Exhibit A

DOCUMENT REDACTED PURSUANT TO PENDING MOTION TO SEAL

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA
EASTERN DIVISION

No. 5:26-mj-1468-JG

IN THE MATTER OF THE SEARCH OF: INFORMATION ASSOCIATED WITH THE APPLIED APPLE ID Redacted THAT IS STORED AT PREMISES CONTROLLED BY APPLE INC.	UNDER SEAL

APPLICATION FOR NON-DISCLOSURE ORDER UNDER 18 U.S.C. § 2705(b)

The United States of America, by and through the United States Attorney for the Eastern District of North Carolina, hereby moves this Honorable Court, pursuant to 18 U.S.C. § 2705(b), for an Order prohibiting Apple Inc., from notifying any person of the existence of the search warrant submitted herewith until further order of the Court. In support of this application, the government states as follows:

1. Pursuant to 18 U.S.C. § 2711, 2703(a), (b)(1)(A) and (c)(1)(A), the government has applied to the Court contemporaneously herewith for a search warrant for content and information associated with the following Instagram account: "comey", that is stored at premises controlled by Apple Inc., an electronic communications service and/or a remote computing service located in Menlo Park, California.

2. Apple Inc. is a provider of electronic communication service, as defined in 18 U.S.C. § 2510(15), and/or a remote computing service, as defined in 18 U.S.C. § 2711(12).

3. This Court has authority under 18 U.S.C. § 2705(b) to issue "an order commanding a provider of an electronic communication service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order." The Court may issue such an order "if it determines that there is reasonable cause to believe that notification of the existence of the warrant, subpoena, or court order will result in (1) endangering the life or physical safety of an individual; (2) flight from prosecution; (3) destruction of or tampering with evidence; (4) intimidation of potential witnesses; or (5) otherwise seriously jeopardizing an investigation or unduly delaying a trial."

4. Such a non-disclosure order is appropriate here because the search warrant relates to an ongoing, non-public criminal investigation. Disclosure of the search warrant will seriously jeopardize the investigation by revealing its existence, thereby giving the targets, known and unknown, and others who may be involved an opportunity and reason to flee, to destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize and obstruct the investigation.

5. Accordingly, the United States respectfully requests that the Court enter the attached proposed Order directing Apple Inc. not to disclose the existence or content of the search warrant for the following account: Redacted, to any person, including the subscriber/customer of

the account identified in the search warrant, except to an attorney for Apple Inc. for the purpose of receiving legal advice, for a period of one year.

Respectfully submitted this 18th day of March, 2026.

W. ELLIS BOYLE
United States Attorney

PHILIP L. AUBART
Assistant United States Attorney
Criminal Division
150 Fayetteville Street, Suite 2100
Raleigh, North Carolina 27601
Telephone: [redacted]
Email: [redacted]

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA
EASTERN DIVISION

NO. 5:24-MJ-1468-JG

IN THE MATTER OF THE SEARCH OF: INFORMATION ASSOCIATED WITH THE APPLIED APPLE ID **Redacted** THAT IS STORED AT PREMISES CONTROLLED BY APPLE INC.	ORDER TO SEAL APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

Upon motion of the United States, for good cause shown and for the reasons stated in the motion, it is hereby ORDERED that the Application and Affidavit for Search Warrant in the above-referenced matter, and the Motion to Seal, be sealed by the Clerk from this date until further order by this Court, except that a certified copy of the same be provided to the United States Attorney's Office, which then may provide copies to the Federal Bureau of Investigation.

This the 23 day of March, 2026.

JAMES E. GATES
United States Magistrate Judge

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA
EASTERN DIVISION

NO. 5:26-mj-1468-JG

IN THE MATTER OF THE SEARCH OF: INFORMATION ASSOCIATED WITH THE APPLIED APPLE ID Redacted THAT IS STORED AT PREMISES CONTROLLED BY APPLE INC.	MOTION TO SEAL APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

The United States of America, by and through the United States Attorney for the Eastern District of North Carolina, hereby moves this Honorable Court for an Order sealing the Application and Affidavit for Search Warrant regarding the above-referenced matter, and this Motion to Seal, and in support thereof, shows unto the Court as follows:

1. A Special Agent of the Federal Bureau of Investigation (FBI) has made an application for a search warrant on March 18, 2026, regarding the above-referenced property or premises.

2. The affidavit submitted in support of the search warrant contains substantial background information concerning an ongoing investigation being conducted by FBI. Disclosure of the affidavit would alert potential targets of the existence, scope, and details of the investigation and, therefore, would pose a risk of flight or the destruction of additional evidence and may otherwise compromise the investigation. See Baltimore Sun Co. v. Goetz, 886 F.2d 60 (4th Cir. 1989).

WHEREFORE, the Government moves for an Order sealing the Application and Affidavit for Search Warrant, and this Motion to Seal, until further order by this Honorable Court, except that a filed copy of the same be provided to the Office of the United States Attorney, which can thereafter provide a copy to the USSS.

Respectfully submitted, this 18th day of March, 2026.

W. ELLIS BOYLE
United States Attorney

PHILIP L. AUBART
Assistant United States Attorney
Criminal Division

UNITED STATES DISTRICT COURT

for the

Eastern District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH THE APPLE ID
Redacted
THAT IS STORED AT PREMISES CONTROLLED BY APPLE INC.

Case No. 5:26-mj-1468-JG

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Northern District of California
(identify the person or describe the property to be searched and give its location):

See Attachment A incorporated as if fully restated herein.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B incorporated as if fully restated herein.

YOU ARE COMMANDED to execute this warrant on or before 6 APRIL 2026 *(not to exceed 14 days)*
☐ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to any EDNC Magistrate Judge.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of ____.

Date and time issued: 23 MARCH 2026 11:09 A.M.

Judge's signature

City and state: Raleigh, NC

James E. Gates, United States Magistrate Judge
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the Apple iCloud account for Apple ID Redacted (SUBJECT ACCOUNT) that is stored at premises owned, maintained, controlled, or operated by Apple, Inc. ("Apple") at One Apple Park Way, Cupertino, CA 95014.

PLA

ATTACHMENT B

Particular Things to Be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, 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 Apple, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on November 17, 2025 and on February 20, 2026, Apple is required to disclose the following information to the government for the SUBJECT ACCOUNT described in Attachment A for the period of **May 14, 2025 to May 21, 2025,** unless otherwise specified:

a) All records or other information regarding the identification of the SUBJECT ACCOUNT, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the SUBJECT ACCOUNT was created, the length of service, the IP address used to register the SUBJECT ACCOUNT, account status, associated devices, and methods of connecting.

b) All records or other information regarding the devices associated with, or used in connection with, the SUBJECT ACCOUNT (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"),

PLA

International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c) Any and all email addresses or social media usernames connected to the SUBJECT ACCOUNT, including by cookie or SMS;

d) For the time period of **May 14, 2025**, to **May 21, 2025,** records of any FaceTime video or audio calls placed or accepted, as well as contents of all instant messages associated with the SUBJECT ACCOUNT, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the SUBJECT ACCOUNT (including all draft and deleted messages), the source and destination account or phone number associated with each instant message or call, the date and time at which each instant message was sent or call was placed, the size and length of each instant message or call, the actual IP addresses of the sender and the recipient of each instant message or call, and the media, if any, attached to each instant message;

e) The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f) All activity, connection, and transactional logs for the SUBJECT ACCOUNT (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and capability query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My and AirTag logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

PLA

g) All records and information regarding locations where the SUBJECT ACCOUNT or devices associated with the SUBJECT ACCOUNT were accessed, including all data stored in connection with AirTags, Location Services, Find My, and Apple Maps;

h) All photos and videos saved under the SUBJECT ACCOUNT, including Exchangeable Image Files ("EXIF") data and any other metadata associated with those photos and videos;

i) All records pertaining to executed search terms and browser history on Safari;

j) All records pertaining to the types of services used;

k) All records pertaining to communications between Apple and any person regarding the SUBJECT ACCOUNT, including contacts with support services and records of actions taken; and

l) All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within (fourteen) 14 DAYS of issuance of this warrant.

PLA

II. SEARCH PROCEDURES FOR HANDLING POTENTIALLY PRIVILEGED INFORMATION

1. The following procedures will be followed at the time of the search in order to appropriately handle potentially privileged information (material that may potentially be protected by the attorney-client privilege, the attorney work product doctrine, or other recognized privilege or protection).

2. These procedures will be executed by: (a) law enforcement personnel conducting the investigation and search and other individuals assisting law enforcement personnel in the search, including any prosecutor participating in these investigation (the "Search Team") and (b) individual(s) not participating in the investigation of the matter, who will be available to assist in the event that a procedure involving potentially privileged information is required (the "Privilege Review Team").

3. The Search Team will receive the material to be seized described in [Section I] above. Account material reasonably considered to contain potentially privileged information will be transferred to the Privilege Review Team. The Privilege Review Team will review the material as set forth herein for potentially privileged information.

4. The Privilege Review Team will conduct a review of the material using search protocols specifically chosen to identify and segregate documents or data containing potentially privileged information, including through the use of search terms. All material capable of containing any of the items to be seized may be reviewed using this procedure. Material identified by this review as not potentially privileged, including material that does not contain the privilege search terms, may be released to the Search Team without court intervention.

5. Material identified during the Privilege Review Team's review to be potentially privileged will be segregated. The Privilege Review Team's attorney may do any of the following with segregated potentially privileged material: (a) apply *ex parte* to the court for a determination whether or not the material contains privileged information; (b) defer seeking court intervention and instead segregate the material in a manner that makes it inaccessible to the Search Team; or (c) disclose the material to the potential privilege holder, request a privilege log if the potential privilege holder asserts privilege, and seek a ruling from the court regarding the material if the parties cannot reach agreement.

6. Notwithstanding these procedures, where a Search Team member otherwise reviews material not previously determined to contain potentially privileged information, and later determines that such material may be potentially privileged, the material will then be segregated from the Search Team, provided to the Privilege Review Team, and handled in accordance with these procedures.

III. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. § 875(c) (communication containing any threat to kidnap any person or any threat to injure the person of another and/or transmitting a threat in interstate commerce) and 18 U.S.C. § 871 (knowingly and willfully making threats to take the life of or inflict bodily harm upon the President of the United States) by James Brien Comey, the owner of the SUBJECT ACCOUNT identified in Attachment A, in the form of the following:

a.) Any evidence of Comey researching "86", "47," or "86 47" including but not limited to historical browser searches and any records with geolocation data on May 15, 2025.

PLA

b.) Any photos or videos of "86," "47," or "86 47" and the metadata associated with the photos.

c.) Any evidence that would speak to Comey's state of mind on or around May 15, 2025.

d.) Any notes or communications related to the Instagram post Comey made on May 15, 2025.

e.) Any records indicating how and when the SUBJECT ACCOUNT was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the Target Offenses;

f.) The identity of the user(s) of the SUBJECT ACCOUNT, including (but not limited to) names, the location of the user, passwords, login IP addresses, session times and durations, and communications with other internet accounts (whether email, domain, or any other) under the control of the user(s);

g.) All records and communications indicating the identity of the user, as well as the identity of the person(s) who communicated with the user of the account about matters relating to the crimes under investigation, including records that help reveal their whereabouts.

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

PLA

disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review. If the government's review reveals any information in any form that may be protected by the attorney-client privilege or work-product doctrine, the review shall stop immediately and the government shall contact the court for guidance.

pcs

PLA

FILED

AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

MAR 23 2026

PETER A. MOORE, JR., CLERK
US DISTRICT COURT, EDNC
BY _____ DEP CLK

UNITED STATES DISTRICT COURT

for the

Eastern District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH THE APPLE ID Redacted THAT IS STORED AT PREMISES CONTROLLED BY APPLE INC.

Case No. 5:26-MJ-1468-JG

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A incorporated as if fully restated herein.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized):*

See Attachment B incorporated as if fully restated herein.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

Second and third boxes marked with "X" at Applicant's direction. JG

The search is related to a violation of:

Code Section	*Offense Description*
18 USC 875(c)	Interstate transmission of threats
18 USC 871	Threats against the President

The application is based on these facts:

See the attached affidavit, incorporated as if fully restated herein.

☑ Continued on the attached sheet.

☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

April Floyd
Applicant's signature

Special Agent April Floyd
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means).*

Date: 23 March 2026

Judge's signature

City and state: Raleigh, NC

James E. Gates, United States Magistrate Judge
Printed name and title

PLA

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH THE APPLE ID **Redacted** THAT IS STORED AT PREMISES CONTROLLED BY APPLE INC.	Case No. 5:26-mj-1468-JG **FILED UNDER SEAL**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, April B. Floyd, of the Federal Bureau of Investigation (FBI), assigned to the Charlotte Division, Wilmington Resident Agency, being duly sworn, deposed, and state as follows:

INTRODUCTION

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI) and have been so employed since March of 2016. I am currently assigned to the FBI Charlotte Division, Wilmington Resident Agency, where I am assigned to investigate complex white collar crimes involving violations of federal law. In my current capacity, I am assigned to investigate public corruption related crimes, deprivations of civil rights, including hate crimes, color of law violations, and violations of the FACE Act and the Hobbs Act, among other federal violations. I previously investigated matters involving complex drug investigations focusing on Transnational Organized Crime in the Western Hemisphere. I received extensive training in investigations as a New Agent Trainee at the FBI Academy in Quantico, Virginia. Prior to my employment with the FBI, I was a state law enforcement agent for four (4) years in the State of North Carolina

PLA

responsible for administering the Unauthorized Substances Tax. I was also a patrol officer at a local law enforcement agency for a year. I have approximately fifteen (15) years of combined law enforcement experience. My training has continued through in-service training seminars during my assignment as an FBI Special Agent. I have participated in ordinary methods of investigation, including, but not limited to, consensual monitoring, physical surveillance, interviews of witnesses and subjects, the use of confidential informants, the use of undercover agents, the execution of digital and physical search warrants, Title III court-ordered interceptions, and FISA court-ordered interceptions. Through these investigations, my training and experience, and conversations with other agents and law enforcement personnel, I have become familiar with methods used by individuals to commit violations of federal law.

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

3. I make this Affidavit in support of an Application for a Search Warrant for information associated with Apple ID **Redacted** (SUBJECT ACCOUNT) that is stored at premises controlled by Apple, Inc ("Apple"), a mobile communications and cloud storage company headquartered at One Apple Park Way, Cupertino, California (CA) 95014. The information to be searched is described in the following paragraphs and in Attachment A. This Affidavit is made 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 to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

PLA

4. The statements contained in this Affidavit are based in part on information provided by FBI Special Agents, United States Secret Service (USSS) Special Agents, and local law enforcement partners; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents; and my experience, training, and knowledge as a Special Agent with the FBI. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause that a violation of 18 U.S.C. § 875(c), and/or 18 U.S.C. § 871 has been committed by James Comey (referred to hereinafter as Comey), the known user of the SUBJECT ACCOUNT, and contraband and evidence, fruits, and instrumentalities of those violations will be found in the SUBJECT ACCOUNT.

STATUTORY AUTHORITY and JURISDICTION

5. As noted above, this investigation concerns an alleged violation of 18 U.S.C. § 875(c), which prohibits communication containing any threat to kidnap any person or any threat to injure the person of another/transmitting a threat in interstate commerce and 18 U.S.C. § 871 which prohibits knowingly and willfully making threats to take the life of or inflict bodily harm upon the President of the United States. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C, §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the 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).

PLA

PROVIDER BACKGROUND[1]

6. Apple is a United States company that designs, manufactures, and markets mobile communication and media devices, personal computers, and portable digital music players, and sells a variety of related software, services, peripherals, networking solutions, and third-party digital content and applications. Apple's products and services include Mac, iPhone, iPad, iPod, Apple TV, a portfolio of consumer and professional software applications, the iOS and Mac OS X operating systems, iCloud, and a variety of accessories, service and support offerings. Apple also sells and delivers digital content and applications through the iTunes Store, App Store, iBookstore, and MacApp Store.

7. The iPhone is a line of smartphones designed and marketed by Apple. It runs Apple's iOS mobile operating system. The user interface is built around the iPhone's multitouch screen, including a virtual keyboard. The iPhone has wireless internet capabilities and can connect to many cellular networks around the world. The iPhone can shoot video, send and receive email, browse the Internet, send text messages, provide navigation services via Global Positioning Satellite location technology, record notes, do mathematical calculations, and receive visual and audio voicemail. Other functions such as video games, reference works, social networking—including Facebook, Instagram and Twitter—can be enabled by downloading application programs ("apps" or, singular, "app"). Apple operates an App Store which offers numerous apps by Apple and third parties.

---

1 The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf; "Manage and use your Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "Introduction to iCloud," available at https://support.apple.com/kb/PH26502; "What does iCloud back up?," available at https://support.apple.com/kb/PH12519; and "Apple Platform Security," available at https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf.

PLA

8. 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 audio and video calls.

c) iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple's servers to utilize iCloud-connected services 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 and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iCloud Backup allows users to create a backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud

PLA

Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

d) Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

e) Find My allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of iOS devices, as well as share their location with other iOS users. It also allows owners of Apple devices to manage, interact with, and locate AirTags, which are tracking devices sold by Apple.

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. When Location Services is turned on for the Camera app, it uses this information to determine the location coordinates where the photo or video is taken. These coordinates are embedded into each photo and video so that you can later search for them in the Photos app based on the location they were taken. When photos and videos that include location metadata are shared, the people you share them with may be able to access the location metadata and learn where it was taken.[2]

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

2 https://support.apple.com/guide/personal-safety/manage-location-metadata-in-photos-ips0d7a5df82/web

PLA

through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

9. 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. The account identifier for an Apple ID is an email address, provided by the user. 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. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

10. 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. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. 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

PLA

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.

11. 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, "capability query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the "Find My" service, including connection logs and requests to remotely find, lock, or erase a device, are also maintained by Apple.

12. 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 into 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.

PLA

13. 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 (iWork 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, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple. Records and data associated with third-party apps, including the instant messaging service WhatsApp, may also be stored on iCloud.

14. The following additional information may be available from Apple:

a) Subscriber Information. When a customer sets up an iCloud account, basic subscriber information such as name, physical address, email address, and telephone number may be provided to Apple. Additionally, information regarding iCloud feature connections may also be available. iCloud subscriber information and connection logs with Internet Protocol ("IP") addresses can be obtained with a subpoena or greater legal process.

b) Mail Logs. Mail logs include records of incoming and outgoing communications such as time, date, sender email addresses, and recipient email addresses.

c) Email Content. iCloud stores the email a subscriber has elected to maintain in the account while the subscriber's account remains active.

PLA

d) Device Information. Apple maintains information regarding the types and identities of devices used to access iCloud accounts, including mobile telephones, computer tablets, laptop and desktop computers, and other computing devices.

e) Other iCloud Content. Photo Stream, Docs, Contacts, Calendars, Bookmarks, iOS, Device Backups, and Encryption Keys. iCloud stores content for the services that the subscriber has elected to maintain in the account while the subscriber's account remains active. Apple does not retain deleted content once it is cleared from Apple's servers. iCloud content may include stored photos, documents, contacts, calendars, bookmarks and iOS device backups. iOS device backups may include photos and videos in the users' camera roll, device settings, app data, iMessage, SMS, and MMS messages and voicemail. iCloud backups for all operating systems are encrypted by default. However, an iCloud account may include encryption keys contained in "keybag" and "FileInfoList.txt" files – enabling law enforcement to decrypt the contents of these backups.

f) 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

PLA

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.

g) Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

h) Historical geolocation data. Apple stores information regarding the historical location of iPhone and other Apple devices associated with iCloud accounts;

i) Find My iPhone and Remote Deletion Activity: Find My iPhone is a user-enabled feature by which an iCloud subscriber is able to locate his/her lost or misplaced iPhone, iPad, iPod touch or Mac and/or take certain actions, including putting the device in lost mode, locking or wiping the device.

j) App Store and iTunes Store. These 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. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

k) iPhone Dev Center and Apple Developer. These services allow users to develop software and computer code for Apple platforms, including iPhone apps.

PLA.

l) Preserved Data. Apple typically maintains preserved copies of the foregoing categories of records with respect to an account, for at least 90 days, upon receiving a preservation request from the Government pursuant to 18 U.S.C. § 2703(f).

PROBABLE CAUSE

15. Based upon findings of the investigation to date, there is probable cause to believe that evidence, fruits, and/or instrumentalities of crimes, including a violation of 18 U.S.C. § 875 (c) and 871 are located on the Apple account attributable to Redacted (SUBJECT ACCOUNT).

16. On May 15, 2025, the United States Secret Service (USSS) was notified of an Instagram post authored by Comey, Redacted in Emerald Isle, North Carolina, utilizing the Instagram handle "comey." The post included a photo containing seashells arranged on a beach to form the numbers "86 47" and the caption "Cool shell formation on my beach walk." The post was reported to the USSS as a possible call for violence against President Donald J. Trump given the association of the numbers. Use of the number "86" to imply a specific meaning has been attributed to multiple origins and resulting meanings. The number "86" has been associated as a slang term having the meaning "to kill," and the number "47" is widely recognized as a reference to the 47th President of the United States of America, Donald J. Trump. Additionally, one (1) common belief is that the term "86" originated within the restaurant industry to mean "to throw out, to get rid of, or to refuse service to."[3] More recently, the term has been attributed to an organized crime context, in which it refers to taking someone "eight miles out of town" and putting

3 See e.g., What does 'Eighty-Six' mean?, Merriam-Webster Dictionary, https://www.merriamwebster.com/wordplay/eighty-six-meaning-origin; see also, What are the Origins of and Meaning of '86' ? The History Channel, https://www.history.com/articles/86-meaning.

PLA.

them "six feet under."[4] In addition to serving as an Assistant United States Attorney for a number of years, Comey served as the former United States Attorney for the Southern District of New York from 2002-2003, as the United States Deputy Attorney General from 2003-2005, and as the Director of the Federal Bureau of Investigation from 2013-2017. Within these positions, Comey handled a variety of criminal cases, including serious crimes of violence committed by organized criminal organizations.[5]

17. On May 15, 2025, shortly after he added the post to Instagram, Comey deleted the "86 47" post and authored an apology post and posted it to his Instagram account with the handle "comey," which stated, "I posted earlier a picture of some shells I saw today on a beach walk, which I assumed were a political message. I didn't realize some folks associated those numbers with violence. It never occurred to me but I oppose violence of any kind so I took the post down." Sometime after making the post on May 15, 2025, Comey attempted to call Emerald Isle Police Chief, Michael Panzarella (referred to hereinafter as Panzarella). Panzarella did not answer the phone, and Comey left him a voicemail. In the voicemail, Comey provided his cellular telephone number of **Redacted** Comey stated, "We're down here in Emerald Isle," and that he "accidentally caused some sort of um excitement on social media today by posting a picture of shells that I saw on the beach at The Point and didn't realize that some people interpret it in a dark way..." Comey went on to say that he made the post to Instagram, but took the post down and posted a statement stating he had no idea that people associated those numbers with violence, and

4 See e.g., What Does '86' Mean? White House Reacts to James Comey's Post, Newsweek (May 15, 2025,9:28PM), https://www.newsweek.com/what-does-86-mean-trumn-iames-comev-instagram-2073055.

5 See e.g., James B. Comey Bio, The Whitehouse Archives, https://georgewbush-whitehouse.archives.gov/govemment/comey-bio.html

PLA.

he thought the shells arranged in the numbers "86 47" depicted "a political message." Comey further stated, "I said in my statement I had no idea people associate that with violence which of course I want no part of. But I just wanted to alert you to it because we had some…one of our neighbors walk up and give me the double bird…uh… from the beach as I sat on the porch. I hope that's the end of it, but I wanted to flag it for you all."

18. According to USSS reports, on May 15, 2025, Comey contacted USSS' Washington Field Office (WFO) via his cell phone number of Redacted and spoke to Assistant to the Special Agent in Charge (ATSAIC), [redacted] Comey stated he was walking on the beach that afternoon with his wife (Patrice Comey referred to hereinafter as Patrice) and saw the seashells arranged on the sand. Comey took a picture of the seashells and posted the picture.

19. On May 16, 2025, Comey was interviewed by the USSS. Comey's personal attorney, David Kelly (referred to hereinafter as Kelly), attended the interview telephonically. USSS Special Agents showed Comey printed screenshots of the Instagram account with the handle "comey," and Comey confirmed the Instagram account with the handle "comey" was in fact his account. Comey was shown two (2) posts that were made to his Instagram account on May 15, 2025, one (1) being a photo of seashells arranged on a beach displaying the numbers "86 47," and the second being a post containing an apology and explanation that the previous post had been taken down by him later in the day on May 15, 2025. Comey confirmed that he was the individual who uploaded both posts in question. When Comey was asked to explain why he posted the photo of the seashells, Comey stated that he found them during a walk on the beach with his wife (Patrice) in Emerald Isle, North Carolina. According to Comey, when they first saw the shells, Patrice thought it may have been an address number for a beachside house, but then Comey realized that it was a political message. In the voicemail discussed above that Comey left for Emerald Isle Police Department

PLA

Chief Panzarella, Comey stated he saw the shells on the beach "at The Point." Comey followed the voicemail up with a text message.

Redacted

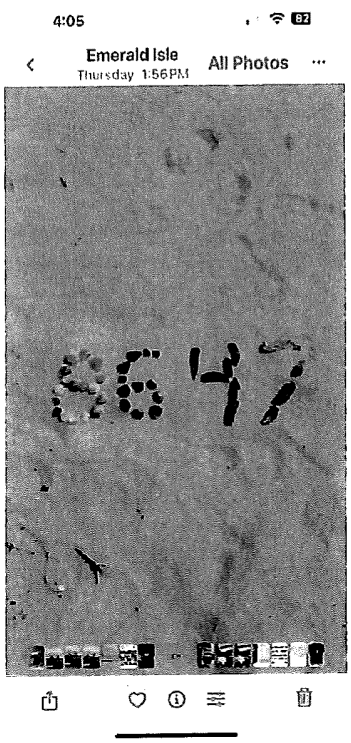
Redacted

PLA.

Comey denied placing the shells on the beach and denied knowing who placed the shells on the beach. According to Comey, Patrice suggested that he should take a picture of the shells. Comey interpreted the number "86" as a term meaning to "ditch, dump, or replace" and the number "47" as representing President Trump. Comey told investigators he viewed this message strictly in a non-violent manner. Comey acknowledged that he was a "political opponent" of President Trump, but that he wished that no harm would come to the President. Comey did not feel that the post was reckless because he stated that at the time he made the post, he did not perceive that people would interpret his message in a dark manner.

20. On May 23, 2025, at approximately 9:53am, USSS Assistant to the Special Agent in Charge, Jamie Marcella (referred to hereinafter as Marcella), sent Kelly (Comey's Attorney) an email requesting the following: "the photograph taken on the beach of the seashells, screenshots of any text conversations related to the seashell photograph, any instagram posts related to the seashell photograph, the signed SSF 1945, Release of Medical and Mental Health records. " On May 23, 2025, at approximately 2:29pm, Kelly responded to Marcella's email with, "Please see below and attached." In the email, Kelly included his responses to Marcella's original request/email in red text. Kelly emailed multiple screenshots, to include a screenshot of the photograph taken on the beach of the seashells and a screenshot of the image posted to Comey's Instagram account after the shell formation post was taken down:

PLA



21. Notably, Kelly did not send the original photo of the shell formation despite USSS' request for "the photograph taken on the beach of the seashells." In my training and experience, I am familiar with the method of sending screenshots of photographs rather than the original photos as an attempt to hide metadata associated with the original images. Additionally, the screenshot contained part of the "camera roll" of Comey's phone and included small thumbnails of other photos in the Photo Library. It is typical for images in a camera roll to be ordered sequentially when they are taken. Appearing after the image of the shell formation are two (2) images of two (2) unidentified individuals walking up a wooden walkway from the ocean/beach. In the aforementioned voicemail Comey left Panzarella, Comey stated in part, "But I just wanted to alert you to it because we had some…one of our neighbors walk up and give me the double bird…uh… from the beach as I sat on the porch." Other photos that appear after the shell formation photo include a t-shirt with numbers "86 46" and a partial cover of Comey's crime novel, FDR DRIVE.

PLA.

Comey's crime novel, FDR DRIVE, was released in May 2025 around the time of his Instagram post of the seashells on the beach.

22. On May 17, 2025, USSS Agents telephonically interviewed Patrice on her telephone number of Redacted Patrice told investigators that she and Comey found the shell formation, and she did not know who placed the seashells on the beach. Patrice recalled the term "86" from her time as a waitress, and in that context, "86" meant that the restaurant was out of an item, "like we're 86 on broccoli." Patrice told investigators she also thought the term could mean to dump or get rid of an item in a non-violent way. According to Patrice, sometime around 1600 hours on May 15, 2025, she received a text message from Redacted Redacted stating that the post that Comey made was a call to violence against President Trump. Since this had not occurred to her, Patrice performed a search on Google of the numbers "86 47" and learned that it could be interpreted in a violent manner. Patrice immediately notified Comey about this interpretation, and he took down the post.

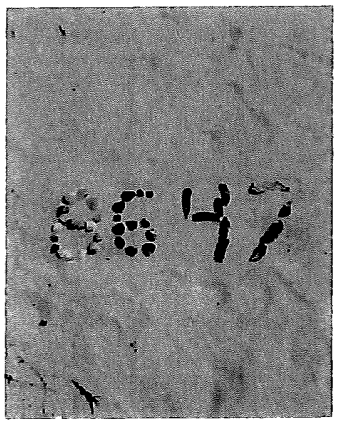
23. On May 15, 2025, USSS Agents telephonically interviewed Redacted on Redacted telephone number of Redacted. One (1) of Redacted friends sent him a screenshot of Comey's post via text message. Redacted reported that Redacted worked in the restaurant industry and was familiar with the term "86" meaning that a restaurant was out of food or a type of ingredient; however, Redacted immediately perceived Comey's post to contain a violent meaning. Redacted immediately perceived the term "86 47" as a call to get rid of, in a violent way, or even to assassinate President Trump. Redacted told investigators Redacted contacted Patrice via text message to voice Redacted dissatisfaction and frustration with the post. Based on Comey's extensive experience as a lawyer and with the FBI, Redacted felt Comey must have known that "86 47" was a call for violence.

24. On August 22, 2025, the USSS executed a search warrant on Meta for information

PLA.

associated with Comey's Instagram account (see 5:25-MJ-2073-J6). According to Meta, the registered email address for the account was Redacted. The email was listed as "verified" which indicated the account holder responded to an email sent to the listed email address. The name on the account was James Comey and the verified phone number on the account was Redacted

25. According to the Meta returns, on May 15, 2025, at approximately 19:14:04 UTC (3:14pm EDT), the "comey" Instagram account posted the following photo:



26. The source of the photo was listed as iOS Library with an upload IP of Redacted The general location of the IP address was Redacted The status of the post was listed as "Deleted by user."

27. After Comey's posts to Instagram, he participated in appearances on various media outlets. One (1) such appearance was on The Late Show on May 20, 2025. During his appearance on the Late Show, Stephen Colbert asked Comey about the "86 47" Instagram post. Comey provided a detailed response to Colbert showing him a placard displaying the Instagram post. Darby Stanchfield (referred to hereinafter as Stanchfield), an actress in the ABC drama Scandal,

6 Based on a search using https://ipwhois.io/

PLA.

answered questions about what it was like to be a late-night talk show guest.[7] According to Stanchfield, prior to appearances on late-night shows, producers of the shows conducted "pre-interviews." Stanchfield spoke of her experience as a guest on Jimmy Kimmel Live. As part of these interviews, producers of the show went over "stories, anecdotes, current events, etc. that you might think to share." Next, the producer reviewed the pre-interview with the host, and the producer and the host decided what to include in the show. According to Stanchfield, the subjects that were covered during the show with the guest were "planned out," and before the guest appeared on the show, the guest was advised what would be talked about on the show. Based on Stanchfield's account of appearing on a light-night show, I believe it is likely that Comey engaged in conversations prior to the interview regarding the topic of the "86 47" post.

28. On November 17, 2025, and again on February 20, 2026, the FBI submitted a preservation request to Apple for iCloud account data associated with Comey's number of Redacted Redacted On November 19, 2025, a Federal Grand Jury Subpoena was served on Apple for information for accounts associated with telephone number Redacted On November 26, 2025, in response to the subpoena, Apple provided information for two (2) accounts associated with phone number Redacted one (1) with apple ID Redacted (SUBJECT ACCOUNT) and one (1) with Apple ID Redacted

29. According to the Apple returns, the SUBJECT ACCOUNT uses the following iCloud features: iCloud Backup, Bookmarks, Calendars, iCloud Photos, Contacts, Find My friends, iCloud Drive, Messages in iCloud, Notes, and Sign in with Apple. Apple additionally provided iCloud logs for the account from November 13, 2024 to November 14, 2025. The logs

7 https://slate.com/human-interest/2014/11/jimmy-kimmel-what-is-it-like-to-be-a-late-night-talk-show-guest-on-his-show.html

PLA

show the SUBJECT ACCOUNT utilized the Cloud Photo Library service via IP address Redacted (the IP address associated with the May 15, 2025 post) as recently as November 10, 2025.

Evidence located in Comey's iCloud account

30. Based on my training and experience, I know that various apps back up to the iCloud; and data stored in iCloud accounts also captures geolocation data, photos and videos taken by the account holder, and communications sent or received by the account holder. Additionally, information gleaned from close-in-time photographs may be of investigative/evidentiary value. There is probable cause to believe evidence related to communications containing any threat to kidnap any person or any threat to injure the person of another/transmitting a threat in interstate commerce and/or threats against the President will be found in Comey's personal iCloud account.

31. This search warrant application requests data from the SUBJECT ACCOUNT from May 14, 2025 to May 21, 2025, for the purpose of identifying any evidence related to communications containing any threat to kidnap any person or any threat to injure the person of another and/or transmitting a threat in interstate commerce, and/or threats against the President, through geolocation data, photo data and/or search history; to identify any evidence that Comey deliberately deleted data to destroy evidence of his alleged criminal activity; to identify his knowledge of the meaning behind "86," and to identify any unenumerated evidence of the allegations described herein.

DEFINITIONS

32. The following definitions apply to this Affidavit:

a) "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or

PLA

storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, and mobile phones and devices. *See* 18 U.S.C. § 1030(e)(1). "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

b) A provider of "Electronic Communication Service" ("ESP"), as defined in 18 U.S.C. § 2510(15), is any service that provides to users thereof the ability to send or receive wire or electronic communications. For example, "telephone companies and electronic mail companies" generally act as providers of electronic communication services. *See* S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3568.

c) Instant messaging (IM) is a collection of technologies that create the possibility of real-time text-based communication between two or more participants via the Internet. Instant messaging allows for the immediate transmission of communications, including immediate receipt of acknowledgment or reply.

PLA

d) The term "Internet" is defined as the worldwide network of computers, a noncommercial, self-governing network devoted mostly to communication and research with roughly 500 million users worldwide. The Internet is not an online service and has no real central hub. It is a collection of tens of thousands of computer networks, online services, and single user components. In order to access the Internet, an individual computer user must use an access provider, such as a university, employer, or commercial Internet Service Provider ("ISP"), which operates a host computer with direct access to the Internet.

e) The term "ISP" (Internet Service Provider), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

f) An IP address is a number that uniquely identifies internet-connected computers. When one computer interacts with a second computer over the internet, the first computer communicates its IP address to the second computer, so that each computer can communicate with the other. The system of IP addresses is managed by the Internet Corporation For Assigned Names and Numbers ("ICANN"), together with five Regional Internet Registries (essentially, one for each populated continent except Australia, which is combined with most of Asia), including the American Registry for Internet Numbers ("ARIN"), which has responsibility for North America. ARIN registers IP addresses for internet-connected computers in North America and maintains records about the registered owners for those IP

PLA

addresses. ARIN registered owners are typically large users or organizations, such as remote computing or internet service providers (e.g., Comcast), who can internally assign IP addresses to computers that belong to individual subscribers.

g) The term "mobile device," as used herein, is defined as a small, hand-held computing device, having a display screen, and an operating system (OS), with some type of input capabilities (such as a touch screen or a small keyboard), and is typically powered by a battery. Mobile devices are used to run various types of application software, known as "apps," as well as communication functions allowing voice telephone calls, email communications, SMS and MMS functions. Cell phones, "Smart phones", tablets, and PDAs are popular forms of mobile devices. Most handheld devices are often equipped with Wi-Fi, Bluetooth, and GPS capabilities, allowing the device to connect to the Internet and other devices (such as a vehicle or a microphone headset) or can be used to provide location-based services (like mapping and directional applications). Most mobile devices typically have an internal camera for taking and recording still image and video files, which are then stored within the memory of the mobile device or on a digital media storage device, like an SD card.

h) "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

i) A "server" is a centralized computer that provides services for other computers connected to it via a network or the Internet. The computers that use the server's services are sometimes called "clients." When a user accesses email, Internet web

PLA

pages, or accesses files stored on the network itself, those files are pulled electronically from the server, where they are stored, and are sent to the client's computer via the network or Internet. Notably, server computers can be physically located in any location; for example, it is not uncommon for a network's server to be located hundreds (or even thousands) of miles away from the client computers. In larger networks, it is common for servers to be dedicated to a single task. For example, a server that is configured so that its sole task is to support a World Wide Web site is known simply as a "Web server." Similarly, a server that only stores and processes e-mail is known as a "mail server."

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

33. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

34. I respectfully submit that reasonable cause exists to permit the execution of the requested warrant at any time in the day or night, because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it.

CONCLUSION

Based on the foregoing factual information, I respectfully submit that there is probable cause to believe that evidence of criminal offenses, namely 18 U.S.C. § 875(c) (communication containing any threat to kidnap any person or any threat to injure the person of another and/or

PLA

transmitting a threat in interstate commerce) and 18 U.S.C. § 871 (knowingly and willfully making threats to take the life of or inflict bodily harm upon the President of the United States) is located in the SUBJECT ACCOUNT, as described in Attachment A, and this evidence, more fully described in Attachment B, is contraband, the fruits of crime, or property which is or has been used as the means of committing the foregoing offenses.

PLA.

35. I respectfully request that the attached warrant be issued authorizing the search of the SUBJECT ACCCOUNT as described in Attachment A, and authorizing the seizure and search of the items described in Attachment B.

April B. Floyd

Special Agent

Federal Bureau of Investigation

Pursuant to Rule 4.1 of the Federal Rules of Criminal Procedure, the affiant appeared before me via reliable electronic means, was placed under oath, and attested to the contents of this affidavit this 23 day of March 2026.

James E. Gates

United States Magistrate Judge

PLA

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the Apple iCloud account for Apple ID Redacted (SUBJECT ACCOUNT) that is stored at premises owned, maintained, controlled, or operated by Apple, Inc. ("Apple") at One Apple Park Way, Cupertino, CA 95014.

PLA.

ATTACHMENT B

Particular Things to Be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, 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 Apple, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on November 17, 2025 and on February 20, 2026, Apple is required to disclose the following information to the government for the SUBJECT ACCOUNT described in Attachment A for the period of **May 14, 2025 to May 21, 2025,** unless otherwise specified:

a) All records or other information regarding the identification of the SUBJECT ACCOUNT, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the SUBJECT ACCOUNT was created, the length of service, the IP address used to register the SUBJECT ACCOUNT, account status, associated devices, and methods of connecting.

b) All records or other information regarding the devices associated with, or used in connection with, the SUBJECT ACCOUNT (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"),

PLA

International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c) Any and all email addresses or social media usernames connected to the SUBJECT ACCOUNT, including by cookie or SMS;

d) For the time period of **May 14, 2025**, to **May 21, 2025,** records of any FaceTime video or audio calls placed or accepted, as well as contents of all instant messages associated with the SUBJECT ACCOUNT, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the SUBJECT ACCOUNT (including all draft and deleted messages), the source and destination account or phone number associated with each instant message or call, the date and time at which each instant message was sent or call was placed, the size and length of each instant message or call, the actual IP addresses of the sender and the recipient of each instant message or call, and the media, if any, attached to each instant message;

e) The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f) All activity, connection, and transactional logs for the SUBJECT ACCOUNT (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and capability query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My and AirTag logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

PLA

g) All records and information regarding locations where the SUBJECT ACCOUNT or devices associated with the SUBJECT ACCOUNT were accessed, including all data stored in connection with AirTags, Location Services, Find My, and Apple Maps;

h) All photos and videos saved under the SUBJECT ACCOUNT, including Exchangeable Image Files ("EXIF") data and any other metadata associated with those photos and videos;

i) All records pertaining to executed search terms and browser history on Safari;

j) All records pertaining to the types of services used;

k) All records pertaining to communications between Apple and any person regarding the SUBJECT ACCOUNT, including contacts with support services and records of actions taken; and

l) All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within (fourteen) 14 DAYS of issuance of this warrant.

PLA

II. SEARCH PROCEDURES FOR HANDLING POTENTIALLY PRIVILEGED INFORMATION

1. The following procedures will be followed at the time of the search in order to appropriately handle potentially privileged information (material that may potentially be protected by the attorney-client privilege, the attorney work product doctrine, or other recognized privilege or protection).

2. These procedures will be executed by: (a) law enforcement personnel conducting the investigation and search and other individuals assisting law enforcement personnel in the search, including any prosecutor participating in these investigation (the "Search Team") and (b) individual(s) not participating in the investigation of the matter, who will be available to assist in the event that a procedure involving potentially privileged information is required (the "Privilege Review Team").

3. The Search Team will receive the material to be seized described in [Section I] above. Account material reasonably considered to contain potentially privileged information will be transferred to the Privilege Review Team. The Privilege Review Team will review the material as set forth herein for potentially privileged information.

4. The Privilege Review Team will conduct a review of the material using search protocols specifically chosen to identify and segregate documents or data containing potentially privileged information, including through the use of search terms. All material capable of containing any of the items to be seized may be reviewed using this procedure. Material identified by this review as not potentially privileged, including material that does not contain the privilege search terms, may be released to the Search Team without court intervention.

PLA

5. Material identified during the Privilege Review Team's review to be potentially privileged will be segregated. The Privilege Review Team's attorney may do any of the following with segregated potentially privileged material: (a) apply *ex parte* to the court for a determination whether or not the material contains privileged information; (b) defer seeking court intervention and instead segregate the material in a manner that makes it inaccessible to the Search Team; or (c) disclose the material to the potential privilege holder, request a privilege log if the potential privilege holder asserts privilege, and seek a ruling from the court regarding the material if the parties cannot reach agreement.

6. Notwithstanding these procedures, where a Search Team member otherwise reviews material not previously determined to contain potentially privileged information, and later determines that such material may be potentially privileged, the material will then be segregated from the Search Team, provided to the Privilege Review Team, and handled in accordance with these procedures.

III. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. § 875(c) (communication containing any threat to kidnap any person or any threat to injure the person of another and/or transmitting a threat in interstate commerce) and 18 U.S.C. § 871 (knowingly and willfully making threats to take the life of or inflict bodily harm upon the President of the United States) by James Brien Comey, the owner of the SUBJECT ACCOUNT identified in Attachment A, in the form of the following:

a.) Any evidence of Comey researching "86", "47," or "86 47" including but not limited to historical browser searches and any records with geolocation data on May 15, 2025.

PLA

b.) Any photos or videos of "86," "47," or "86 47" and the metadata associated with the photos.

c.) Any evidence that would speak to Comey's state of mind on or around May 15, 2025.

d.) Any notes or communications related to the Instagram post Comey made on May 15, 2025.

e.) Any records indicating how and when the SUBJECT ACCOUNT was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the Target Offenses;

f.) The identity of the user(s) of the SUBJECT ACCOUNT, including (but not limited to) names, the location of the user, passwords, login IP addresses, session times and durations, and communications with other internet accounts (whether email, domain, or any other) under the control of the user(s);

g.) All records and communications indicating the identity of the user, as well as the identity of the person(s) who communicated with the user of the account about matters relating to the crimes under investigation, including records that help reveal their whereabouts.

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

PLA.

disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

PLA.

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA
EASTERN DIVISION

No. 5:26-MJ-1468-JG

IN THE MATTER OF THE SEARCH OF:

INFORMATION ASSOCIATED WITH THE APPLIED APPLE ID
Redacted
THAT IS STORED AT PREMISES CONTROLLED BY APPLE INC.

NON-DISCLOSURE ORDER
(UNDER SEAL)

This matter is before the Court upon the United States' application, pursuant to 18 U.S.C. § 2705(b), requesting that the Court issue an Order prohibiting Apple Inc., an electronic communication service provider and/or a remote computing service, from notifying any person of the existence of the attached search warrant until further order of the Court.

The attached search warrant requires Apple Inc. to disclose to the United States information and content pertaining to the following Instagram account: "comey", that is stored at premises controlled by Apple Inc., as set forth in the search warrant.

The Court determines that there is reason to believe that notification of the existence of the attached search warrant will seriously jeopardize the investigation by giving targets of the investigation an opportunity to flee, to destroy or tamper with evidence, or to change patterns of behavior. *See* 18 U.S.C. § 2705(b).

IT IS THEREFORE ORDERED, pursuant to 18 U.S.C. § 2705(b), that Apple Inc. shall not disclose the existence of the attached search warrant, or this Order of

the Court, to the listed subscriber or to any other person, unless and until otherwise authorized to do so by the Court for a period of one year, except that Apple Inc. may disclose the attached search warrant to an attorney for Apple Inc. for the purpose of receiving legal advice.

23 MARCH 2026
Date

JAMES E. GATES
United States Magistrate Judge