Associated Email: helenkiller1969@gmail.com
Discord	Username: roskenicholas@gmail.com **(TARGET DISCORD-1)**

[1] The data extracted from ROSKE's cell phone did not reflect an email address or any UserID information associated with **TARGET REDDIT-3** as was the case with **TARGET REDDIT-1, TARGET REDDIT-2**, and **TARGET REDDIT-4.** Based on the similarity of the username "AmericanPyro" to other usernames and accounts for which there is further information corroborating a connection to ROSKE, such as "AmericanNick," "pyronick7@gmail.com," and "AmericanNick7," and the presence of digital evidence, which when categorized, placed the username "AmericanPyro" with information from ROSKE's other accounts which were logged into ROSKE's phone, I submit that there is probable cause to believe that ROSKE operated or controlled **TARGET REDDIT-3** and that **TARGET REDDIT-3** contains evidence of the Target Offenses.

10. An initial review of the contents of ROSKE's cell phone revealed the following:.

a. On May 10, 2022, under the Reddit page r/TwoXChromosomes, **TARGET REDDIT-4** posted the text "Would Kavanaugh being removed from the SC help women long term?"

b. On May 25, 2022, **TARGET EMAIL-1** received an email from info@smokinbarrelguns.com that stated "We appreciate you stopping by and checking out our range and training facility. As a thank you, we would like to give you $5 dollars off your next visit."

c. On May 27, 2022, **TARGET EMAIL-1** received an email from sales@southord.com with an order confirmation for a Snap Gun Lock Pick for $49.95 and an order number of #35710.

d. On June 6, 2022, **TARGET EMAIL-1** received an email from noreply@discord.com addressed to "Sophie42." The email stated Discord had received a request to permanently delete the Sophie42 Discord account (**TARGET DISCORD-1**). The email further stated the Sophie42 Discord account was deactivated and that it would be deleted in fourteen days.[2]

e. On June 6, 2022, **TARGET EMAIL-4** received an email from Reddit that showed Reddit user u/13804 replied to **TARGET REDDIT-4**'s comment on the Reddit page r/USMC. According to that email, 34 minutes earlier, **TARGET**

[2] The FBI served a preservation letter on Discord for all data connected to Discord accounts connected to **TARGET EMAILS 1** and **2**, which I know, based on a subsequent response received from Discord, included **TARGET DISCORD-1** and **TARGET DISCORD-2**. Based on my experience and knowledge, I know that data in a Discord account is often still available even after the user deletes the account.

REDDIT-4 had posted the following: "How difficult is it to covertly take out an HVT?" Based on my training, knowledge, and experience, I believe "HVT" to refer to "High Value Target."

f. Between May 5, 2022 and June 8, 2022, the search history on ROSKE's cell phone included the following terms or phrases: "quietest semi auto rifle," "Reagan assassination attempt," "most effective place to stab someone," "assassin skills," "assassin equipment," "assassinations," "supreme court," "how to be stealthy," "gun lubricant," and "supreme court" among other things.

g. A review of the web history on ROSKE's phone revealed visits to the "Current Members" page of the Supreme Court of the United States' website ("https://www.supremecourt.gov/about/biographies.aspx"), and the "List of assassinations" page on Wikipedia ("https://en.m.wikipedia.org/wiki/List_of_assassinations").

11. Subscriber information from Discord revealed that the **TARGET DISCORD-1** was connected to **TARGET EMAIL-1** and ROSKE's known cell phone number. Discord subscriber information also connected **TARGET DISCORD-2** to **TARGET EMAIL-2**.

12. Based on my knowledge and experience, I know that individuals who use Discord accounts often join Discord servers which corollate to specific Reddit threads. Based on my knowledge and experience, I also know that Reddit comments and threads are publicly visible. If a Reddit user wants to converse privately with individuals active on a particular Reddit thread, who may claim to have expertise, knowledge, or interest in the topic of that thread, that user must seek out those individuals on a different platform. Because Discord often has servers and channels which are the analog of Reddit threads, Reddit users go to Discord to engage with a

similar group or the same individuals in order to obtain the information they seek. On Discord, the conversations may take place in private messages (direct messages) or in servers and channels which may be restricted or otherwise obscured from public view.

13. During his interview with the FBI on June 8, 2022, ROSKE identified an associate (hereinafter "Person #1") as someone with whom he discussed the leaked Supreme Court draft opinion. On June 13, 2022, FBI agents interviewed Person #1, who advised that in the weeks leading to up to June 8, 2022, Person #1 and ROSKE used Discord to communicate. Person #1 stated that ROSKE'S Discord username was Sophie42. [3] Person #1 provided consent for agents to review Person #1's Discord communications with ROSKE.

14. In reviewing those Discord communications, FBI agents discovered the following exchange, dated May 25, 2022, between Person #1 and Sophie 42 (ROSKE):

ROSKE: im gonna stop roe v wade from being overturned

Person #1: what u tryna do

ROSKE: remove some people from the supreme court

Person #1: u gonna Tun? Run?

ROSKE: after you mean?

Person #1: oh haha good one
Two dead judges ain't gonna do nothing
The whole government is fucked
There's no fixing that
You would die before you killed them all

ROSKE: yeah but I could get at least one, which would change the votes for decades to come, and I am shooting for 3

[3] Based on my knowledge and experience, I know that Discord users refer to accounts or users by the portion of the username that precedes the hashtag or pound sign and the trailing four digits of a user name. Those four digits are often randomly generated and can change intermittently. Therefore, I believe that Person #1's reference to Sophie42 corresponded to **TARGET DISCORD-1.**

> all of the major decisions for the past 10 years have been along party lines so if there are more liberal than conservative judges, they will have the power

15. I also know, based on my knowledge and experience, that conversations between users which begin on one platform, website, or application, may migrate to other sites or encrypted chat applications. For example, in this case specifically, a screenshot located on ROSKE's cell phone depicts a text message conversation with an individual (hereinafter "Person #2") whom ROSKE identified in his interview with FBI Agents. In this conversation, Person #2 stated, "Idk if you're getting these messages because I don' think androids have iMessage on them". ROSKE responded, "I only got the last one. WhatsApp or discord is better." Person #2 later confirmed to the FBI that Person #2 communicated with ROSKE via Discord.

16. When communications online move from one platform to another, messages and links indicating such activity are stored not only in the messages themselves, but also in e-mail notifications (*see* ¶10d and 10e of this affidavit) and other messages as the result of two-factor authentication and other account creation requirements. Based on the interconnected nature of various online accounts, the nature of modern, online communication, and criminal actors' attempts to conceal their illegal activity, there is probable cause to believe that all of the **TARGET ACCOUNTS** contain evidence of ROSKE's criminal activity.

CONCLUSION

17. For these reasons, I submit that there is probable cause to believe the **TARGET ACCOUNTS** will contain evidence, fruits and instrumentalities of violations of 18 U.S.C. § 115(a)(1)(B) (Threatening United States Judge), 18 U.S.C. § 351(c) (Attempt to Kill Justice of the United States), as described in Attachments B-1, B-2 and B-3.

18. Therefore, in consideration of the facts presented, I respectfully request that this Court issue search warrants for the **TARGET ACCOUNTS**, more fully described in

Attachments A-1, A-2, and A-3, and authorize the seizure of the items described in Attachments B-1, B-2, and B-3.

19. This Court has jurisdiction to issue the requested warrants because it is "a court of competent jurisdiction," as defined by 18 U.S.C. § 2711. 18 U.S.C. § § 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, this "Court is a district court of the United States that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

20. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of these warrants. The government will execute these warrants by serving them on Discord, Google and Reddit (the "Service Providers") respectively. Because warrants will be served on the Service Providers, who will then compile the records at a time convenient to each Service Provider, reasonable cause exists to permit the execution of the requested warrants at any time in the day or night.

Respectfully Submitted,

Ian Montijo
Ian Montijo
Special Agent, FBI

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4.1 and 41(d)(3) this 21st day of June, 2022.

The Honorable Timothy J. Sullivan
United States Magistrate Judge

ATTACHMENT A-1

Property to Be Searched

This warrant applies to information which is associated with any Discord account that is owned, maintained, or controlled by Discord, a company located at 444 De Haro Street, San Francisco, California 94107, that is associated with:

1. e-mail address **roskenicholas@gmail.com** and username **Sophie42#6535**;
2. e-mail address **pyronick7@gmail.com** and username **AmericanSophie#1595**.

ATTACHMENT B-1

Particular Things to Be Seized

I. Information to be disclosed by Discord

To the extent that the information described in Attachment A-1 is within the possession, custody, or control of Discord, regardless of whether such information is stored, held or maintained inside or outside the United States, and including any information that has been deleted but is still available, or has been preserved pursuant to a legal request, Discord is required to disclose to the government the following information for the account identifiers listed in Attachment A-1, along with any other accounts linked by shared attributes such as phone number, email, browser or site cookie, session, or device, for the time period **from January 1, 2022 to the present**:

a. The contents of all communications, including written, audio, and images, sent to and from the account(s), and the user account contact information associated with the source and destination of each communication, the date and time at which each communication was sent, and any IP address, port number, or session numbers associated with the sender and the recipient of the communications;

b. All records or other identification regarding the identifiers listed in Attachment A-1, to include full name, email address, physical address, telephone numbers and other identifiers (including, but not limited to screen names, passwords, and websites), records of session times and durations, the date on which the account was created, the length of service, the Internet Protocol address used to register/create the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, means and source of payment (including any credit or bank account

numbers), other associated accounts connected or linked to the account (for example by cookie, device, telephone or SMS number, or secondary email address), and device-specific information (such as hardware model, operating system version, unique device identifiers, and mobile network information including phone number);

c. The types of service utilized by the associated account(s);

d. All records pertaining to communications between Discord and any other person regarding the account(s) identified in Attachment A-1, including contacts with support services and records of actions taken, to include claims or "flags" for violations of Terms of Service or Community Guidelines committed by the account(s) identified in Attachment A-1;

e. All records or other information stored by any individual using the account, including address books, contacts and buddy lists, servers the user participates in, pictures and files;

f. All records and information relating to the location, past or present, of any individual using the account(s);

g. Metadata for images that are associated with the account(s);

h. All other records pertaining to the devices and computers from which the account(s) downloaded or accessed any Discord service or to which any Discord service was synced, including telephone number, model number, MAC addresses, Electronic Serial Numbers (ESN), Mobile Electronic Identity Numbers (MEIN), Mobile Equipment Identifier (MEID), Mobile Identification Numbers (MIN), Subscriber Identity Modules (SIM), Mobile Subscriber Integrated Services Digital Network Number (MSISDN), International Mobile Subscriber Identifiers (IMSI) or International Mobile Subscriber Identities (IMEI).

II. Information to be seized by the Government

All information described above in Section I that constitutes evidence and instrumentalities of violations of 18 U.S.C. § 115(a)(1)(B) (threatening to murder a United States Supreme Court Justice) and 18 U.S.C § 351(c) (attempt to assassinate Justice of United States), (the Target Offenses") including but not limited to the following:

a. Evidence of communication and actions as they relate to the Target Offenses;

b. Evidence indicating how and when the account(s) was accessed or used, to determine the geographic and chronological context of events relating to the Target Offenses;

c. Evidence relating to any credit or bank account numbers used by the account(s) users and co-conspirators in connection with the commission of the Target Offenses ;

d. Evidence reasonably indicating the account users' and co-conspirators' state of mind as it relates to the Target Offenses;

e. Evidence indicating the identity of the person who used the account(s); and

f. Evidence that may identify any co-conspirators or other persons relevant to the Target Offenses, including records that help reveal the whereabouts of any such persons.

This warrant authorizes a review of electronically stored information, communications, and other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities of the Target Offenses. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

With respect to the search of the information provided pursuant to this warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable. If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review. The investigative team will take no further steps regarding any review of information so segregated absent further order of the court. The investigative team may continue to review any information not segregated as potentially privileged.

ATTACHMENT A-2

Property to Be Searched

This warrant applies to information which is associated with the Google accounts:

1) **roskenicholas@gmail.com** ;

2) **pyronick7@gmail.com;**

3) **JotunnJotnar@gmail.com; and**

4) helenkiller1969@gmail.com

that are stored at premises owned, maintained, controlled, or operated by Google, LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California.

ATTACHMENT B-2

Particular Things to be Seized

I. Information to be disclosed by Google, LLC (the "Provider")

To the extent that the information described in Attachment A-2 is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment B-1, all for the time period **from January 1, 2022 through the present**:

A. Google Account Information

1. Google account registration information, including name, user-specified contact information, recovery email address, recovery SMS number, account creation timestamp and IP address, and a list of Google services the account holder has enabled or accessed;

2. Account change history IP addresses and associated timestamps;

3. Google account login and logout IP addresses and associated timestamps;

4. All means and sources of payment for all Google products and services (including complete credit or bank account numbers), and detailed billing records;

5. All cookie and user-specific advertising data, including third-party cookies;

B. Gmail Account Information

6. Gmail specific subscriber information, login and logout IP addresses and associated timestamps;

7. Gmail specific non-content email header information, originating message IP addresses, and account settings;

8. The contents of all e-mails, attachments and chat messages stored in the account, including copies of e-mails sent to and from the account, draft e-mails, the source and destination e-mails sent addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;

9. Contents of all available deleted emails;

C. Google Voice Account Information

10. Voice specific subscriber information, including signup IP and associated timestamp and user-provided name;

11. Most recent 28 days of call and text logs;

12. All account settings and account change history;

13. Contents of all voicemail messages and text messages;

D. Android Account Information

14. Android specific subscriber and IP address information, including associated timestamps;

15. All device IDs, IMEIs, and MEIDs associated with the target account(s);

16. Timestamps, including device registration, first check-in, and last check-in;

17. All Google accounts tied to the Android device(s) if any;

18. Android hardware information;

19. Cell carrier/service provider;

20. All apps downloaded to the device;

E. Google Location and Search History Information

21. All location history with associated timestamps;

22. All search history and associated timestamps, including all "clicks" and "queries;"

F. Photos Account Information

1. Photos specific subscriber and IP address information, including associated timestamps;

2. All upload IP addresses and associated timestamps;

3. Contents of all Photos and Albums, including all exif data included by the user as part of the upload;

G. Drive Account Information

4. Drive specific subscriber and IP address information, including associated timestamps;

5. All upload IP addresses and associated timestamps;

6. All Drive content, including Docs, Sheets and Slides;

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. § 115(a)(1)(B) (threat to murder a United States Supreme Court Justice); and 18 U.S.C § 351(c) (attempt to assassinate Justice of United States), ("the Subject Offenses"), those violations involving the individuals identified in the affidavit as well as their co-conspirators, including but not limited to, for each account or identifier listed on Attachment B-1, information pertaining to the following matters:

(a) Records regarding any violation of the Subject Offenses, including but not limited to planning, preparing, and staging for any Subject Offense; the purchase or procurement of any firearms, ammunitions, other weapons, or explosives; and the selection of targets;

(b) All images, messages, communications, calendar entries, and contacts, including any and all preparatory steps taken in furtherance of the Subject Offenses;

(c) Communication, information, documentation and records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts;

(d) Evidence of the times the account was used;

(e) All images, messages and communications regarding wiping software, encryption or other methods to avoid detection by law enforcement;

(f) Passwords and encryption keys, and other access information that may be necessary to access the account and other associated accounts;

(g) Credit card and other financial information, including but not limited to, bills and payment records evidencing ownership of the subject account;

(h) All "address books" or other lists of contacts.

(i) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the Subject Offenses and to the email account owner;

(j) Evidence indicating the email account owner's state of mind as it relates to the Subject Offenses;

(k) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

(l) The identity of the person(s) who communicated with the user ID about the Subject Offenses, including records that help reveal the whereabouts of any such persons.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

With respect to the search of the information provided pursuant to this warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable. If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review. The investigative team will take no further steps regarding any review of information so segregated absent further order of the court. The investigative team may continue to review any information not segregated as potentially privileged.

ATTACHMENT A-3

Property to Be Searched

This warrant applies to records and information associated with any Reddit accounts associated with the following information:

1. The e-mail address r**oskenicholas@gmail.com**, associated with username **AmericanNick** and UserID **th12v**;
2. The e-mail address **pyronick7@gmail.com**, associated with username **AmericanNick7** and UserID **97h5ic**;
3. The username **AmericanPyro**; and
4. The e-mail address **helenkiller1969@gmail.com**, associated with username **Narrow_Frosting_1539** and UserID **c9dqz5I2**,

that are stored at premises owned, maintained, controlled, or operated by Reddit, a company located at 2710 Gateway Oaks Drive, Suite 150N, Sacramento, California 95833.

ATTACHMENT B-3

Particular Things to Be Seized

I. Information to be disclosed by Reddit

To the extent that the information described in Attachment A-1 is within the possession, custody, or control of Reddit, regardless of whether such information is stored, held or maintained inside or outside the United States, and including any information that has been deleted but is still available, or has been preserved pursuant to a legal request, Reddit is required to disclose to the government the following information for the Reddit account identifiers listed in Attachment A-1, along with any other Reddit accounts linked by shared attributes such as phone number, email, browser or site cookie, session, or device, for the time period **from January 1, 2022 to the present**:

a. The contents of all communications, including written, audio, and images, sent to and from the account(s), and the user account contact information associated with the source and destination of each communication, the date and time at which each communication was sent, and any IP address, port number, or session numbers associated with the sender and the recipient of the communications;

b. All records or other identification regarding the identifiers listed in Attachment A-3, to include full name, email address, physical address, telephone numbers and other identifiers (including, but not limited to screen names, passwords, and websites), records of session times and durations, the date on which the account was created, the length of service, the Internet Protocol address used to register/create the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, means and source of payment (including any credit or bank account

numbers), other associated accounts connected or linked to the account (for example by cookie, device, telephone or SMS number, or secondary email address), and device-specific information (such as hardware model, operating system version, unique device identifiers, and mobile network information including phone number);

c. The types of service utilized by the associated account(s);

d. All records pertaining to communications between Reddit and any other person regarding the account(s) identified in Attachment A-1, including contacts with support services and records of actions taken, to include claims or "flags" for violations of Terms of Service or Community Guidelines committed by the account(s) identified in Attachment A-3;

e. All records or other information stored by any individual using the account, including address books, contacts and buddy lists, servers the user participates in, pictures and files;

f. All records and information relating to the location, past or present, of any individual using the account(s);

g. Metadata for images that are associated with the account(s);

h. All other records pertaining to the devices and computers from which the account(s) downloaded or accessed any Reddit service or to which any Reddit was synced, including telephone number, model number, MAC addresses, Electronic Serial Numbers (ESN), Mobile Electronic Identity Numbers (MEIN), Mobile Equipment Identifier (MEID), Mobile Identification Numbers (MIN), Subscriber Identity Modules (SIM), Mobile Subscriber Integrated Services Digital Network Number (MSISDN), International Mobile Subscriber Identifiers (IMSI) or International Mobile Subscriber Identities (IMEI).

II. Information to be seized by the Government

All information described above in Section I that constitutes evidence, fruits and instrumentalities of violations of 18 U.S.C. § 115(a)(1)(B) (threatening to murder a United States Supreme Court Justice); and 18 U.S.C § 351(c) (attempt to assassinate Justice of United States), ("the Subject Offenses"), including but not limited to the following:

a. Evidence of communication and actions that relate to the Subject Offenses;

b. Evidence indicating how and when the account(s) was accessed or used, to determine the geographic and chronological context of events relating to the crimes under investigation;

c. Evidence relating to any credit or bank account numbers used by the account(s) users and co-conspirators during or in preparation for the commission of the Subject Offenses;

d. Evidence reasonably indicating the account users' and co-conspirators' state of mind as it relates to the Subject Offenses;

e. Evidence indicating the identity of the person who used the account(s);

f. Evidence that may identify any co-conspirators or other persons relevant to the Subject Offenses, including records that help reveal whereabouts of such persons.

This warrant authorizes a review of electronically stored information, communications, and other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

With respect to the search of the information provided pursuant to this warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable. If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review. The investigative team will take no further steps regarding any review of information so segregated absent further order of the court. The investigative team may continue to review any information not segregated as potentially privileged.