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

UNITED STATES DISTRICT COURT

for the

Central District of California

United States of America

v.

KIERNAN MAJOR,

Defendant

Case No. 2:22-mj-02873-DUTY

CRIMINAL COMPLAINT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

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

On or about the dates of January 20, 2022 in the county of Los Angeles in the Central District of California, the defendant violated:

Code Section	*Offense Description*
18 U.S.C. § 2261A(2)	Stalking

This criminal complaint is based on these facts:

Please see attached affidavit.

☒ Continued on the attached sheet.

/s/ Caitlin Bowdler
Complainant's signature

Caitlin Bowdler, FBI Special Agent
Printed name and title

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

Date: July 25, 2022

Alicia G. Rosenberg
Judge's signature

City and state: Los Angeles, California

Hon. Alicia G. Rosenberg, U.S. Magistrate Judge
Printed name and title

AUSA: Juan M. Rodriguez (x0304)

AFFIDAVIT

I, Caitlin Bowdler, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI"), and have been so employed since March 2017. I am currently assigned to the Los Angeles Field Division Violent Crime Squad which is responsible for investigating kidnappings, extortion, bank robberies, Hobbs Act violations, and other violent crimes. During the time I have been employed by the FBI, I have also worked on a White Collar Crime Squad.

2. Since becoming an FBI Special Agent, I have received formal training at the FBI Training Academy in Quantico, Virginia. This training included segments on conducting criminal investigations, narcotics identification, organized crime, and other law enforcement topics. During the time I have been employed by the FBI, I have participated in investigations relating to extortion, cybercrimes, wire fraud, mortgage fraud, identity theft, mail fraud, and various types of financial institution fraud and violent crimes. I have participated in many aspects of criminal investigations, such as, but not limited to, reviewing evidence, the issuance of subpoenas, the analysis of pen and trap and trace records, consensually monitored telephone calls, conducting physical and electronic surveillance, working with informants, and the execution of search and arrest warrants.

II. PURPOSE OF AFFIDAVIT

3. This affidavit is made in support of a criminal complaint against and arrest warrant against KIERNAN MAJOR ("MAJOR") for stalking Victim # 1[1] and Victim # 2 in violation of 18 U.S.C. § 2261A(2) (Stalking).

4. This affidavit is also made in support of an application for a warrant to search the person of MAJOR as described more fully in Attachment A, for evidence, fruits, or instrumentalities of violations of 18 U.S.C. §§ 2261A(2), (stalking), 875(c) (interstate threats), and 1343 (wire fraud) (the "Subject Offenses"), as described more fully in Attachment B. Attachments A and B are incorporated herein by reference.

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

[1] The two victims and some witnesses are described herein using names such as "Victim # 1" or "Witness # 1" to protect their privacy and safety. Their identities are known to the FBI and government.

III. SUMMARY OF PROBABLE CAUSE

6. The FBI has been investigating MAJOR for stalking and sending threatening communications to two female victims, Victim # 1 and Victim # 2, after Victim # 2 reported the threats to the FBI National Threat Operations Center on June 24, 2022. Specifically, throughout 2021, MAJOR sent voluminous and threatening communications to Victim # 1, who terminated her employment relationship with MAJOR after she reported that he induced her to move to California, but failed to pay her. MAJOR then began dating Victim # 2 in 2022, who connected with Victim # 1, and both began to receive additional threatening communications from accounts associated with MAJOR.

7. Recently, on July 10, 2022, Victim # 1 received a message from an account that she believes belongs to MAJOR telling her, "YOU WILL DIE OVER THIS IF YOU DONT SMARTEN UP" and threatening to kill her father. Victim # 2 also reported that in early July 2022, one of her friends saw an Instagram post on an account associated with MAJOR depicting a hand holding a firearm. Both Victim # 1 and Victim # 2 are afraid of MAJOR and believe their personal safety is at risk.

8. As detailed below, I believe that MAJOR's person will contain evidence, including digital evidence, related to MAJOR's stalking and harassment of, and threats to, multiple victims, including evidence related to the accounts MAJOR used to send various threatening communications.

IV. STATEMENT OF PROBABLE CAUSE

A. MAJOR's Harassment of Victim # 1 & Victim # 2

1. MAJOR Induces Victim # 1 to Move to California under the Guise of Employment, and Threatens Her Once She Terminates the Relationship

9. Based on my review of interviews with Victim # 1, my review of emails and documents containing threats from MAJOR, and from discussions with other law enforcement officers, I know the following:

10. Victim # 1 reported to law enforcement that she initially met MAJOR when they went to the same high school in New York, and she has known of him since middle school. In 2020, Victim # 1 reported that she was searching for employment and had heard from mutual friends that MAJOR had a successful business in Los Angeles. Victim # 1 and MAJOR had mutual friends, but no formal relationship when Victim # 1 reached out to MAJOR about a job opportunity.

11. According to Victim # 1, MAJOR told Victim # 1 that he had a producer friend, J.R., who was looking for a personal assistant and that she could work part-time for the producer and part-time for MAJOR's cyber security company Digital Spartan (later changed to EyesOnly).

a. On July 22, 2022, I reviewed the Colorado Secretary of State Business Database and learned that EyesOnly Enterprises LLC was registered to Kiernan Michael Major as of April 28, 2021. The business was previously registered as Digital Spartan LLC.

12. MAJOR provided Victim # 1 with a formal employment contract, which I have reviewed, in which MAJOR agreed to pay Victim # 1 approximately $92,500 per annum. According to the contract, Victim # 1's job description involved writing emails, running errands, and managing other day-to-day activities for MAJOR. MAJOR also provided her screenshots of article links about his company receiving Department of Defense grants and making over $19 million in profit annually, which I have also reviewed.

13. Victim # 1 reported that she moved to Los Angeles in approximately September 2020 to begin working for MAJOR. Shortly before arriving, MAJOR called to tell her that due to government involvement with his company, her job would be different and there was more that he could not share over the phone, due to security reasons. He also had her fill out a security clearance package. On July 19, 2022, Victim #1 provided the FBI with access to her Apple laptop which included emails and all messages linked to her iPhone, which I have started reviewing. Victim # 1 stated that MAJOR sent her an encrypted email requesting that Victim # 1 complete a security clearance package (Standard Form SF-86). She recalled messaging with him about this on the application Signal, which allows messages to be automatically deleted after one week.

14. Once Victim # 1 arrived in Los Angeles, she reported that she quickly realized she was not doing any of the work that was promised to her. MAJOR convinced her that his identity needed to be protected and thus, he could not use his credit

card, obtain new credit cards, pay for hotels, nor pay for other expenses using his name. Victim # 1 reported that she used her own money, totaling approximately $17,000 over the course of one month, to purchase hotels, meals, Ubers, alcohol, and cannabis for MAJOR. I have reviewed Victim # 1's bank statements, which confirm large expenses during this time period.

15. Victim # 1 also reported that she maxed out her credit card, drained her savings account, and never received a single paycheck from MAJOR. Occasionally he would send her some money through CashApp, but would usually just ask her to use that money to cover MAJOR's ongoing expenses.[2] After one month, she realized that MAJOR did not have a legitimate business. She learned from two of MAJOR's roommates that he had taken money from them as investments for his company and that they also believed he had defrauded them.

16. Victim # 1 reported that she cut off all communication with MAJOR in October 2020. According to Victim # 1, MAJOR "freaked out" and mass texted and called her. Victim # 1 reported that she would receive 700-1000 phone calls a day and he would also reach out to her by email and Instagram. Ultimately, Victim # 1 reported that she blocked MAJOR's email and Instagram accounts.

17. Victim # 1 identified MAJOR's Instagram handles as Kiernan.major, kiernanmajor00, eyesonly.usa, eyesonly.intel, eyesonly.cyber, and eyesonly.labs, and I have reviewed Victim #

[2] I have requested, but not yet received records from CashApp. I have reviewed Chase bank statements that show the CashApp transactions linked to Victim #1's bank account.

1's Instagram account and have seen the messages that she received from the Kiernan.major account.

18. In January 2021, Victim # 1 went to the Auburn Police Department from her and MAJOR's hometown in New York to report all of the threatening phone messages and emails. According to Victim # 1 and Cayuga County DA Joseph DiVietro, she was told that the police could not assist her because the conduct took place in California.

19. For the next year, Victim # 1 reported that MAJOR continued to send Victim # 1 serious threatening messages and emails about killing her and her family members using different accounts that Victim # 1 hadn't blocked. Additionally, even though Victim # 1 reported that she never had a romantic relationship with MAJOR, MAJOR would send messages to her father, which I have reviewed, talking about how "he already fucked his daughter," and implying they had an intimate relationship, which was all fabricated. MAJOR also wrote to the father, "Stop hurting me or someone will get hurt. Realize that. I could legally follow you and your lying daughter wherever –if I can't my company can."

20. The FBI has interviewed Victim # 1's father, who confirmed MAJOR started sending text messages to him, in addition to one email from Kiernan@spartan.consulting. MAJOR told the father on June 3, 2022, that he wanted to provide Maggie with a check for $100k to make things right and have her call him. On July 6, 2022, MAJOR messaged the father, "Get your daughter to call me and we are done. Don't and we will have your

life upside down in a week or less. Bet against me lol. I already fucked your daughter enough boy I'll fuck you too."

21. In 2021, according to Victim # 1, MAJOR brought up the topic of reimbursing her. Victim # 1's father worked at the same hospital in Auburn as MAJOR's mother, M.M. MAJOR told Victim # 1 that his mother would pay her father the reimbursement. According to reports and records from the criminal case, which I have reviewed, M.M. wrote Victim # 1 a check for $25,000, however the check bounced, and she was arrested on April 25, 2021, for writing the bad check. As a result, M.M. was required to pay Victim # 1 $100 per month for the course of five years.

22. Victim # 1 reported that over the span of two years, MAJOR sent approximately 64 emails to Victim # 1 from the following email addresses: masonscott@cia.ic.gov, masonscott22@protonmail.ch, majorkm@pm.me, kiernanmaj@protonmail.ch, kiernan@spartan.consulting, kiernan@eyesonlyusa.com. Victim # 1 reported that MAJOR has previously used the alias Mason Scott.

23. I have reviewed the emails sent to Victim # 1 as reflected on her email account, and they contained, among other things, the following:

a. On April 21, 2021, MAJOR sent approximately 36 emails from majorkm@pm.me telling Victim # 1 that it was an emergency and he needed to talk with her about two very important questions. He even brought up reimbursing her and that he only wanted the best for her. Victim # 1 has responded

to similar emails, referring to the sender as Kiernan, and the sender has replied instructing her to contact him. Based on this and other information contained within the emails, Victim #1 believes it is MAJOR.

b. On April 24, 2021, between 9:46 p.m. and 10:01 p.m., Victim # 1 received approximately ten emails from masonscott22@protonmail.ch.[3] One of the emails sent at 9:49 p.m. was titled, "Show dad and his friends", and included the following message:

> *I will kill you and mutilate your siblings for years. It's only a matter of time the way you are acting. Please report me ASAP it will help you at least a little.*

c. Between 9:51 p.m. and 9:53 p.m., Victim # 1 received two emails from the same address titled, "Re: Show dad and his friends", and included the following message:

> *I will kill your family one by one. And then i will have a field day embarrassing your whore parents next week. Lol this is what you get for blocking me. Cunt.*
>
> *Wait till i target john and charlie hahaha.. bye.*

i. In my interviews with Victim # 1, I know that John and Charlie are references to her brothers.

[3] Victim # 1 told the FBI that she believed this email address was associated with MAJOR because MAJOR told her that Mason Scott was one of his alias' due to his top secret work with the government and the need to protect his identity.

d. At 9:55 p.m., Victim # 1 received an email with the subject line "you may not be scared," and including the following message:

but if youob dont think i would torture your fam for fun hahahahahahaha youre not even thinking right. You better relax whore.

e. At 9:58 p.m., Victim # 1 received an email with the subject line, "youre gonna die," and included the following message:

im killing you and whoever lives at all the addresses i know you reside at

f. At 9:59 p.m., Victim # 1 received an email with the subject line, "youre gonna die," and included the following message:

Btw if youre not there no worries someone will be alive and ready to die

g. At 10:00 p.m., Victim # 1 received an email with the subject and body titled, "unblock me or die by 4pm tomorrow."

h. On May 12, 2021, at approximately 6:31 a.m., Victim # 1 received an email from majorkm@pm.me entitled, "Warning", and included the following message:

[Victim #1],

I cannot sustain the suffrage that comes with our dispute at the present moment. It genuinely drives me insane to re-experience the past everyday with counsel, especially in such detail. For these reasons

I am temporarily choosing to focus on and invest in my own well-being for a change. This message serves only as a purpose to forewarn you of what is patiently awaiting each and every living specimen of your past, current and future and to update you on the status of your court summons'. The nastiest truth's about all of you will be relentlessly exposed and I will conduct this in such as public manner that it will continue to haunt you guys in every corner of this planet until I finally succeed in your guys' total extinction. You and your father are absolutely terrible people and do not ***ever*** *attempt to convince yourselves otherwise. This doesn't even scratch the surface of how I feel about you or the 'discomfort' you're all about to experience for the rest of your lives. Good luck to you all :) I almost hope you underestimate me. Count your fucking blessings, -Kiernan*

Based on the name in the signature block the similarity to other email communications and messages, Victim # 1 believed that this message was sent by MAJOR.

i. On or about May 14, 2021, Victim # 1 received a series of messages from johnmorgan@secmail.pro:[4]

We have just made our first round of calls to your employers. I wish you a horrible weekend. Please

[4] Based on the previous pattern of messages and the similarity of this message, Victim # 1 believed that MAJOR used this email address.

commit suicide sooner rather than later. See ya in court ya slut

You will have to lock me up for life to stop me from going after you, your family and your friends. I am insanely creative and have been prepping this for over a year. Don't ruin your life. I beg you because when you apologize I'll end up feeling really bad. This will destroy your family without question. My last warning. I just feel it's moral to warn you. Sorry to harass.

You will always be an entitled little gold digging cunt. You're nothing but a waitress turned glorified nanny. Get over yourself and your fabricated reality. Remember that you have gotten no where in life on your own, neither has anyone in your family. You will never earn shit in your life unless throwing your pussy at rich men counts. I will expose you and our megalomaniac father. Your time is running thin slut and I will not relent. You can think you are making progress but you could own the state of NY and it wouldn't prevent what's to come. Good luck. You'll really need it. Sad you think I'm all talk. Bye.

2. MAJOR Harasses Victim # 2 after She Terminates a Romantic Relationship with Him

24. Based on my review of interviews with Victim # 2 and memoranda describing interviews with Victim # 2, my review of emails, messages, and documents containing threats from MAJOR,

and from discussions with other law enforcement officers, I know the following:

25. Victim # 2 reported that she met MAJOR at the Four Seasons Hotel in San Francisco on January 6, 2022. Victim # 2 and MAJOR ultimately become friends and then romantic partners. Early in their relationship, MAJOR become very paranoid and would tell Victim # 2 that he worked for various "agencies" and was involved in counter-espionage projects involving China and Russia. MAJOR would only use cash to pay for his expenses and after several dates he began to ask Victim # 2 to cover his expenses. He claimed that she would be reimbursed generously for doing something good for national security.

26. Victim # 2 initially paid for meals, but it quickly escalated to her covering hotel costs, airplane tickets, and other expenses. MAJOR would pay Victim # 2 back through a friend named "Trent Valentino," via a Paypal account with email address trentval03@protonmail.com, however that quickly stopped and the majority of that money went to funding MAJOR's lifestyle.

27. According to Victim # 2, MAJOR continued to tell Victim # 2 that he was a CIA operative working with the DOD, NSA, and the FBI. He would bring Victim # 2 to meetings, even though no one would show up, and would prepare her to introduce herself as either a colleague, assistant, or client relations manager for MAJOR's company, EyesOnly. Victim # 2 continued to cover all of MAJOR's expenses and when she ran out of money, MAJOR would encourage her to ask her parents for money.

28. Based on my review of bank statements provided by Victim #2, Victim # 2's accounts were over-drawn and MAJOR convinced her to open two new checking accounts and two new credit cards, to overdraft Paypal, to write checks, and to withdraw money from her savings accounts, all to fund MAJOR's lifestyle in the name of national security. Victim # 2 believed that MAJOR still had the AMEX credit card that was opened in Victim # 2's name. This caused significant stress to Victim # 2, but she reported that she continued to listen to MAJOR because he would constantly threaten her and tell her that she would get nothing back if she didn't follow through and those certain "agencies" would target her as a consequence.

29. Victim # 2 reported that she felt afraid and was worried that she would let everyone down if she didn't continue to do what MAJOR told her to do. MAJOR would make promises to repay Victim # 2, making her feel better momentarily, and then he would berate her, threaten her with his "friends in the Government," and would even threaten to kill himself if she didn't comply. MAJOR also took nude and sexual photos and videos of Victim # 2 without her knowledge or consent and, after he showed them to her, would not delete them when she asked him to. He also posted these images and short videos of her on Instagram, where her face was not shown, but she recognized herself.

30. According to Victim # 2, MAJOR would string Victim # 2 along by attempting to pay her back with alleged wire transfers that were never processed. He would offer to cover Victim # 2's

rent, but never did. He even stated that he had attorneys involved to help pay her back but wouldn't let Victim # 2 speak to them due to "privacy concerns." Victim # 2 calculated the approximate total of funds she provided to MAJOR that was not reimbursed was $111,000.

3. Victim # 1 and Victim # 2 Connect

31. Towards the end of Victim # 2's relationship with MAJOR in approximately June 2022, MAJOR encouraged Victim # 2 to reach out to a woman who MAJOR identified as his "ex-girlfriend" and whom he claimed was the love of his life and that he could not get over. MAJOR had claimed that he wanted to make things right with this ex-girlfriend and asked that Victim # 2 reach out and set up a meeting between MAJOR and this ex-girlfriend. Victim # 2 agreed, and based on contact information provided by MAJOR, successfully connected with Victim # 1, the alleged ex-girlfriend.

32. According to Instagram messages that I have reviewed, Victim # 2 reached out to Victim # 1 on Instagram on or about June 22, 2022, telling her that MAJOR wanted closure with her and asked if she would reach out to MAJOR. Victim # 1 told her that she would not reach out to MAJOR but was happy to talk with her. In their discussions, Victim # 1 told Victim # 2 about her situation with MAJOR, including the fraud, lack of reimbursement for all the expenses, and the threats.

33. Victim # 2 reported that after Victim # 1 explained her experiences with MAJOR, Victim # 2 quickly realized that she was being victimized by MAJOR and needed to get away from him

4. MAJOR Begins to Stalk and Harass Victim # 2 after She Connected with Victim # 1

34. At the time that Victim # 2 connected with Victim # 1 over Instagram, Victim # 2 reported that she had been staying with MAJOR at the Peninsula Hotel in Beverly Hills, CA from June 8, 2022, to June 18, 2022. According to Victim # 2, she left Beverly Hills, CA on June 18, 2022, but continued to be charged for her hotel room until her father called the Peninsula Hotel and cancelled the room on June 23, 2022. According to Victim # 2 and her father, MAJOR had been occupying the room and was forcibly removed from the hotel.

35. According to Victim # 2, around this time MAJOR began to blame Victim # 2 for putting him on the streets and began to increase his abusive, harassing, and threatening messages and phone calls to Victim # 2. MAJOR became aware that Victims # 1 and # 2 were sharing their experiences regarding MAJOR with each other and MAJOR escalated his threats to both victims.

36. On June 27, 2022, Victim # 2 received the following text messages from MAJOR,[5] which I reviewed:

You've drank too much of [Victim # 1's] Kool-Aide.

For that expect to suffer life-long consequences along side her until you guys get over yourselves and take your fathers cock out of your mouths.

And its sad you're naïve enough to believe her.

[Victim # 1] IS A LIAR!

[5] The messages came from the same number that Victim # 2 reported she always used to communicate with MAJOR.

I will fucking find you fuckers and I will fucking hold you accountable by whatever means necessary.

MEET WITH ME AND BE EVEN

Or fucking DIE

And I mean DIE

You will both regret this

Just speak to me on the phone or meet in person and it's over. Until then you're 1 year away from a bullet in your head. Metaphorically… that is…

But I'm gonna fucking make you guys pay for this

37. I reviewed subscriber information from T-Mobile for the phone number associated with MAJOR, (628) 358-7004 ("7004 number"), and learned that the phone is registered to Kiernan M. Major.

38. On July 1, 2022, according to my review of screenshots from her cell phone, Victim # 2 received approximately 40 phone calls in the span of 10 minutes via a No Caller ID number. She believed these phone calls were from MAJOR. That same day, Victim # 2 received a series of threatening messages sent via iMessage from MAJOR. Below is a portion of the series of messages sent:

I INTEND TO KILL YOUR WHOLE FAMILY

HOW DARE YOI

IM COMING TO KILL THE FIRST FUCKING PERSON I SEE

YOU MOTHERFUCKING BITCH

I WILL FIND YOU

AND I WILL FUCKING SLAUGHTER YOU

39. Between approximately July 3, 2022, and July 4, 2022, Victim # 2 was informed by a friend who had been following one of MAJOR's Instagram accounts with the handle "Kiernan.major[6]" that MAJOR had posted two photos of a handgun on his Instagram "story." One of the photos was of someone's hand holding a Glock handgun box and the second was of a Glock handgun on a kitchen counter with an ejected magazine next to it, that appeared to be loaded with real pistol rounds. The images are below.

[6] "Kiernan.Major" is a private Instagram account, but has a profile photo that depicts a male that appears to be MAJOR, based on my review of his New York State Driver's License. Additionally, the profile has a link to the Instagram account for EyesOnly, MAJOR's cyber security company registered in Colorado. Additionally, Victim #1 received direct messages from this Kiernan.Major account.

40. Victim # 2 said that she has been in fear for her life ever since she left MAJOR in Los Angeles. She had to move back in with her parents, who have increased security measures to protect Victim # 2. Victim # 2 has been scared to leave her parent's house and rarely does because she knows that MAJOR has her parent's address.

5. MAJOR's renewed Stalking & Harassment of Victim # 1

41. On July 1, 2022, Victim # 1 received iMessages to her email address from MAJOR's 7004 number, which was the same number from which Victim # 2 received the threatening communications described above that is registered to MAJOR.[7] Some of the messages are highlighted below:

I would stay inside this Independence Day.

I could kill your father in about 30 minutes so relax.

Hide ur family because you motherfuckers have destroyed me for nothing. And I DONT owe that retard money.

I hope you're dumb enough to ignore this because I'm 200% killing you or someone you know

IM GONNA KILL ALL OF YOU FUCKING BITCHES

PLEASE DONT THINK I WONT

AND I IDK WHAT THE FUCK SHE TOLD YOU BUT IM FOR SURE GONNA KILL HER

When I kill your father what would you like me to use?

[7] Victim # 1 also had no prior communications with this number, but similarly believed it to be from MAJOR because of her prior experiences receiving threatening messages from him.

Should I text first?

Hammer?

Knife?

1000 rounds?

In front of family?

Or drag his dead ass in the street

42. On July 1, 2022, Victim # 1 continued to receive iMessages from MAJOR's 7004 number, in which I believe MAJOR is referring to asking Victim # 2 to set up a meeting with him and Victim # 1. The messages are as follows:

She was supposed to set up a meeting and this is what comes of it

Love it

I hope you realize how serious I am

Because I will kill your family and a sibling at a minimum

I mean that from the bottom of my heart

How fucking dare you do this shit to me

I JUST WANTED CLOSURE AND YOURE SO FULL OF YOURSELF YOU WOULDNT GIVE IT

SO I WILL WITHOUT A DOUBT SHOW TOU HOW FAST I CAN FIND AND KILL SOMEONE YOU KNOW

I know where [Victim # 2] lives

Hahahahha

When I stare at you before your death we will see if that's true.

But I PROMISE I will kill someone

I'm not fucking kidding

And that's all on you

Could've just been nice to me

But you tell everyone lies

43. On July 6, 2022, Victim # 1 received iMessages to her email address from MAJOR's 7004 number. Some of the messages are highlighted below:

And you're whole family about to get murdered tonight for it

I will fucking fix this now or I will do something to someone

I will go to jail to accomplish this

If I need to find ANYONE you know and kill them I will

BUT DONT THINK I WONT HIT YOUR SISTER FIRST TJAT WHOE

I COULD SHOOT THAT BUTCH ANY DAY

Figure it out because I have set out to learn your father and sisters' patter of life.

44. On July 10, 2022, between 2:56 a.m. and 5:02 a.m., Victim # 1 received a series of approximately 11 emails from kiernan@eyesonlyusa.com. One of the emails sent at 3:10 a.m. included the title, "YOU WILL DIE OVER THIS IF YOU DONT SMARTEN UP," but did not include a message in the main body of the email. Another one of the emails sent at 3:12 a.m. included the title, "I WILL MAKE SURE YOUR FATHER DIES A BRUTAL DEATH." The email also didn't include a message in the main body of the email.

45. On July 10, 2022, Victim # 1 received an email to her email address from kiernan@eyesonlyusa.com with the subject line

"I 100% WILL SCALP YOUR FATHER ALIVE," and the following message:

> *[VICTIM # 1's FIRST NAME],*
>
> *Please realize I am not trying to sound scary. I'm just mad I can't get my hands on you sooner for the sake of the success of it anyway. When I do though, boy, are you guys gonna suffer all the way to hell. Have fun working 36 jobs the rest of your life so you can pretend you're happy with your basic fucking boring ass life. Fuck you slut.*
>
> *Best,*
>
> *Kiernan*

46. Victim # 1 said that the emails and iMessages that she had received over the course of nearly two years made her feel extremely scared, frightened, angry, annoyed, and fearful for her life and the lives of her family members. She began to feel numb, but the idea that MAJOR may have acquired a handgun made Victim # 1 extremely concerned with her safety and the safety of her family causing additional emotional distress. She believes MAJOR is capable of causing her harm or death. Additionally, she has filed and was granted a restraining order against MAJOR.

47. FBI Special Agent Robert McElroy submitted an Emergency Disclosure Request to T-Mobile for GPS location pings for MAJOR's 7004 phone number on June 27, 2022. T-Mobile provided pings for this phone for 48 hours. MAJOR was in the Beverly Hills area between June 27, 2022, and June 29, 2022. Special Agent McElroy submitted another Emergency Disclosure

Request to T-Mobile for GPS location pings for MAJOR's 7004 phone number on July 1, 2022, as the threats to each victim continued. T-Mobile again provided pings for this phone for 48 hours. MAJOR was in the Beverly Hills and Silverlake area of Los Angeles between July 1, 2022 and July 3, 2022.

48. Beverly Hills Police Department was assisting the FBI with the investigation and obtained a search warrant for T-Mobile, which was signed by Magistrate Stacey Wise on July 13, 2022. T-Mobile provided subscriber information and GPS location pings for this phone. The phone is believed to be an iPhone. I have learned that MAJOR's phone has been pinging off a cell phone tower in Ames, Iowa since July 15, 2022.

49. Based on my training and experience investigating stalking and threat-to-life cases, I know that individuals engaged in such conduct commonly use fake or anonymized accounts, false identifications or identities, or stolen identifications, in order to avoid detection and to hide their true identities. These individuals often also keep evidence related to these accounts and identifiers in secure, easily-accessible places, like their homes, cars, and on their person.

50. Based on the foregoing, as well as my training, experience, and knowledge of this investigation, I also believe that electronic devices, including computers, laptops, tablets, and cellular telephones capable of making telephone calls and accessing the internet and that were likely used by MAJOR during the activities described herein will be found on MAJOR's person. Based on MAJOR's use of international email servers and accounts

to harass and threaten victims, I also believe digital and physical evidence related to the stalking, harassment, and the threatening communications (including evidence related to identity) will be found on MAJOR's person.

V. TRAINING AND EXPERIENCE ON DIGITAL DEVICES[8]

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

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

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

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

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

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

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

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

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

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

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or

eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

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

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

VI. CONCLUSION

55. For all the reasons described above, there is probable cause to believe that MAJOR has committed a violation of 18 U.S.C. § 2261A(2) (Stalking). Further, there is also probable cause that the items to be seized described in Attachment B will be found in a search of MAJOR's person as further described in Attachment A.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 25th day of July, 2022.

Alicia G. Rosenberg

HONORABLE ALICIA G. ROSENBERG
UNITED STATES MAGISTRATE JUDGE