AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR SEARCH WARRANTS

I, Special Agent Keith A. Leavitt Jr., being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been employed since October, 2024. I am currently assigned to the FBI Boston Joint Terrorism Task Force (JTTF). During my time assigned to the FBI Boston Division, I have investigated and participated in the investigations of nihilistic violent extremism, violent crimes against children, anti-government extremism, and domestic terrorism. During the course of these investigations, I have conducted analysis of digital records, social media, cloud communications, physical and electronic surveillance, assisted in the execution of arrest and search warrants, debriefed informants, and reviewed pertinent records and evidence. Based on my training and experience, I am familiar with the means through which individuals use computers and information networks to conduct criminal activity, including threatening communications made on social media platforms.

2. I am currently investigating Alden RUML ("RUML") for transmitting a threat in interstate commerce, in violation of 18 U.S.C. § 875(c).

3. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple Inc. to disclose to the government records and other information, including the contents of communications, associated with the Apple ID alden.ruml@icloud.com (the "Target Apple Account"), as described in Attachment A-1, that is stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Infinite Loop, Cupertino, CA, because there is cause to believe

that the information described in Attachment A-1 contains evidence or instrumentalities of violations of 18 U.S.C. § 875(c) as described in Attachment B-1.

4. I also make this affidavit in support of an application for warrants to search:

a. The residence of RUML at 29 Concord Avenue, Apt. 606, Cambridge, MA 02138 (the "Target Residential Address"), as described in Attachment A-2, because there is probable cause to believe that it contains evidence and instrumentalities of violations of 18 U.S.C. § 875(c) as described in Attachment B-2; and

b. the person of RUML as described in Attachment A-3, because there is probable cause to believe that it contains evidence and instrumentalities—in particular, electronic devices—of violations of 18 U.S.C. § 875(c), as described in Attachment B-3.

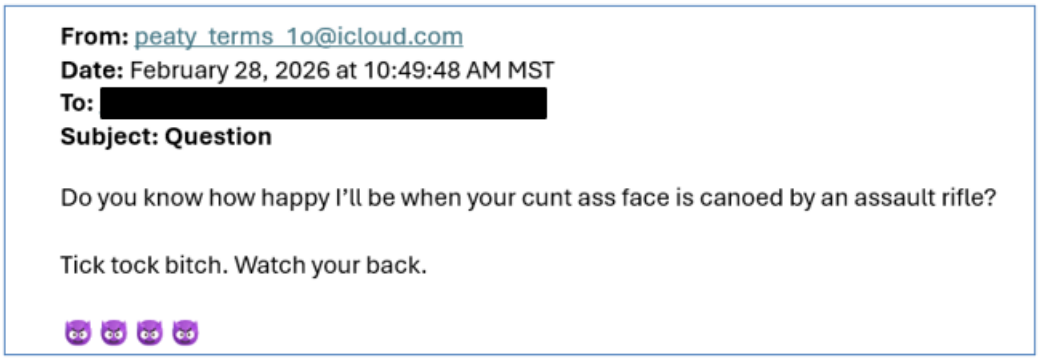
5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show simply that there is sufficient probable cause for the requested warrants and does not set forth all my knowledge about this matter.

PROBABLE CAUSE TO BELIEVE THAT A FEDERAL CRIME WAS COMMITTED

6. Alexis Wilkins ("Person 1") is the girlfriend of Kash Patel ("Federal Official"), the Director of the Federal Bureau of Investigation ("FBI").

7. The relationship between Person 1 and Federal Official has been the subject of extensive media attention and news reporting. On February 28, 2026, a news article was published describing the use of FBI resources to provide security to Person 1. The article also described Person 1 and the Federal Official's conservative political views and their association with the Make America Great Again ("MAGA") political movement.

8. On or about February 28, 2026, Person 1 received an email[1] from the email address peaty_terms_1o@icloud.com. The subject line of the was "Question." The email stated: "Do you know how happy I'll be when your cunt ass face is canoed by an assault rifle?[2] Tick tock bitch. Watch your back. 😈😈😈😈" A copy of the email is reproduced below:


From: peaty_terms_1o@icloud.com
Date: February 28, 2026 at 10:49:48 AM MST
To: [redacted]
Subject: Question

Do you know how happy I'll be when your cunt ass face is canoed by an assault rifle?

Tick tock bitch. Watch your back.

😈😈😈😈

9. Person 1 forwarded the email to law enforcement on February 28, 2026.

10. In response to a law enforcement request, Apple provided records indicating that peaty_terms_1o@icloud.com is an anonymized email account associated with the Target Apple Account.[3]

---

[1] The threatening email was sent to an email address that was publicly available on Person 1's website.

[2] In this context, I understand "canoed" to refer to causing a v-shaped or canoe-shaped wound in the skull.

[3] Apple provides a "Hide My Email" function to iCloud+ subscribers. The Hide My Email function generates random anonymized email addresses that can be used to send or receive emails from the subscriber's email account.

11. Apple provided the following subscriber information for the Target Apple Account:

Subscriber Name: Alden Ruml
Email address: alden.ruml@icloud.com

12. Records provided by Apple also indicate (i) that the Target Apple Account was used to generate 134 anonymized email accounts; and (ii) that multiple Apple electronic devices have been registered to the Target Apple Account, including an iPad Mini, an iPhone 17 Pro, and an Apple Watch Ultra 3.

13. Law enforcement agents interviewed Person 1 on March 2, 2026. Person 1 indicated that they received the threatening email while in Arizona. Person 1 indicated being frightened by the threatening email and changing their upcoming travel arrangements as a result.

14. Law enforcement agents interviewed RUML on March 2, 2026 at his place of employment in Cambridge, MA. During that interview RUML was shown a copy of the threatening email and confirmed that he had sent the email to Person 1. RUML stated that he had read the February 28, 2026 news article described above and became upset, leading him to send the threatening email. RUML denied any intent of harming anyone through violence or harmful words.

15. According to a report of the interview with RUML, RUML identified his residential address as: **28 Concord** Avenue, Apartment 606, Cambridge, MA 02138.[4] When law

[4] Records obtained from Apple and open-source records identify Ruml's address as 38 Dana St, Cambridge, MA 02138-4204. During his interview with law enforcement agents, RUML indicated that he no longer lives at that address.

enforcement officers attempted to locate this address, they found that this was likely an incorrect address as no building with that address existed.

16. On March 10, 2026, I visited **29 Concord Avenue**, Cambridge, MA 02138 (the Target Residential Address). I entered the public access lobby of the building and observed a mailbox with the name "RUML" and the number 606. An image of the mailbox is below:

17. On March 11, 2026, law enforcement officers conducted a ruse to confirm RUML's residence. A law enforcement officer attempted to make a food delivery to 29 Concord Avenue, Apartment 606, Cambridge, MA 02138. RUML answered the door and there was no indication of other residents in the apartment.

18. On March 2, 2026, a preservation request for the Target Apple Account was submitted to Apple.

19. A grand jury returned an indictment on March 12, 2026, charging RUML with transmitting a threat in interstate commerce in violation of 18 U.S.C. § 875(c).

TECHNICAL BACKGROUND CONCERNING APPLE[5]

20. Apple is a United States company that produces the iPhone and iPad, which use the iOS operating system, and desktop and laptop computers, which use the Mac OS operating system.

21. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to manage iOS device backups and data associated with third-party apps. If a user signs up for iCloud, iCloud automatically backs up information on the user's mobile devices, such as an

---

[5] The information in this section is based on information published by Apple on its website.

iPhone or iPad, daily over wifi (when the device is turned on, connected to a power supply, and locked), unless the user manually changes the settings to prevent automatic backups. The backup includes, among other things, purchase history from the iTunes store and App Store, photos and videos, device settings, app data, iMessage, text messages, visual voicemail password, and device settings. The backup includes data that is not already otherwise stored in iCloud. Generally, iCloud Photo already stores photographs and videos in iCloud, so these items thus would not be included in the backup.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs enables iCloud to be used to synchronize webpages opened in the Safari web browsers on all of the user's Apple devices. iWorks Apps, a suite of productivity apps (Pages, Numbers, and Keynote), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices.

f. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

g. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS.

22. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

23. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user.

24. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. In addition, Apple captures the date on which the

account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

25. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

26. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains

records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

27. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWorks and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, text messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

28. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

29. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

30. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

31. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

32. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and

experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

LEGAL AUTHORITY FOR THE APPLE SEARCH WARRANT

33. The government may obtain both electronic communications and subscriber information from a provider of electronic communication services and remote computing services by obtaining a search warrant. 18 U.S.C. §§ 2703(a), 2703(c)(1)(A).

34. Any court with jurisdiction over the offense under investigation may issue a search warrant under 18 U.S.C. § 2703(a), regardless of the location of the provider whose information will be searched. 18 U.S.C. § 2703(b)(1)(A). Furthermore, unlike other search warrants, § 2703 warrants do not require an officer to be present for service or execution of the search warrant. 18 U.S.C. § 2703(g). If the government obtains a search warrant, there is no requirement that either the government or the provider give notice to the subscriber. 18 U.S.C. §§ 2703(b)(1)(A), 2703(c)(3).

FOURTEEN-DAY RULE FOR EXECUTION OF APPLE iCLOUD WARRANT

35. Federal Rules of Criminal Procedure 41(e)(2)(A) and (B) direct the United States to execute a search warrant for electronic evidence within fourteen (14) days of the warrant's issuance. If the Court issues the requested warrant for the Target Apple Account, the United States will execute the warrant not by entering the premises of Apple, as with a conventional warrant, but rather by serving a copy of the warrant on the respective companies and awaiting their production of the requested data. This practice is approved in 18 U.S.C. § 2703(g),[6] and it

[6] Section 2703(g) provides that "[n]otwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with

is generally a prudent one because it minimizes the government's intrusion onto internet companies' physical premises and the resulting disruption of their business practices.

36. Based on the training and experience of myself and other law enforcement agents, I understand that electronic account providers sometimes produce data in response to a search warrant outside the 14-day (formerly 10-day) period set forth in Rule 41 for execution of a warrant. I also understand that electronic account providers sometimes produce data that was created or received after this 14-day deadline ("late-created data").

37. The United States does not ask for this extra data or participate in its production.

38. Should Apple produce late-created data in response to the Apple iCloud warrant, I request permission to view all late-created data that was created by Apple, including subscriber, IP address, logging, and other transactional data, without a further order of the Court. This information could also be obtained by grand jury subpoena or an order under 18 U.S.C. § 2703(d), neither of which contains a 14-day time limit. However, law enforcement personnel will seek to avoid reviewing any late-created data that was created by or received by the account-holder(s), such as messages, absent a follow-up warrant.

39. For these reasons, I request that the Court approve the procedures in Attachment B-1, which set forth these limitations.

---

this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service."

PROBABLE CAUSE TO BELIEVE THAT THE PREMISES AND PERSON TO BE SEARCHED CONTAINS EVIDENCE AND INSTRUMENTALITIES OF A FEDERAL CRIME

40. I have probable cause to believe that the premises and person to be searched, as described in Attachments A-2 and A-3 contain evidence and instrumentalities of violations of 18 U.S.C. § 875(c), as described in Attachments B-2 and B-3.

41. As described above, there is probable cause to believe that RUML transmitted a threat in interstate commerce, in violation of 18 U.S.C. § 875(c) by sending a threatening email to Person 1. There is also probable cause to believe that RUML owns multiple devices, including an iPhone 17 Pro, iPad, and Apple Watch that are associated with his Apple iCloud Account.

42. Based on the data provided by Apple, the iPhone and Apple Watch were both purchased in September 2025 and registered to the Target Apple Account on September 19, 2025.

43. Based on my training and experience, I am aware that mobile phones, smartwatches, and other devices can be used to send emails and other messages. I am also aware that mobile phone users typically keep their mobile phones on their persons or, while at home, elsewhere in their residences.

44. Based on my training and experience, it is likely that records related to a violation of 18 U.S.C. § 875(c) are stored locally on an electronic device. Additionally, I am aware that users of email frequently access email accounts on a smartphone, a smartwatch, and on other electronic devices.

45. From my training, experience, and information provided to me by other agents, I am aware that individuals frequently use computers to create and store records of their actions by

communicating about them through e-mail; arranging for travel; and researching topics of interest.

46. Based on my training, experience, and information provided by other law enforcement officers, I know that many cell phones (which are included in Attachment B-2 and B-3's definition of "hardware") can now function essentially as small computers. An Apple iPhone 17 Pro is such a type of phone. Phones have capabilities that include serving as a wireless telephone to make audio calls, digital camera, portable media player, GPS navigation device, sending and receiving text messages and emails, and storing a range and amount of electronic data. Examining data stored on devices of this type can uncover, among other things, evidence of communications and evidence that reveals or suggests who possessed or used the device.

47. Based on my knowledge, training, experience, and information provided to me by other agents, I know that computer files or remnants of such files can be recovered months or years after they have been written, downloaded, saved, deleted, or viewed locally or over the Internet. This is true because:

a. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their computers, they can easily transfer the data from their old computer to their new computer.

b. Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, a computer's operating

system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how the computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is typically required for that task.

d. Similarly, files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

e. Data on a storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage

media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

f. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the

chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

g. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

h. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an

accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

i. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

48. Based on my knowledge and training and the experience of other agents with whom I have spoken, I am aware that in order to completely and accurately retrieve data maintained in computer hardware, computer software or storage media, to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, and storage media ("computer equipment") be seized and subsequently processed by a computer specialist in a laboratory setting rather than in the location where it is seized. This is true because of:

a. The volume of evidence — storage media such as hard disks, flash drives, CDs, and DVDs can store the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by

storing it in random order or with deceptive file names. Searching authorities may need to examine all the stored data to determine which particular files are evidence, fruits, or instrumentalities of criminal activity. This process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis on-site.

b. Technical requirements — analyzing computer hardware, computer software or storage media for criminal evidence is a highly technical process requiring expertise and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert possesses sufficient specialized skill to best analyze the system and its data. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence and to recover even "hidden," deleted, compressed, or encrypted files. Many commercial computer software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a "booby trap."

Consequently, law enforcement agents may either copy the data at the premises to be searched or seize the computer equipment for subsequent processing elsewhere.

49. The premises may contain computer equipment whose use in the crime or storage of the things described in this warrant is impractical to determine at the scene. Computer equipment and data can be disguised, mislabeled, or used without the owner's knowledge. In

addition, technical, time, safety, or other constraints can prevent definitive determination of their ownership at the premises during the execution of this warrant. If the things described in Attachments B-2 or B-3 are of the type that might be found on any of the computer equipment, this application seeks permission to search and seize it onsite or off-site in order to determine their true use or contents, regardless of how the contents or ownership appear or are described by people at the scene of the search.

50. The law enforcement agents will endeavor to search and seize only the computer equipment which, upon reasonable inspection and/or investigation conducted during the execution of the search, reasonably appear to contain the evidence in Attachments B-2 or B-3. If however, the law enforcement agents cannot make a determination as to use or ownership regarding any particular device, the law enforcement agents will seize and search that device pursuant to the probable cause established herein.

51. This warrant authorizes a review of electronically stored information, communications, other records and information seized, copied or 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 seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNLOCKING A DEVICE USING BIOMETRIC FEATURES

52. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices,

particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

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

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

55. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to

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

56. As discussed in this affidavit, I have reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the devices subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the devices, making the use of biometric features necessary to the execution of the search authorized by this warrant.

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

58. I further request that the Court authorize law enforcement to change device settings on any seized devices to disable "Stolen Device Protection," which is a security measure that can be used to prevent unauthorized access to the device and data. When enabled, however, this feature might prevent forensic tools from being able to extract data from devices

REQUEST TO SEAL AND PRECLUDE NOTICE TO THE SUBSCRIBER(S)

59. I request that this application, the warrants, the order, and any related papers be sealed by the Court until such time as the Court pursuant to Local Rule 7.2 directs otherwise. I further request that, pursuant to the preclusion-of-notice provisions of 18 U.S.C. § 2705(b), the Court order Apple Inc. ("Apple") not to notify any person (including the subscriber to whom the materials relate) of the existence of this application or the Court's Order for the earlier of one year from the date of the Court's Order or upon notice by the government within 30 days of the conclusion of its investigation, unless the Court extends such period under 18 U.S.C. § 2705(b). Non-disclosure is appropriate in this case because the Court's Order relates to an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation, and its disclosure may alert the targets to the existence of the investigation. There is accordingly reason to believe that notification of the existence of the Order will seriously jeopardize the investigation including by giving targets the opportunity to destroy or tamper with evidence or change patterns of behavior. *See* 18 U.S.C. § 2705(b). Moreover, some of the evidence in this investigation is stored electronically. If alerted to the existence of the Order, the targets could destroy that evidence, including information saved to their personal computers, on other electronic media, or in social media accounts.

//

//

CONCLUSION

60. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe (i) that evidence and instrumentalities of violations of 18 U.S.C. § 875(c), as described in Attachment B-1, exist on the computer systems in the control of Apple, as described in Attachment A-1; and (ii) that evidence or instrumentalities of violations of 18 U.S.C. 875(c), as described in Attachments B-2 and B-3, are contained within the premises described in Attachment A-2 or on the person of RUML as described in Attachment A-3.

Sworn to under pains and penalties of perjury,

Keith A. Leavitt Jr. by JCB

Keith A. Leavitt Jr.
Special Agent, Federal Bureau of Investigation

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

Honorable Jennifer C. Boal
United States Magistrate Judge

On March 12, 2026