STEVEN W. MYHRE
Acting United States Attorney
District of Nevada
CRISTINA D. SILVA
PATRICK BURNS
Assistant United States Attorneys
501 Las Vegas Blvd. South, Ste. 1100
Las Vegas, Nevada 89101
Telephone: (702) 388-6336
Fax (702) 388-6698
john.p.burns@usdoj.gov

Attorney for the United States of America

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA
-oOo-

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH EMAIL ACCOUNTS CENTRALPARK1@LIVE.COM THAT IS STORED AT A PREMISES CONTROLLED BY MICROSOFT. A1	**Magistrate No.** 17-mj-968-NJK **AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR SEARCH WARRANTS** **(Under Seal)**
IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH EMAIL ACCOUNTS MARILOUROSES@LIVE.COM THAT IS STORED AT A PREMISES CONTROLLED BY MICROSOFT. A2	**Magistrate No.** **AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR SEARCH WARRANTS** **(Under Seal)**

STATE OF NEVADA)
) ss:
COUNTY OF CLARK)

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR SEARCH WARRANTS

I, Ryan S. Burke, Special Agent, Federal Bureau of Investigation (FBI), having been duly sworn, hereby depose and say:

INTRODUCTION AND AGENT BACKGROUND

1. Your Affiant makes this affidavit in support of an application for search warrants for information associated with email accounts centralpark1@live.com ("Target Account 1") and marilouroses@live.com ("Target Account 2"). Target Account 1 is an account associated with STEPHEN PADDOCK. Target Account 2 is an account associated with MARILOU DANLEY. The information associated with both accounts is stored at a premises owned, maintained, controlled, or operated by Microsoft Corporation ("Microsoft"), an American multinational technology company based in Redmond, Washington that specializes in Internet-related services and products along with the development and manufacturing of computer-related items. Those online services include, but are not limited to, email services, cloud computing, and many other services. The information to be searched is described in the following paragraphs and in Attachment "A" (attached hereto and incorporated herein by reference). This affidavit is made in support of an application for search warrants under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Microsoft to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the Target Accounts.

2. I am an "investigative or law enforcement officer of the United States" within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of

the United States who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Title 18, United States Code, Section 2516.

3. I have been employed as a Special Agent of the FBI for approximately five years, which began at the FBI Academy in October 2012. Upon completion of the academy, I was transferred to the Las Vegas Division's white collar crime squad and then the human trafficking squad. Since October 2015, I have been assigned to the Las Vegas Division's violent crime/gang squad. Additionally, I have been a certified member of the FBI's Cellular Analysis Survey Team since August 2015 due to my expertise in the field of historical cell site analysis.

4. During my tenure with the FBI, I have conducted surveillance, analyzed telephone records, interviewed witnesses, supervised activities of sources, executed search warrants, executed arrest warrants, and participated in court-authorized interceptions of wire and electronic communications. These investigative activities have been conducted in conjunction with a variety of investigations, to include those involving robbery, drug trafficking, kidnapping, murder, criminal enterprises, and more. In addition to my practical experiences, I received five months of extensive law enforcement training at the FBI Academy.

5. The facts in this affidavit are derived from your Affiant's personal observations, his training and experience, and information obtained from other agents, detectives, and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not set forth all of the Affiant's knowledge about this matter.

6. Based on your Affiant's training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of:

a. Destruction/Damage of Aircraft or Aircraft Facilities - 18 U.S.C.A. § 32(a);

b. Violence at International Airport - 18 U.S.C. § 37(a)(2); and

c. Unlawful Interstate Transport/Delivery of Firearms by Non Federal Firearms Licensee – 18 U.S.C. §§ 922(a)(3) and (5);

d. Aiding and Abetting – 18 U.S.C. § 2.

(hereafter, "Subject Offenses") have been committed by STEPHEN PADDOCK, MARILOU DANLEY, and others yet unknown. There is also probable cause to search the information described in Attachment "A" for evidence of these crimes and information which might reveal the identities of others involved in these crimes, as described in Attachment "B" (attached hereto and incorporated herein by reference).

PROBABLE CAUSE

7. On the evening of Sunday, October 1, 2017, Route 91 Harvest, a music festival, was in progress at 3901 South Las Vegas Boulevard, Las Vegas, Nevada. At approximately 10:08 p.m., the Las Vegas Metropolitan Police Department (LVMPD) received calls reporting shots had been fired at the concert and multiple victims were struck. LVMPD determined the shots were coming from Rooms 134 and 135 on the 32nd floor of the Mandalay Bay Resort and Casino, located due west of the festival rounds at 3950 South Las Vegas Boulevard, Las Vegas, Nevada. These rooms are an elevated position which overlooks the concert venue. Witness statements and video footage captured during the attack indicates that the weapons being used were firing in a fully-automatic fashion.

8. LVMPD officers ultimately made entry into the room and located an individual later identified as Stephen Paddock. Paddock was deceased from an apparent self-inflicted gunshot wound.

9. Paddock's Nevada driver's license was located in the Mandalay Bay hotel room with Paddock, and both hotel rooms were registered in his name. A player's club card in name of Marilou Danley was located in Paddock's room, and the card returned to the address located on Babbling Brook Street in Mesquite, Nevada. FBI Agents located Danley, who was traveling outside the United States at the time of the shooting. It was ultimately determined that Danley resided with Paddock at the Babbling Brook address.

10. On October 2, 2017, search warrants were executed on Paddock's Mandalay Bay hotel rooms, Paddock's vehicle at Mandalay Bay, and two Nevada residences owed by Paddock: 1372 Babbling Brook Court in Mesquite, and 1735 Del Webb Parkway in Reno, Nevada. Officers and Agents found over 20 firearms, hundreds of rounds of ammunition, and hundreds of spent shell casings in the Mandalay Bay hotel rooms, in close proximity to Paddock's body. Over a thousand rounds of rifle ammunition and 100 pounds of explosive material was found in Paddock's vehicle. Additional explosive material, approximately 18 firearms, and over 1,000 rounds of ammunition was located at the Mesquite residence. A large quantity of ammunition and multiple firearms were recovered from the Reno residence.

11. As of this date, 58 people have been identified to have been killed in Paddock's attack and another 557 were reportedly injured. Additionally, investigators discovered that STEPHEN PADDOCK also utilized a firearm to shoot large fuel tanks

on Las Vegas McCarran International Airport property. Multiple bullet holes were found on the tank, which investigators believe was an attempt by STEPHEN PADDOCK to cause the tanks to explode.

12. In an effort to determine whether or not STEPHEN PADDOCK was assisted and/or conspired with unknown individuals, investigators have attempted to identify all of STEPHEN PADDOCK's associated. It was quickly determined that a casino player's card in the name of MARILOU DANLEY was located in the room at the time of the attack. She has been identified thus far as the most likely person who aided or abetted STEPHEN PADDOCK based on her informing law enforcement that her fingerprints would likely be found on the ammunition used during the attack. Subsequently, investigators worked to identify the communication facilities utilized by STEPHEN PADDOCK and MARILOU DANLEY.

13. Based on a review of STEPHEN PADDOCK's financial accounts, Target Account 1 was determined to belong to STEPHEN PADDOCK. On October 3, 2017, investigators requested an emergency disclosure of records from Microsoft related to Target Account 1 so it could be immediately searched for any evidence of additional co-conspirators. Unfortunately, the information was only requested for a six month timeframe. Within the account, investigators identified Target Account 2 as one that belonged to MARILOU DANLEY, which was clear based on the communications between the two email accounts.

14. On September 25, 2017, an email was exchanged between the Target Accounts which discussed a wire transfer of funds which was to be sent by STEPHEN

PADDOCK to MARILOU DANLEY. It is unclear what the purpose of the wire transfer was, but MARILOU DANLEY is known to have been in the Philippines at the time.

15. Additionally, on July 6, 2017, Target Account 1 sent an email to centralpark4804@gmail.com which read, "try an ar before u buy. we have huge selection. located in the las vegas area." Later that day, an email was received back from centralpark4804@gmail.com to Target Account 1 that read, "we have a wide variety of optics and ammunition to try." And lastly, Target Account 1 later sent an email to centralpark4804@gmail.com that read, "for a thrill try out bumpfire ar's with a 100 round magazine." Investigators believe these communications may have been related to the eventual attack that occurred at the Mandalay Bay in Las Vegas.

16. Your Affiant believes the requested search warrants will yield significant information from Microsoft such as STEPHEN PADDOCK's and MARILOU DANLEY's contact lists, email messages content, IP address usage, photographs, third-party applications associated with the account, and more, which may constitute evidence of the planning of the attack and potentially identify other participants in the attack. Ultimately, your Affiant strongly believes the requested information will lead investigators to determine the full scope of STEPHEN PADDOCK's plan and MARILOU DANLEY's possible involvement.

RELEVANT TECHNICAL TERMS

17. The following non-exhaustive list of definitions applies to this Affidavit and the Attachments to this Affidavit:

a. The "Internet" is a worldwide network of computer systems operated by governmental entities, corporations, and universities. In order to access the Internet,

an individual computer user must subscribe to an access provider, which operates a host computer system with direct access to the Internet. The World Wide Web is a functionality of the Internet which allows users of the Internet to share information.

b. "Internet Service Providers" are companies that provide access to the Internet. ISPs can also provide other services for their customers including website hosting, email service, remote storage, and co-location of computers and other communications equipment. ISPs offer different ways to access the Internet including telephone-based (dial-up), broadband-based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite-based subscription. ISPs typically charge a fee based upon the type of connection and volume of data (bandwidth). Many ISPs assign each subscriber an account name, such as a user name, an email address, and an email mailbox, and the subscriber typically creates a password for his/her account.

c. "ISP Records" are records maintained by ISPs pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often in the form of log files), emails, information concerning content uploaded and/or stored on the ISP's servers, and other information, which may be stored both in computer data format and in written or printed record format. ISPs reserve and/or maintain computer disk storage space on their computer system for their subscribers' use. This service by ISPs allows for both temporary and long-term storage of electronic communications and many other types of electronic data and files.

d. "Online service providers" (also referred to here as "service providers") are companies that provide online services such as email, chat or instant

messaging, word processing applications, spreadsheet applications, presentation applications similar to PowerPoint, online calendar, photo storage and remote storage services. Sometimes they also can provide web hosting, remote storage, and co-location of computers and other communications equipment. Typically, each service provider assigns each subscriber an account name, such as a user name or screen name and the subscriber typically creates a password for his/her account.

e. "Computer," as used herein, is defined as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

f. A "server" is a centralized computer that provides services for other computers connected to it via a network. The other computers attached to a server are sometimes called "clients." For example, in a large company, it is common for individual employees to have client computers at their desktops. When the employees access their email, or access 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. Notably, servers can be physically stored in any location: it is not uncommon for a network's server to be located hundreds (and even thousands) of miles away from the client computers.

g. "Internet Protocol address," or "IP address," refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, that

is, an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

h. The term "domain" refers to a word used as a name for computers, networks, services, etc. A domain name typically represents a website, a server computer that hosts that website, or even some computer (or other digital device) connected to the internet. Essentially, when a website (or a server computer that hosts that website) is connected to the internet, it is assigned an IP address. Because IP addresses are difficult for people to remember, domain names are instead used because they are easier to remember than IP addresses. Domain names are formed by the rules and procedures of the Domain Name System (DNS). A common top level domain under these rules is ".com" for commercial organizations, ".gov" for the United States government, and ".org" for organizations. For example, www.usdoj.gov is the domain name that identifies a server used by the U.S. Department of Justice, and which uses IP address of 149.101.46.71.

i. "Web hosting services" maintain server computers connected to the Internet. Their customers use those computers to operate websites on the Internet. Customers of web hosting companies place files, software code, databases, and other data on servers. To do this, customers typically connect from their own computers to the server computers across the Internet.

j. The term "WhoIs" lookup refers to a search of a publicly available online database that lists information provided when a domain is registered or when an IP address is assigned.

k. The terms "communications," "records," "documents," "programs," or "materials" include all information recorded in any form, visual or aural, and by any

means, whether in handmade form (including, but not limited to, writings, drawings, paintings), photographic form (including, but not limited to, pictures or videos), or electrical, electronic or magnetic form, as well as digital data files. These terms also include any applications (i.e. software programs). These terms expressly include, among other things, emails, instant messages, chat logs, correspondence attached as to emails (or drafts), calendar entries, buddy lists.

l. "Chat" is usually a real time electronic communication between two or more individuals. Unlike email, which is frequently sent, then read and responded to minutes, hours, or even days later, chats frequently involve an immediate conversation between individuals, similar to a face-to-face conversation. Nearly all chat programs are capable of saving the chat transcript, to enable users to preserve a record of the conversation. By default, some chat programs have this capability enabled, while others do not. Many popular web-based email providers, like Microsoft and Microsoft, provide chat functionality as part of the online services they provide to account holders.

FACTS ABOUT EMAIL PROVIDERS

18. In my training, my experience and this investigation, I have learned that Microsoft (the Service Provider) is a company that provides free web-based Internet email access to the general public, and that stored electronic communications, including opened and unopened email for Microsoft subscribers may be located on the computers of Microsoft. I have also learned that Microsoft Inc. provides various on-line service messaging services to the general public. Instant Messaging ("IM") is a form of real-time direct text-based communication between two or more people using shared clients. The text is conveyed via devices connected over a network such as the Internet. In addition

to text, Microsoft's software allows users with the most current updated versions to utilize its webcam service. This option enables users from distances all over the world to view others who have installed a webcam on their end. Thus, the Service Provider's servers will contain a wide variety of the subscriber's files, including emails, address books, contact or buddy lists, calendar data, pictures, chat logs, and other files.

19. To use these services, subscribers register for online accounts like the Target Accounts. During the registration process, service providers such as the ones here ask subscribers to provide basic personal information. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit card or bank account number). Based on my training and my experience, I know that subscribers may insert false information to conceal their identity; even if this proves to be the case, however, I know that this information often provide clues to their identity, location or illicit activities.

20. In general, when a subscriber receives an email, it is typically stored in the subscriber's "mail box" on that service provider's servers until the subscriber deletes the Email. If the subscriber does not delete the message, the message (and any attachments) can remain on that service provider's servers indefinitely.

21. Similarly, when the subscriber sends an email, it is initiated at the subscriber's computer, transferred via the Internet to the service provider's servers, and then transmitted to its end destination. That service provider often saves a copy of the email sent. Unless the sender of the email specifically deletes the Email from the provider's server, the email can remain on the system indefinitely.

22. A sent or received email typically includes the content of the message, source and destination addresses, the date and time at which the email was sent, and the size and length of the email. If an email user writes a draft message but does not send it, that message may also be saved by that service provider, but may not include all of these categories of data.

23. Just as a computer on a desk can be used to store a wide variety of files, so can online accounts, such as the accounts subject to this application. First, subscribers can store many types of files as attachments to emails in online accounts. Second, because service providers provide the services listed above (e.g. word processing, spreadsheets, pictures), subscribers who use these services usually store documents on servers maintained and/or owned by service providers. Thus, these online accounts often contain documents such as pictures, audio or video recordings, logs, spreadsheets, applications and other files.

24. Reviewing files stored in online accounts raises many of the same difficulties as with reviewing files stored on a local computer. For example, based on my training, my experience and this investigation, I know that subscribers of these online services can conceal their activities by altering files before they upload them to the online service. Subscribers can change file names to more innocuous sounding names (e.g. renaming "FraudRecords.doc" to "ChristmasList.doc"), they can change file extensions to make one kind of file appear like a different type of file (e.g. changing the spreadsheet "StolenCreditProfiles.xls" to "FamilyPhoto.jpg" to appear to be a picture file, where the file extension ".xls" denotes an Excel spreadsheet file and ".jpg" a JPEG format image file), or they can change the times and dates a file was last accessed or modified by

changing a computer's system time/date and then uploading that file to the Online Accounts. Thus, to detect any files that the subscriber may have concealed, agents will need to review all of the files in the Target Accounts; they will, however, only seize the items that the Court authorizes to be seized. Similarly, subscribers can conceal their activities by encrypting files. Thus, these files may need to be decrypted to detect whether it constitutes an Item to be Seized.

25. I also believe that people engaged in crimes such as the one described herein often use online accounts because they give people engaged in these crimes a way to easily communicate with other co-conspirators. Moreover, online accounts are easily concealed from law enforcement. Unlike physical documents, electronic documents can be stored in a physical place far away, where they are less likely to be discovered.

26. Service providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) 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 the account (such as logging into the account via websites controlled by the Service Provider), and other log files that reflect usage of the account. In addition, service providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the online account.

27. In some cases, subscribers will communicate directly with a service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from or about other users. Service providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

28. In my training and experience, evidence of who was using an online account may be found in address books, contact or buddy lists, emails in the account, and pictures and files, whether stored as attachments or in the suite of the service provider's online applications. Therefore, the computers of the Service Providers are likely to contain stored electronic communications (including retrieved and un-retrieved email for their subscribers) and information concerning subscribers and their use of the provider's services, such as account access information, email transaction information, documents, pictures, and account application information.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

29. Your Affiant anticipates executing these warrants 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 Microsoft to disclose to the government copies of the records and other information (including the content of communications) 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."

CONCLUSION

30. Based on the forgoing, I request that the Court issue the proposed search warrant. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, 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). Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

REQUEST FOR SEALING

31. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully Submitted,

Ryan S. Burke, Special Agent
Federal Bureau of Investigation

SWORN TO AND SUBSCRIBED
before me this 6th day of October 2017.

UNITED STATES MAGISTRATE JUDGE

ATTACHMENT "A1"

ONLINE ACCOUNT TO BE SEARCHED

1. This warrant applies to information associated with the Microsoft email account centralpark1@live.com (the "Target Accounts") from their inception to present, which is stored at premises owned, maintained, controlled, or operated by Microsoft Corporation, headquartered at 1 Microsoft Way, Redmond, Washington, 98052.

ATTACHMENT "A2"

ONLINE ACCOUNT TO BE SEARCHED

1. This warrant applies to information associated with the Microsoft email account marilouroses@live.com (the "Target Accounts") from their inception to present, which is stored at premises owned, maintained, controlled, or operated by Microsoft Corporation, headquartered at 1 Microsoft Way, Redmond, Washington, 98052.

ATTACHMENT "B"
Particular Things to be Seized

I. **Information to be disclosed by the Service Provider**

To the extent that the information described in Attachment A1 and A2 is within the possession, custody, or control of Microsoft, including any Emails, records, files, logs, or information that have been deleted but are still available to Service Provider, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Service Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A1 and A2 from account inception to present:

a. The contents of all emails associated with the account, including copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
c. All records or other information stored in the Online Accounts, including address books, contact and buddy lists, calendar data, pictures, applications, documents, and other files;
d. All records pertaining to communications between Service Provider and any person regarding the account, including contacts with support services and records of actions taken.
e. All third-party application data and content associated with the Target Account through any Android operating system and/or any Microsoft-related facility.

II. **Information to be seized by the United States**

After reviewing all information described in Section I, the United States will seize evidence of violations of Title 18, United States Code Sections 32(a) (Destruction/Damage of Aircraft or Aircraft Facilities); 37(a)(2) (Violence at International Airport); and 922(a)(3); and 5 (Unlawful Interstate Transport/Delivery of Firearms by Non Federal Firearms Licensee); and 2 (Aiding and Abetting) (the "Subject Offenses") that occur in the form of the following, from account inception to present:

a. Communications, transactions and records that may establish ownership and control (or the degree thereof) of the Target Account, including address books, contact or buddy lists, bills, invoices, receipts, registration records, bills, correspondence, notes, records, memoranda, telephone/address books, photographs, video recordings, audio recordings, lists of names, records of payment for access to newsgroups or other online subscription services, and attachments to said communications, transactions and records.

b. Communications, transactions and records to/from persons who may be co-conspirators of the Subject Offenses, or which may identify co-conspirators.

c. Communications, transactions and records which may show motivation to commit the Subject Offenses.

d. Communications, transactions and records that relate to the Subject Offenses.

e. The terms "communications," "transactions", "records," "documents," "programs," or "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, paintings), photographic form (including, but not limited to, pictures or videos), or electrical, electronic or magnetic form, as well as digital data files. These terms also include any applications (i.e. software programs). These terms expressly include, among other things, Emails, instant messages, chat logs, correspondence attached as to Emails (or drafts), calendar entries, buddy lists.

ATTACHMENT "C"

PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED PURSUANT TO THIS SEARCH WARRANT

1. In executing this warrant, the government must make reasonable efforts to use methods and procedures that will locate and expose in the electronic data produced in response to this search warrant ("the Search Warrant Data") those categories of data, files, documents, or other electronically stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.

2. When the Search Warrant Data is received, the government will make a duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The original version of the Search Warrant Data will be sealed and preserved for purposes of: later judicial review or order to return or dispose of the Search Warrant Data; production to the defense in any criminal case if authorized by statute, rule, or the Constitution; for purposes of showing the chain of custody of the Search Warrant Data and the Search Warrant Data Copy; or for any other lawful purpose. The original of the Search Warrant Data will not be searched or examined except to ensure that it has been fully and completely replicated in the Search Warrant Data Copy.

3. The investigating agents will then search the entirety of the Search Warrant Data Copy using any and all methods and procedures deemed appropriate by the United States designed to identify the information listed as Information to be Seized in Attachment B, Section II. The United States may copy, extract or otherwise segregate information or data listed as Information to be Seized in Attachment B, Section II. Information or data so copied, extracted or otherwise segregated will no longer be subject to any handling restrictions that might be set out in this protocol beyond those required by binding law. To the extent evidence of crimes not within the scope of this warrant appear in plain view during this review, a supplemental or "piggyback" warrant will be applied for in order to further search that document, data, or other item.

4. Once the Search Warrant Data Copy has been thoroughly and completely examined for any document, data, or other items identified in Attachment B, Section II as Information to be Seized, the Search Warrant Data Copy will be sealed and not subject to any further search or examination unless authorized by another search warrant or other appropriate court order. The Search Warrant Data Copy will be held and preserved for the same purposes identified above in Paragraph 2.

5. The search procedures utilized for this review are at the sole discretion of the investigating and prosecuting authorities, and may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. examination of all of the data contained in the Search Warrant Data to view the data and determine whether that data falls within the items to be seized as set forth herein;

b. searching for and attempting to recover from the Search Warrant Data any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. surveying various file directories and the individual files they contain;

d. opening files in order to determine their contents;

e. using hash values to narrow the scope of what may be found. Hash values are under- inclusive, but are still a helpful tool;

f. scanning storage areas;

g. performing keyword searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment A1 and A2; and/or

h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B, Section II.

Return and Review Procedures

6. Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant part:

(e) Issuing the Warrant.

(2) Contents of the Warrant.

(A) Warrant to Search for and Seize a Person or Property. Except for a tracking-device warrant, the warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to:

(i) execute the warrant within a specified time no longer than 14 days;

(B) Warrant Seeking Electronically Stored Information. A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or

copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.

(f) Executing and Returning the Warrant.

(1) Warrant to Search for and Seize a Person or Property.

(B) Inventory. An officer present during the execution of the warrant must prepare and verify an inventory of any property seized. . . . In a case involving the seizure of electronic storage media or the seizure or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied. The officer may retain a copy of the electronically stored information that was seized or copied.

7. Pursuant to this Rule, the government understands and will act in accordance with the following:

a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution of the warrant, an agent is required to file an inventory return with the Court, that is, to file an itemized list of the property seized. Execution of the warrant begins when the United States serves the warrant on the named custodian; execution is complete when the custodian provides all Search Warrant Data to the United States. Within fourteen (14) days of completion of the execution of the warrant, the inventory will be filed.

b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within which the electronically stored information must be seized after the issuance of the warrant and copied after the execution of the warrant, not the "later review of the media or information" seized, or the later off-site digital copying of that media.

c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court may be limited to a description of the "physical storage media" into which the Search Warrant Data that was seized was placed, not an itemization of the information or data stored on the "physical storage media" into which the Search Warrant Data was placed;

d. Under Rule 41(f)(1)(B), the government may retain a copy of that information for purposes of the investigation. The government proposes that the original storage media on which the Search Warrant Data was placed plus a full image copy of the seized Search Warrant Data be retained by the government.

e. If the person from whom any Search Warrant Data was seized requests the return of any information in the Search Warrant Data that is not set forth in Attachment B, Section II, that information will be copied onto appropriate media and returned to the person from whom the information was seized.