



U.S. Department of Justice

Criminal Division

Office of Enforcement Operations

Washington, D.C. 20530

VIA Electronic Mail

October 19, 2020

Jonathan Manes, Esq.
Roderick & Solange MacArthur Justice Center
160 E. Grand Ave., Sixth Floor
Chicago, IL 60611
jonathan.manes@law.northwestern.edu

Request No. CRM-300680988
Privacy International et al. v. Federal
Bureau of Investigation, et al., 18-cv-1488
(W.D.N.Y.)

Dear Mr. Manes:

This is the eleventh installment of the Criminal Division's rolling production regarding your Freedom of Information Act request dated September 10, 2018, for certain records pertaining to "computer network exploitation" or "network investigative techniques." Your request is currently in litigation, Privacy International, et al. v. Federal Bureau of Investigation, et al., 18-cv-1488 (W.D.N.Y.). You should refer to this case number in any future correspondence with this Office. This request is being processed in accordance with the interpretation and parameters set forth by defendants in the July 12, 2019, letter to you from Senior Trial Counsel Marcia Sowles, as well as subsequent conversations regarding the Criminal Division's processing of the request.

Please be advised that a search has been conducted in the appropriate sections, and we are continuing to review and process potentially responsive records. After carefully reviewing 691 pages of records, I have determined that ninety-three (93) pages are responsive to your request: fifty-two (52) pages are appropriate for release in full, copies of which are enclosed. Additionally, forty-one (41) pages are exempt from disclosure pursuant to:

5 U.S.C. § 552(b)(5), which concerns certain inter- and intra-agency communications protected by the deliberative process privilege and the attorney work-product privilege;

5 U.S.C. § 552(b)(6), which concerns material the release of which would constitute a clearly unwarranted invasion of the personal privacy of third parties; and

5 U.S.C. § 552(b)(7)(C), which concerns records or information compiled for law enforcement purposes the release of which could reasonably be expected to constitute an unwarranted invasion of the personal privacy of third parties.

Contained within the records described in this production letter are records that were referred to this Office by the Federal Bureau of Investigation: ten pages of records that contain Bates Stamp Nos. 1378-1387 are being released in full as part of this production; two pages of records (Bates Stamp Nos. 1376-1377) are exempt pursuant to 5 U.S.C. § 552(b)(5), which

concerns certain inter- and intra-agency communications protected by the deliberative process privilege and the attorney work-product privilege.

For your information, Congress excluded three discrete categories of law enforcement and national security records from the requirements of the FOIA. See 5 U.S.C. § 552(c). This response is limited to those records that are subject to the requirements of the FOIA. This is a standard notification that is given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist.

You may contact Senior Trial Counsel Marcia K. Sowles by phone at (202) 514-4960, by email at Marcia.Sowles@usdoj.gov, or by mail at the Civil Division, Federal Programs Branch, 1100 L Street, N.W., Room 10028, Washington, D.C. 20005, for any further assistance and to discuss any aspect of your request.

Although I am aware that your request is the subject of ongoing litigation and that appeals are not ordinarily acted on in such situations, I am required by statute and regulation to inform you of your right to an administrative appeal of this determination. If you are not satisfied with my response to this request, you may administratively appeal by writing to the Director, Office of Information Policy (OIP), United States Department of Justice, 441 G Street, NW, 6th Floor, Washington, D.C. 20530, or you may submit an appeal through OIP's FOIA STAR portal by creating an account on the following website: <https://foiastar.doj.gov>. Your appeal must be postmarked or electronically transmitted within 90 days of the date of my response to your request. If you submit your appeal by mail, both the letter and the envelope should be clearly marked "Freedom of Information Act Appeal."

Sincerely,



Amanda Marchand Jones
Chief
FOIA/PA Unit

cc: Marcia K. Sowles
Senior Trial Counsel
Civil Division, Federal Programs Branch
1100 L Street, N.W., Room 11028
Washington, D.C. 20005
Marcia.Sowles@usdoj.gov

Michael S. Cerrone
michael.cerrone@usdoj.gov

Enclosures

AFFIDAVIT OF [NAME]
IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, [name], being first duly sworn, hereby depose and state as follows:

A. Introduction and Affiant Background

1. I make this affidavit in support of an application for a search warrant to use a network investigative technique (“NIT”). I request approval to send one or more communications to [address]. Each such communication is designed to cause the computer receiving it to transmit data that will help identify the computer, its location, other information about the computer, and the user of the computer. As set forth herein, there is probable cause to believe that violations of Section [crime] of Title 18, United States Code ([crime]) have occurred and that evidence of those violations exists on the computer that receives the NIT described above.

2. [agent background]

3. [USE ALL THAT APPLY] - The facts set forth in this affidavit are based on my personal knowledge, knowledge obtained during my participation in this investigation from other individuals, including other law enforcement officers, my review of documents and computer records related to this investigation, communications with others who have personal knowledge of the events and circumstances described herein, and information gained through my training and experience.] Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation.

B. Probable Cause

4. [explain why probable cause exists to believe that a NIT sent to the address will reveal evidence, such as how the computer expected to receive the NIT was used in the commission of a crime or how identifying the computer or account user is evidence of who committed the crime under investigation.]

C. Place to be Searched and Property to be Seized

5. If a computer successfully activates the NIT, the NIT will conduct a one-time limited search of that computer. The NIT utilizes computer instructions to cause an activating computer to send certain information to a computer controlled by the [server owner, typically the investigating agency].

6. The NIT is designed to collect the items described in Attachment B – *i.e.*, information that may assist in identifying the computer, its location, other information about the computer, and the user of the computer, all of which is evidence of violations of Section [crime] of Title 18, United States Code ([crime]). This information may include the portion of the activating computer that contains environmental variables and/or certain registry-type information, such as:

A. The computer's IP address. An IP Address is a unique numeric address used to direct information over the Internet and is written as a series of four numbers, each in the range 0 – 255, separated by periods (e.g., 121.56.97.178). Conceptually, IP addresses are similar to telephone numbers in that they are used to identify computers that send and receive information over the Internet.

- B. The computer's MAC address. Each time a computer communicates over a local area network (or "LAN"), it uses a hardware device called a network interface card. Manufacturers of network interface cards assign each one a unique numeric identifier called a media access control or "MAC address."
- C. The computer's open communication ports. A communication port number is information that helps computers to associate a communication with a particular program or software process running on a computer efficiently. For example, if a communication is sent to port 80, the receiving computer will generally associate it with world wide web traffic and send it to the web server, which can then send back a web page to the requesting computer.
- D. A list of running programs running on the computer.
- E. The type of operating system running on the computer, including type (e.g., Windows), version (e.g., Vista), and serial number.
- F. The web browser and version running on the computer. The web browser is the program that allows user to view web pages. Firefox, Internet Explorer, Netscape, Opera and Safari are examples of web browsers.
- G. The computer's language encoding and default language. Users can set computers to display text in a particular language.
- H. The computer's time zone information.

- I. The registered computer name and registered company name. Users generally input this information when the computer is first purchased.
- J. The current logged-in user name and list of user accounts.
- K. The computer's wired and wireless network connection information, dial-up account information, and trace-route information. This information identifies the way that the computer is connected to the Internet.
- L. Uniform Resource Locator ("URL") to which the target computer was previously connected. URLs, such as www.uscourts.gov, are used to access web sites.
- M. Other similar information on the activating computer that may assist in identifying the computer, its location, other information about the computer, and the user of the computer may also be accessed by the NIT.

7. Each of these categories of information sought by the NIT may contain evidence of the crime under investigation, including information that may help to identify the computer receiving the NIT and its user. The computer's true assigned IP address can be associated with an Internet service provider ("ISP") and a particular ISP customer. The MAC address is unique to a specific computer on a network. A list of open communication ports and running programs can corroborate whether the NIT is reading the correct computer by showing whether that computer is using the world wide web, sending and receiving emails, or reading attachments. The operating system and browser types and versions can also corroborate the identity of a computer and, in the case of an

operating system's serial number, can provide evidence to identify the user because corporations maintain databases of purchasers of their operating systems. The language encoding and computer default language can help identify the subject by identifying his native spoken language. The computer name, company name, logged-in user name can identify the network, specific computer on a network, and perhaps even the name of the person(s) who use the computer. Traceroute information can help identify where on a network or even where physically a computer may be located. Wireless network connection information can tell from where a computer accessed the Internet, even if it was through the unauthorized use of a wireless network (a technique used by Internet criminals). Wired network information and dial-up account information can help identify what computer was used to access the Internet to receive the NIT. Time zone information will assist in confirming the geographical location of the subject computer. The last-visited URL can sometimes help corroborate the identity of the computer and user by, for example, showing that the NIT ran after the user visited the web-based e-mail server for the target email address.

8. Based on my training, experience, and the investigation described herein, I know that network level messages and information gathered directly from a sending computer can be more effective than other types of information in identifying a computer, its location and individual(s) using a computer. For instance, individual(s) using the Internet can use compromised computers or commercial services to conceal their true originating IP address and thereby intentionally inhibit their identification. Getting IP address and other information directly from the computer being used by the subject can defeat such techniques.

9. The NIT will cause the above-described information to be sent over the Internet to a computer controlled by [server owner, typically the investigating agency] located in [jurisdiction] [and then relayed to investigators in this District].

10. Based upon the information above, I have probable cause to believe that the computer that receives the NIT is [an instrumentality and contains evidence] of violations of Title 18, United States Code, Section [crime]. I further submit that there is probable cause to believe that using a NIT in conjunction with the target address will assist in identifying the activating computer, its location and the individual(s) using the activating computer to commit these violations of the United States Code. By this affidavit and application, I request that the Court issue a search warrant authorizing the use of the NIT described herein.

11. **[[USE THIS PARAGRAPH IF USING A PUBLICLY AVAILABLE TOOL THAT ALLOWS FOR ONGOING MONITORING OF IP ADDRESSES]]** After the one-time search, the NIT will record routing, addressing and signaling information for electronic communications originating from the activating computer for 30 days. More specifically, the NIT may report the following types of information: IP address, MAC address, open communication ports, trace-route information, wireless network connection information, wired network connection information, dates, and times of the electronic communications, but not the contents of such communications. For a period of thirty days the NIT will forward that data to a computer controlled by the [server owner, typically the investigating agency.] Such information is relevant and material to the government's ongoing criminal investigation.

12. **[[USE THIS PARAGRAPH IF USING A PUBLICLY AVAILABLE TOOL THAT ALLOWS FOR ONGOING MONITORING OF IP ADDRESSES]]**

The routing, addressing and signaling information described in the preceding paragraph will help show the ordinary things that a pen register on the user's Internet connection would reveal, that is, with what Internet sites the user communicates. Such information can help reveal the user's techniques, interests, and associations, and thereby may assist in attributing to a particular person the use of the computer receiving the NIT. The routing and addressing information to be collected will show where and when the computer(s) access the Internet over that period, if it changes. Once the government knows the IP addresses from which it accesses the Internet, the government will be better able to determine the physical location of those IP addresses by using publicly available data or grand jury subpoenas. **[additional grounds]**.

13. **[[USE THIS PARAGRAPH IF USING A PUBLICLY AVAILABLE TOOL THAT ALLOWS FOR ONGOING MONITORING OF IP ADDRESSES]]**A

separate application for the installation and use of a pen register and trap and trace device is also being sought for the use of the NIT.

14. Because notice as required by Rule 41(f)(3) of the Federal Rules of Criminal Procedure would jeopardize the success of the investigation, and because the investigation has not identified an appropriate person to whom such notice can be given, I hereby request authorization to delay such notice for 30 days from the sending of the NIT.

15. Because there are legitimate law enforcement interests that justify an unannounced use of the NIT and review of the messages generated by the activating

computer in this case, I ask this Court to authorize the proposed use of a NIT without the prior announcement of its use. One of these legitimate law enforcement interests is that announcing the use of the NIT would assist a person using the activating computer to defeat the activation of the NIT.

16. Rule 41(e)(2) of the Federal Rules of Criminal Procedure requires that the warrant command the law enforcement officer (a) “to execute the warrant within a specified time no longer than 10 days” and (b) to “execute the warrant during the daytime unless the judge for good cause expressly authorizes execution at another time” The government seeks permission to deploy the NIT at any time of day or night within 10 days of the date the warrant is authorized. There is good cause to allow such a method of execution as the time of deployment causes no additional intrusiveness or inconvenience to anyone. The government also seeks to read any messages generated by the activating computer as a result of a NIT at any time of day or night during the execution of the warrant. This is because the individuals using the activating computer may activate the NIT after 10:00 PM or before 6:00 AM and law enforcement would seek to read the information it receives as soon as it is aware of the NIT response.

17. The government does not currently know the exact configuration of the computer that may be used to access the target address. Variations in configuration, e.g., different operating systems, may require the government to send the target address more than one communication in order to get the NIT to activate properly. Accordingly, I request that this Court authorize the government to continue to send communications to the target address for up to 10 days after this warrant is authorized, until the NIT has returned the information authorized to be collected by this warrant.

18. To the extent that use of a NIT to obtain the information described herein can be characterized as a seizure of an electronic communication or electronic information under 18 U.S.C. § 3103a(b)(2), such a seizure is reasonably necessary for the reasons described herein.

19. Accordingly, it is respectfully requested that this Court issue a search warrant authorizing the following:

- A. the use of multiple communications until the NIT has returned the information authorized to be collected by this warrant, without prior announcement, within 10 days from the date this Court issues the requested warrant;
- B. the NIT may cause an activating computer – wherever located – to send to the government in [location], [and thereafter to the government in this District,] network level messages containing information that may assist in identifying the computer, its location, other information about the computer and the user of the computer;
- C. that the government may receive and read, at any time of day or night, within 10 days from the date the Court authorizes of use of the NIT, the information that the NIT causes to be sent to the computer controlled by the [server owner, typically the investigating agency];
- D. **[[USE THIS PARAGRAPH IF USING A PUBLICLY AVAILABLE TOOL THAT ALLOWS FOR ONGOING MONITORING OF IP ADDRESSES]]** that once the government has received an initial NIT response from the activating computer, the

government may for 30 days thereafter collect dialing, routing addressing, and signaling information that can be collected pursuant to a pen register and trap and trace device order; and

E. that, pursuant to 18 U.S.C. § 3103a(b)(3), to satisfy the notification requirement of Rule 41(f)(3) of the Federal Rules of Criminal Procedure, the government may delay providing a copy of the search warrant and the receipt for any property taken for thirty (30) days from the sending of the NIT [or, in the case of a NIT with ongoing monitoring, 30 days after the termination of the pen/trap order] unless notification is further delayed by court order.

F. that provision of a copy of the search warrant and receipt may, in addition to any other methods allowed by law, be effectuated by electronic delivery of true and accurate electronic copies (e.g., Adobe PDF file) of the fully executed documents in the same manner as the NIT is delivered.

20. I further request that this Application and the related documents be filed under seal. The information to be obtained is relevant to an on-going criminal investigation. Premature disclosure of this Application and related materials may jeopardize the success of the above-described investigation. Further, this affidavit describes a law enforcement technique in sufficient detail that disclosure of the technique could assist others in thwarting its use in the future. Accordingly, I request that the affidavit remain under seal until further order of the Court.

WHEREFORE, Affiant respectfully requests that a warrant described above be issued.

[affiant]

Subscribed and sworn to me before me
this _____ day of _____, _____

HON. [judge]
U.S. Magistrate Judge

Attachment A

Place to Be Searched

The portion of the computer activating the NIT that may assist in identifying the computer, its location, other information about the computer, and the user of the computer.

Attachment B

Things To Be Seized

Information that may assist in identifying the computer, its location, other information about the computer, and the user of the computer, all of which is evidence of violations of Section [crime] of Title 18, United States Code ([crime]).

Attachment C

IT IS ORDERED that the government is authorized to use multiple communications until the NIT has returned the information authorized to be collected by this warrant, without prior announcement, within 10 days from the date this Court issues the requested warrant;

IT IS ORDERED that the NIT may cause an activating computer – wherever located – to send to the government in [location], [and thereafter to the government in this District,] network level messages containing information that may assist in identifying the computer, its location, other information about the computer and the user of the computer;

[[USE THIS PARAGRAPH IF USING A PUBLICLY AVAILABLE TOOL THAT ALLOWS FOR ONGOING MONITORING OF IP ADDRESSES]] IT IS ORDERED that once the government has received an initial NIT response from the activating computer, the government may for 30 days thereafter collect dialing, routing addressing, and signaling information that can be collected pursuant to a pen register and trap and trace device order; and

IT IS ORDERED that provision of a copy of the search warrant and receipt may, in addition to any other methods allowed by law, be effectuated by electronic delivery of true and accurate electronic copies (e.g., Adobe PDF file) of the fully executed documents in the same manner as the NIT is delivered.

UNITED STATES DISTRICT COURT

for the District of Colorado

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

Case No.

Network Investigative Technique ("NIT") for email address texas.slayer@yahoo.com

12-sw-05685-KMT

APPLICATION FOR A SEARCH WARRANT

I, Craig W. Roegner, 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", which is attached to and incorporated in this Application, Affidavit and Attachment C

located in the State and District of Colorado, there is now concealed (identify the person or describe the property to be seized):

SEE "ATTACHMENT B", which is attached to and incorporated in this Application, Affidavit and Attachment C

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.

The search is related to a violation of:

Title 18 U.S.C. § 1038 False Information and Hoaxes related to Terrorism and Crimes of Violence

The application is based on these facts:

- Continued on the attached affidavit, which is incorporated by reference. Delayed notice until the arrest of the suspect (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.

s/ Craig W. Roegner Applicant's signature

Craig W. Roegner, Special Agent, (ATF) Printed name and title

Sworn to before me and signed in my presence.

Date: Oct 09, 2012 4:14 pm

Kathleen M. Tafoya Judge's signature

Kathleen M. Tafoya United States Magistrate Judge

City and state: Denver, Colorado

Printed name and title

Attachment A

Place to Be Searched

The portion of the computer activating the network investigative technique (“NIT”) that may assist in identifying the computer, its location, other information about the computer, and the user of the computer.

Attachment B

Things To Be Seized

Information that may assist in identifying the computer, its location, other information about the computer, and the user of the computer, all of which is evidence of violations of Section 1038 of Title 18, United States Code (False information and hoaxes). This information may include environmental variables and/or certain registry-type information, such as:

A. The computer's IP address. An IP Address is a unique numeric address used to direct information over the Internet and is written as a series of four numbers, each in the range 0 - 255, separated by periods (e.g., 121.56.97.178).

Conceptually, IP addresses are similar to telephone numbers in that they are used to identify computers that send and receive information over the Internet.

B. The computer's MAC address. Each time a computer communicates over a local area network (or "LAN"), it uses a hardware device called a network interface card. Manufacturers of network interface cards assign each one a unique numeric identifier called a media access control or "MAC address."

C. The computer's open communication ports. A communication port number is information that helps computers to associate a communication with a particular program or software process running on a computer efficiently. For example, if a communication is sent to port 80, the receiving computer will generally associate it with world wide web traffic and send it to the web server, which can then send back a web page to the requesting computer.

D. A list of programs running on the computer.

E. The type of operating system running on the computer, including type (e.g., Windows), version (e.g., Vista), and serial number.

F. The web browser and version running on the computer. The web browser is the program that allows user to view web pages. Firefox, Internet Explorer, Netscape, Opera and Safari are examples of web browsers.

G. The computer's language encoding and default language. Users can set computers to display text in a particular language.

H. The computer's time zone information.

I. The registered computer name and registered company name. Users generally input this information when the computer is first purchased.

J. The current logged-in user name and list of user accounts.

K. The computer's wired and wireless network connection information, dial-up account information, and trace-route information. This information identifies the way that the computer is connected to the Internet.

L. The Uniform Resource Locator ("URL") to which the target computer was previously connected. URLs, such as www.uscourts.gov, are used to access web sites.

M. Other similar identifying information on the activating computer that may assist in identifying the computer, its location, other information about the computer, and the user of the computer may be accessed by the NIT.

AFFIDAVIT OF CRAIG W. ROEGNER
IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Craig W. Roegner, being first duly sworn, hereby depose and state as follows:

A. Introduction and Affiant Background

1. I make this affidavit in support of an application for a search warrant to use a network investigative technique (“NIT”). I request approval to send one or more communications to texas.slayer@yahoo.com. Each such communication is designed to cause the computer receiving it to transmit data that will help identify the computer, its location, other information about the computer, and the user of the computer. As set forth herein, there is probable cause to believe that violations of Section 1038 of Title 18, United States Code (False information and hoaxes) have occurred and that evidence of those violations exists on the computer that receives the NIT described above.

2. I have been employed as a Special Agent (SA) for the U. S. Department of Justice, Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) since May 1999. I am currently assigned as a Task Force Officer (TFO) for the Federal Bureau of Investigation (FBI), Joint Terrorism Task Force, National Security, Squad One (NS-1) in Denver, Colorado. Prior to being employed as a Special Agent, I earned a Bachelor’s degree in Criminal Justice from Old Dominion University in Norfolk, Virginia, and earned a Master’s degree in Public Affairs specializing in Justice Administration from the American University in Washington, DC. I am a graduate of the Federal Law Enforcement Training Center and the ATF National Academy. Prior to being employed by the ATF, I was employed as a law enforcement officer for the Arlington County, Virginia, Police Department. As a Special Agent and Task Force Officer, I am authorized

to carry firearms, execute warrants, and make arrests for offenses against the United States and to perform other duties as authorized by law. My primary duties as a FBI TFO involve the investigation of domestic terrorism and Federal firearm and explosive violations and their associated use in violent crimes. During the course of my law enforcement career, I have participated in numerous criminal investigations which resulted with the arrest of individuals armed with firearms and explosives, or explosive materials. During these criminal investigations, I have written affidavits for, executed, or assisted in the execution of numerous state and federal arrest and search warrants for, firearms, explosives, records, books, documents, and proceeds derived as a result of illicit criminal activity. I have also testified concerning the techniques employed by armed and unarmed individuals during the course of their criminal activity, which they use to conceal their identities, firearms, documents, burglary tools, contraband, and their assets.

3. The facts set forth in this affidavit are based your Affiant's personal knowledge, knowledge obtained during my participation in this investigation from other individuals, including other law enforcement officers, my review of documents, police reports, electronic communications, and computer records related to this investigation, communications with others who have personal knowledge of the events and circumstances described herein, and information gained through my training and experience and other sources of information relative to terroristic threats and bomb threat types of investigations. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation.

B. Probable Cause

4. On 07/22/12, the Arapahoe County Sheriff's Office located at 13101 E. Broncos Parkway in the City of Centennial, County of Arapahoe State of Colorado, received a phone call from a male who identified himself as "Andrew Ryan". The caller spoke in an accent, stated he was a friend of James Holmes and he wanted Holmes released from custody. If Holmes was not released he, Andrew Ryan, would blow up building with Ammonium Nitrate and kill people. It was determined that the phone number Andrew Ryan was calling from was (760) 705-8888. At about 5:15 P.M., Arapahoe County Sheriff's Office Deputy Michael Agos was connected by telephone to Andrew Ryan and an approximate three hour dialog ensued between Andrew Ryan and Deputy Agos. Deputy Agos explained that Andrew Ryan spoke with an accent and the "Voice Over Internet" phone connection was poor. Because of this, Andrew Ryan answered Deputy Agos' questions through e-mail account soozanvf@gmail.com. During the three hours of dialog Andrew Ryan spoke with Deputy Agos over the phone, but mostly communicated his thoughts via the e-mail connection. Deputy Agos advised that there is no doubt in his mind that the person he was talking to on the phone was the same person communicating with him via soozanvf@gmail.com. The dialog between Deputy Agos and Andrew Ryan concluded when Andrew Ryan stated he would meet Deputy Agos in ten minutes at an agreed upon location. Andrew Ryan never arrived as agreed.

5. On 07/23/12 at about 12:58 P.M., Deputy Agos received an e-mail from

soozanvf@gmail.com and a dialog ensued. The person using the listed e-mail account advised he was Andrew Ryan and that he was sorry for not meeting Deputy Agos as agreed. The dialog with Andrew Ryan continued for several hours as attempts were made to identify and locate Andrew Ryan. During the dialog Andrew Ryan made renewed threats that he wanted James Holmes released, and that he would blow up building and kill people to achieve that desire. Efforts to locate and or identify Andrew Ryan failed and the dialog eventually concluded.

6. On 07/24/12 at about 3:30 P.M., Investigator Isaacson was contacted by a member of the Arapahoe County Sheriff's Office Dispatch who advised Andrew Ryan called from phone number (760) 705-8888 and was asking to speak to Deputy Agos. Arapahoe County Sheriff's Office Investigator Bruce Isaacson instructed that the phone call be transferred to him. Several moments later, Inv. Isaacson's phone rang and a male caller speaking with a strong accent identified himself as Andrew Ryan. This Affiant spoke to Andrew Ryan for some time and during that conversation, Andrew Ryan stated he had ten pounds of Ammonium Nitrate, numerous conspirators, guns and they were going to blow up a section of the Arapahoe County Jail and free James Holmes. Andrew Ryan explained that he has a spy within the Arapahoe County Jail as well as "snipers" who will kill anyone who tries to stop the escape. When asked what would happen when he was confronted by armed deputies in the jail, Andrew Ryan said he and his associates would shoot and kill the deputies. The conversation was ended by Inv. Isaacson when Andrew Ryan said he was also going to kill random people until James Holmes was released and the deaths would be

the responsibility of Inv. Isaacson. It should be noted that Inv. Isaacson sent Andrew Ryan an e-mail message to e-mail address soozanvf@gmail.com at 4:20 P.M. and Andrew Ryan responded verbally to this Inv. Isaacson reference the e-mail message.

7. On 07/24/12 at approximately about 6:00 P.M., the Denver Police / Sheriff's Department received a phone call from a male caller who spoke with an accent who identified himself as Andrew Ryan and demanded the immediate release of James Holmes. When told that Holmes would not be released Andrew Ryan stated he had Ammonium Nitrate and he would blow up the jail and he had people that would help him. Andrew Ryan reiterated that he had the weapons needed and the explosives to free Holmes from custody. The caller ID listed the phone number from which Andrew Ryan was calling was (760) 705-8888 and the call lasted for 32 minutes. The Denver jail was locked down due to the bomb threat and a search of the perimeter with the assistance of a bomb detection trained dog was completed with no devices located nor any detonation.
8. On 07/25/12, Investigator Isaacson received six phone calls from the telephone number (760) 705-8888. Inv. Isaacson was only able to answer two of the phone calls and both times Isaacson recognized the caller as the male subject who identifies himself as Andrew Ryan. Apparently because Inv. Isaacson was unable to answer the afternoon phone calls from Andrew Ryan, he called the Arapahoe County Sheriff's Office Dispatch, identified himself as Andrew Ryan and asked to talk to Deputy Agos. Dispatch identified the originating number as (760) 705-8888 and then

connected Andrew Ryan's phone call to Investigations Sgt. Bruce Peterson who had been previously briefed on Andrew Ryan. While speaking with Sgt. Peterson, Andrew Ryan stated that he or his associates had shot and killed three people at the Cherry Creek Reservoir and the bodies are in the water at the reservoir. Cherry Creek Reservoir is located within the Cherry Creek State Park at 4201 South Parker Road in unincorporated Arapahoe County. Deputy Sheriff's from the Arapahoe County Sheriff's Office were provided with this information and searched for victims but none were found.

9. On 07/30/12 at about 5:07 P.M., the Greenwood Village Police Department received information of a bomb threat at the Doubletree hotel. The Doubletree hotel is located at 7801 East Orchard Road in the city of Greenwood Village, County of Arapahoe, State of Colorado. Police Officer Rodney Valenzuela was dispatched to the front counter of the hotel as the person making the bomb threat was still on the phone talking to an employee of the Doubletree Hotel. Upon arrival Officer Valenzuela was given a telephone and advised that the person calling in the bomb threat was on the phone. Officer Valenzuela identified himself to the caller as "Rodney" and the caller, a male who spoke with an accent, identified himself as "Andrew Ryan." Andrew Ryan stated he planted ten Ammonium Nitrate bombs in the hotel because he wants James Holmes released. Andrew Ryan also stated that he would blow up the hotel and that people that ran out would be shot and that there was only five more minutes until the bombs exploded. During the conversation with Andrew Ryan Officer Valenzuela distinctly heard another voice in the background advising Andrew Ryan

how many bombs were in the building and how much time remained before the bombs exploded. The entire hotel was evacuated, searched visually and with a bomb detection trained dog from the Jefferson County Sheriff’s Office. No bombs were found nor detonated.

10. The Greenwood Village Police Department advised Inv. Isaacson, who responded to the Doubletree hotel to provide known information on Andrew Ryan, that the phone call by Andrew Ryan originated at phone number (877) 573-9800. It was determined that the listed phone number is also a “Voice Over Internet” server phone number. The Greenwood Police Department submitted an “Emergency Disclosure Request” to Google Inc. reference soozanvf@gmail.com. The following information was then provided to the Greenwood Village Police Department by Google Inc. and then forwarded to this Affiant:

“Google Subscriber Information
 Name: Soozan vf
 e-Mail: soozanvf@gmail.com
 Statue: Enabled
 Services: Docs, Feedburner, Gmail, Google ply, Personalized homepage, Pp 2012, Search history, Spreadsheets, Talk, Toolbar, Tranliteration, Voice, Webmaster tools, Youtube
 Created on: 2009/04/14 15:21:44-UTC
 IP: 177.198.98.149, on 2009/04/14 15:21:44-UTC
 Language Code: en
 SMS: 09365099706

Date/Time	Event	IP
2012/07/20 21:56:00-UTC	Login	199.255.210.87
2012/07/20 21:31:41-UTC	Login	74.115.0.36
2012/07/20 21:30:56-UTC	Logout	74.115.0.36
2012/07/20 21:25:44-UTC	Login	74.115.0.36”

11. Your Affiant was advised by FBI Special Agent Josh Britton that the phone number (760) 705-8888 is a main line used by Google. Inc for server access and does not service any single subscriber. Also your Affiant was advised that the threaten call was a “Voice Over Internet” telephone connection and that a “proxy server” was being used which blocks access to the IP address used. The proxy server being used appeared to be “Anchor Free Proxy.”

12. On 07/31/2012 at approximately 10:36 AM, a party identifying himself as “Andrew Ryan” called the Denver International Airport call center. The suspect stated that he and several of his friends had planted 20 bombs at the airport. Your affiant requested and reviewed the audio tapes of the bomb threat. The suspect has a distinct accent and repeated several times that he and his friends had planted bombs in the baggage area and on planes. The suspect stated that he wanted his friend James Holmes (Aurora Theater shooting suspect) released. The caller identification shows the call was made from 760-705-8888. This number is a Google Voice G-Mail standard telephone number assigned to the G-mail voice system.

13. On 08/02/2012 your affiant attended a meeting at the Aurora Police Department regarding numerous bomb threats that had been made throughout the Denver Metro area. Denver Police Sgt. Mike Reichardt# P95007 advised that the suspect had called Denver Police Department, District Three Police Station on 07/20/2012. On 07/02/2012, Sgt. Reichardt responded to the District Three clerk’s desk upon

being informed of a bomb threat caller who was still on the telephone. Sgt. Reichardt spoke to the suspect who was demanding the release of Aurora shooting suspect James Holmes. If “Holmes” was not release the caller would “blow up hundreds of people”. The telephone number on the call back showed (760) 705-8888 which is consistent with the Google talk application. The suspect then requested that Sgt Reichardt give him an e-mail address to further their conversation. Sgt. Reichardt provided the suspect with an old personal G-mail account address. The suspect then sent several communications from a Google G-mail account “soozanvf@gmail.com”. Sgt. Reichardt relayed the above information in a written communication to Detective Kurt Peterson of the Denver Police Department Bomb Squad. As a result, Detective Kurt Peterson was the affiant for a State of Colorado, Denver County, Search Warrant that was issued to Google, Inc., 1600 Amphitheatre Parkway, Mountain View, California 94043 for any and all information kept, maintained or logged in association with email address/account: soozanvf@gmail.com.

14. Since on or about 08/02/2012, Denver Police Sgt. Mike Reichardt has been communicating via email with soozanvf@gmail.com. Then on 08/14/2012, Sgt. Mike Reichardt spoke to the person he was emailing at soozanvf@gmail.com, who had previously identified himself as “Andrew Ryan”. Sgt. Reichardt and “Andrew Ryan” talked face to face (peer to peer) on a Yahoo Messenger video chat system. During the conversation, the subject admitted to calling bomb threats to the Denver International Airport, the Double Tree Hotel in Greenwood Village, Colorado and the San Antonio Airport in San Antonio, Texas.

15. On 08/14/2012, at approximately 1550 hours the Aurora jail was contacted by a caller who identified himself as “Alex Anderson” and threatened to place ammonium nitrate bombs around the city if James Holmes was not released. The caller said that he also had a .223 caliber rifle and the call came from (760) 705-8888.

16. On or about 09/09/2012, Andrew Ryan via email from email address soozanvf@gmail.com provided Sgt. Reichardt via email multiple photographs of himself. The photographs included the same olive skinned male, medium, muscular build, in his late 20’s, with black hair that appeared to be depicted in the Yahoo Messenger video chat on 08/14/2012. The first picture showed the unidentified male in an Iranian tan camouflaged military uniform. The next picture showed the same unidentified male in a white t-shirt with the “-975” visible on the front, and another photograph with the same unidentified male in a white collared

polo type shirt. During these communications the caller claiming to be “Andrew Ryan” asked Sgt. Reichardt to call him “Mo” which was short for “Mohammed”.

17. On 09/12/2012, at approximately 8:30PM, Denver International Airport Communication Center received a bomb threat to United Flight 6318. According to the caller, who identified himself as “Jason”, there was a chemical bomb composed of ammonium nitrate and that the bomb was in a checked bag on the aircraft. The bomb was set to detonate upon the aircraft’s arrival at Fargo International Airport (FAR) located in Fargo, North Dakota. The caller claimed that he was affiliated with “Al Qaeda” and he is working with ten other people. The group had planted the bomb and was going to blow up the aircraft because they were angry with the U. S. A. and the U. S. Army’s actions. The caller ID for the call was (760) 705-8888.

18. On or about 09/16/2012, Mohammed contacted Sgt. Reichardt via telephone. Mohammed claimed that he called in the bomb threats at the University of Texas in Austin, TX and at North Dakota State University on or about 09/14/2012. Mohammed informed Sgt. Reichardt that his Gmail email account soozanvf@gmail.com had been disabled by Google and that he would start using the Yahoo email account Texas.Slayer@yahoo.com for future conversations.

19. On or about 09/17/2012, the results of the State of Colorado Search Warrant for Google, Inc. in Mountain View, California for any and all information kept,

maintained or logged in association with email address/account:

soozanvf@gmail.com. The following information was ascertained from an analysis of the information provided by Google regarding soozanvf@gmail.com:

- Username: mmmmmaaaaffff
- Email Address: soozanvf@gmail.com
- External ID: 10171uCTC0zpCXdYtNvHRg
- URL: <http://www.youtube.com/user/mmmmmaaaaffff>
- Signup Date: may 5, 2009, 12:04AM (Pacific Time)
- Signup IP: 85.198.16.152
- Name: Not Provided
- Country: Iran
- Date of Birth: 1985-05-04, Age: 27

20. On 09/22/12 at about 3:47 P.M. a male caller, believed to be Andrew Ryan because he called from the telephone number (760) 705-8888, called the Arapahoe County Sheriff's Office Detention Facility that is located at 7573 S. Potomac Street in the City of Centennial, County of Arapahoe, State of Colorado and spoke to Helen Groves. The caller stated that he needed to speak to James Holmes and if he was not allowed to speak to Mr. Holmes he, the caller, would kill more people. Ultimately the request was denied and the caller became angry and said, Do you want me to do what my friend did..." "Like killing people in a public place like a movie theater, amusement park, what the hell I am really mad right now."

21. On 09/23/12 at about 3:30 P.M. the Arapahoe County Sheriff's Office dispatch received a phone call from phone number (760) 705-8888. The caller identified himself as Andrew Ryan and asked to speak to Mike Agos, Bruce Isaacson or Bruce Peterson, by name; who are all employees of the Arapahoe County Sheriff's Office who have spoken to Andrew Ryan in the past. When told by Lt. Chris George that the only person he would be talking to is him, Andrew Ryan said that he was tired of everything and wanted to commit mass murder and end it with his suicide. Andrew Ryan also admitted to murdering Henry Roberts last night and dumped the body in "Jason Park" which is in the city of Englewood, Colorado.

22. On 09/25/2012, Sgt. Reichardt received multiple emails from texas.slayer@yahoo.com. In these emails, Mohammed acknowledged that he is the one that recently called in the bomb threats at Denver University in Denver, Colorado on 09/24/2012. In addition, Mohammed provided Sgt. Reichardt an email copy of a letter "my_first-letter.txt" file where Mohammed claimed that he is 20 years old and that he is the individual who "who hav been threatening the airports and some other pulblic (sic.) places too." The letter was signed "your (sic) truly MO".

23. Since on or about 07/22/2012 to the present, more than 12 significant public and/or private locations throughout the United States have received telephonic and/or email communications where serious bodily injury and/or the destruction of public and/or private property was threatened. The results of these threats were eventually determined to be hoaxes. On or about 09/26/2012, Sgt. Reichardt received an email from texas.slayer@yahoo.com, where “Mohammed” identifies himself as “Mohammed Arian Far” with a date of birth “5-24-92” and claimed responsibility for false bomb threats made to the San Antonio International Airport; the Austin International Airport; Aeroflot Flight 103 from JFK International Airport bound for Moscow; Washington-Dallas International Airport, Baton Rouge International Airport, North Dakota International Airport, Double Tree Hotel in Englewood, Colorado; University of Texas Austin; North Dakota State University; the Virginia Commonwealth University; and the Denver University.

24. Based on the facts, probable cause exists to believe that a NIT sent to the texas.slayer@yahoo.com will reveal evidence, such as how the computer expected to receive the NIT was used in the commission of a crime or how identifying the computer or account user is evidence of who committed the crime under investigation.

C. Place to be Searched and Property to be Seized

25. If a computer successfully activates the NIT, the NIT will conduct a one-time limited search of that computer. The NIT utilizes computer instructions to cause an activating computer to send certain information to a computer controlled by the Federal Bureau of Investigation (“FBI”), which will assist the FBI Denver JTTF NS-1 in the forensic aspects of this investigation.

26. Specifically, the NIT is designed to collect the items described in Attachment B i.e., information that may assist in identifying the computer, its location, other information about the computer, and the user of the computer, all of which is evidence of violations of Section 1038 of Title 18, United States Code (False information and hoaxes). This information may include the portion of the activating computer that contains environmental variables and/or certain registry-type information, such as:

A. The computer’s IP address (Internet Protocol Address). An IP Address is a unique numeric address used to direct information over the Internet and is written as a series of four groups of numbers, each in the range 0 255, separated by periods (e.g., 121.56.97.178). Conceptually, IP addresses are similar to telephone numbers in that they are used to identify computers that send and receive information over the Internet.

B. The computer’s MAC address. Each time a computer communicates over a local area network (or “LAN”), it uses a hardware device called a network interface card (“NIC”). Manufacturers of NICs assign each one a unique numeric identifier called a media access control or “MAC address.”

C. The computer's open communication ports. A communication port number is information that helps computers to associate a communication with a particular program or software process running on a computer efficiently. For example, if a communication is sent to port 80, the receiving computer will generally associate it with world wide web traffic and send it to the web server, which can then send back a web page to the requesting computer.

D. A list of programs running on the computer.

E. The type of operating system running on the computer, including type (e.g., Windows), version (e.g., Vista), and serial number.

F. The web browser and version running on the computer. The web browser is the program that allows computer users to view web pages. Firefox, Internet Explorer, Netscape, Opera, and Safari are examples of web browsers.

G. The computer's language encoding and default language. Users can set computers to display text in a particular language.

H. The computer's time zone information.

I. The registered computer name and registered company name. Users generally input this information when the computer is first purchased.

J. The current logged-in user name and list of user accounts.

K. The computer's wired and wireless network connection information, dial-up account information, and trace-route information. This information identifies the way that the computer is connected to the Internet.

L. The Uniform Resource Locator (“URL”) to which the target computer was previously connected. URLs, such as www.uscourts.gov, are used to access web sites.

M. Other similar identifying information on the activating computer that may assist in identifying the computer, its location, other information about the computer, and the user of the computer may be accessed by the NIT.

27. Each of these categories of information sought by the NIT may constitute and/or contain evidence of the crimes under investigation, including information that may help to identify the computer receiving the NIT and its user. The computer’s true assigned IP address can be associated with an Internet service provider (“ISP”) and a particular ISP customer. The MAC address is unique to a specific computer on a network. A list of open communication ports and running programs can corroborate whether the NIT is reading the correct computer by showing whether that computer is using the world wide web, sending and receiving emails, or reading attachments. The operating system and browser types and versions can also corroborate the identity of a computer and, in the case of an operating system’s serial number, can provide evidence to identify the user because corporations maintain databases of purchasers of their operating systems. The language encoding and computer default language can help identify the subject by identifying his native spoken language. The computer name, company name, and logged-in user name can identify the network, specific computer on a network, and perhaps even the name of the person(s) who use the computer. Trace-route

information can help identify where on a network or even where physically a computer may be located. Wireless network connection information can tell from where a computer accessed the Internet, even if it was through the unauthorized use of a wireless network (a technique used by Internet criminals). Wired network information and dial-up account information can help identify what computer was used to access the Internet to receive the NIT. Time zone information will assist in confirming the geographical location of the subject computer. The last-visited URL can sometimes help corroborate the identity of the computer and user by, for example, showing that the NIT ran after the user logged into the SG online client account access portion of DLA in order to view the fraudulent account information over the internet.

28. Based on my training, experience, my consultation with forensic computer experts, and the investigation described herein, I know that network level messages and information gathered directly from a sending computer can be more effective than other types of information in identifying a computer, its location and individual(s) using a computer. For instance, individual(s) using the Internet can use compromised computers or commercial services to conceal their true originating IP address and thereby intentionally inhibit their identification. For example, as mentioned earlier, the subject accessing the texas.slayer@yahoo.com email account used the services of an Internet company, to mask the IP address from which they are logging on to the fraudulently created texas.slayer@yahoo.com account. Getting IP address and other information directly from the computer

being used by the subject can defeat such techniques. The NIT will cause the above-described information to be sent over the Internet to a computer controlled by the FBI, located in Quantico, Virginia, in the Eastern District of Virginia, and then be relayed to the investigators in the District of Colorado who will analyze the resulting information.

29. Based upon the information above, I have probable cause to believe that any computer seeking to access the texas.slayer@yahoo.com email account, to make threatening statements and bomb threats which will receive the NIT, is an instrumentality, and contains evidence, violations of Section 1038 of Title 18, United States Code (False information and hoaxes). I further submit that there is probable cause to believe that using a NIT in conjunction with the Target Addresses will assist in identifying the activating computer, its location, and the individual(s) using the activating computer to commit and facilitate these violations of the United States Code. By this affidavit and application, I request that the Court issue a search warrant authorizing the use of the NIT described herein.

D. Delayed Notification Request

30. Because notice as required by Rule 41(f)(3) of the Federal Rules of Criminal Procedure would jeopardize the success of the investigation, and because the investigation has not identified an appropriate person to whom such notice can be given, I hereby request authorization to delay such notice until the time that a suspect has been identified and has been placed in custody. Because there are

legitimate law enforcement interests that justify an unannounced use of the NIT and review of the messages generated by the activating computer. I ask this Court to authorize the proposed use of a NIT without the prior announcement of its use. One of these legitimate interests is that announcing the use of the NIT would assist a person using the activating computer to defeat the activation of the NIT.

E. Time and Manner of Execution of the Search

31. Rule 41(e)(2) of the Federal Rules of Criminal Procedure requires that the warrant command the law enforcement officer (a) “to execute the warrant within a specified time no longer than 30 days” and (b) to “execute the warrant during the daytime unless the judge for good cause expressly authorizes execution at another time” The government seeks permission to deploy the NIT at any time of day or night within 30 days of the date the warrant is authorized or within 30 days from the time the texas.slayer@yahoo.com account is accessed. There is good cause to allow such a method of execution as the time of deployment causes no additional intrusiveness or inconvenience to anyone. More specifically, the government has no control of the timing or when the subject(s) will access the texas.slayer@yahoo.com account whereby triggering the NIT warrant to be executed. The government also seeks to read any messages generated by the activating computer as a result of a NIT at any time of day or night during the execution of the warrant. This is because the individuals using the activating computer may activate the NIT after 10:00 PM or before 6:00 AM and law

enforcement would seek to read the information it receives as soon as it is aware of the NIT response.

32. The account belonging to texas.slayer@yahoo.com is sporadically accessed. In order to get the NIT to activate properly. Accordingly, I request that this Court authorize the government to preserve the Internet web link within the texas.slayer@yahoo.com login script for up to 30 days after this warrant is authorized or until the NIT has returned the information authorized to be collected by this warrant.

33. To the extent that use of a NIT to obtain the information described herein can be characterized as a seizure of an electronic communication or electronic information under 18 U.S.C. § 3103a(b)(2), such a seizure is reasonably necessary for the reasons described herein.

34. Accordingly, for each of the aforementioned reasons, it is respectfully requested that this Court issue a search warrant authorizing the following:

A. the use of an Internet based web link added to the login script of the account belonging to texas.slayer@yahoo.com executing on the Target Computers until the NIT has returned the information authorized to be collected by this warrant, without prior announcement, within 30 days from the date this Court issues the requested warrant or until 30 days after the subject triggers the NIT warrant to be executed;

B. the NIT may cause an activating computer wherever located to send to the FBI, located in Quantico, Virginia, in the Eastern District of Virginia, and then be relayed to the investigators in the District of Colorado, network level messages containing information that may assist in identifying the computer, its location, other information about the computer and the user of the computer;

C. that the government may receive and read, at any time of day or night, within 30 days from the date the Court authorizes the use of the NIT or until 30 days after the subject triggers the NIT warrant to be executed, the information that the NIT causes to be sent to the computer controlled by the FBI;

D. that, pursuant to 18 U.S.C. § 3103a(b)(3), to satisfy the notification requirement of Rule 41(f)(3) of the Federal Rules of Criminal Procedure, the government may delay providing a copy of the search warrant and the receipt for any property taken until the time that a suspect has been identified and has been placed in custody from the sending of the NIT unless notification is further delayed by the court; and

E. that provision of a copy of the search warrant and receipt may, in addition to any other methods allowed by law, be effectuated by electronic delivery of true and accurate electronic copies (e.g., Adobe PDF file) of the fully executed documents in the same manner as the NIT is delivered.

35. I further request that this application and the related documents be filed under seal.

The information to be obtained is relevant to an ongoing criminal investigation. Premature disclosure of this application and related materials may jeopardize the success of the above-described investigation. Further, this affidavit describes a

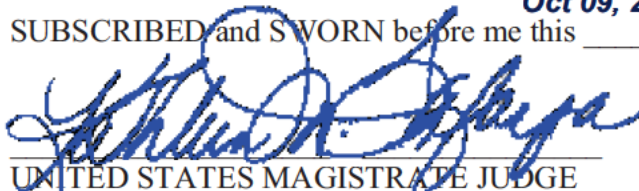
law enforcement technique in sufficient detail that disclosure of the technique could assist others in thwarting its use in the future. Accordingly, I request that the affidavit remain under seal until further order of the Court.

36. WHEREFORE, Affiant respectfully requests that a warrant described above be issued.

FURTHER AFFIANT SAYETH NOT.

s/ Craig W. Roegner
Craig W. Roegner
Special Agent
ATF/FBI TFO

SUBSCRIBED and SWORN before me this 09 day of October, 2012 **Oct 09, 2012 4:14 pm**



UNITED STATES MAGISTRATE JUDGE

Kathleen M. Tafoya
United States Magistrate Judge

Application for search warrant was reviewed and is submitted by Gregory Holloway, Assistant United States Attorney.

Attachment C

IT IS ORDERED that the government is authorized to add a Internet web link until the network investigative technique (“NIT”) has returned the information authorized to be collected by this warrant, without prior announcement, within 14 days from the date this Court issues the requested warrant or until 14 days after the NIT warrant was successfully executed;

IT IS ORDERED that the NIT may cause an activating computer wherever located to send to the government, specifically the Federal Bureau of Investigation, located in Quantico, Virginia, in the Eastern District of Virginia, network level messages containing information that may assist FBI Denver, NS-1 investigations in the District of Colorado in identifying the computer, its location, other information about the computer and the user of the computer; and

IT IS ORDERED that provision of a copy of the search warrant and receipt may, in addition to any other methods allowed by law, be effectuated by electronic delivery of true and accurate electronic copies (e.g., Adobe PDF file) of the fully executed documents in the same manner as the NIT is delivered.

AFFIDAVIT OF [NAME]
IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, [name], being first duly sworn, hereby depose and state as follows:

A. Introduction and Affiant Background

1. I make this affidavit in support of an application for a search warrant to use a network investigative technique (“NIT”). I request approval to send one or more communications to [address]. Each such communication is designed to cause the computer receiving it to transmit data that will help identify the computer, its location, other information about the computer, and the user of the computer. As set forth herein, there is probable cause to believe that violations of Section [crime] of Title 18, United States Code ([crime]) have occurred and that evidence of those violations exists on the computer that receives the NIT described above.

2. [agent background]

3. [USE ALL THAT APPLY - The facts set forth in this affidavit are based on my personal knowledge, knowledge obtained during my participation in this investigation from other individuals, including other law enforcement officers, my review of documents and computer records related to this investigation, communications with others who have personal knowledge of the events and circumstances described herein, and information gained through my training and experience.] Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation.

B. Probable Cause

4. [explain why probable cause exists to believe that a NIT sent to the address will reveal evidence, such as how the computer expected to receive the NIT was used in the commission of a crime or how identifying the computer or account user is evidence of who committed the crime under investigation.]

C. Place to be Searched and Property to be Seized

5. If a computer successfully activates the NIT, the NIT will conduct a one-time limited search of that computer. The NIT utilizes internet protocols to cause an activating computer to send certain information to a server connected to the internet but controlled by the FBI.

6. The NIT is designed to collect the computer's IP address. An IP Address is a unique numeric address used to direct information over the Internet and is written as a series of four numbers, each in the range 0 – 255, separated by periods (e.g., 121.56.97.178). Conceptually, IP addresses are similar to telephone numbers in that they are used to identify computers that send and receive information over the Internet.

7. The NIT will be delivered through a Hypertext Markup Language (HTML) file that will be saved as a Microsoft Word document. When the document is opened on an internet connected computer instructions within the document direct the activating computer to connect to the FBI controlled server. The communications with the FBI controlled server result in the server capturing the originating IP Address from the activating computer. The computer's true assigned IP address can be associated with an Internet service provider ("ISP") and a particular ISP customer.

8. Based on my training, experience, and the investigation described herein, I know that network level messages and information gathered directly from a sending

computer can be more effective than other types of information in identifying a computer, its location and individual(s) using a computer. For instance, individual(s) using the Internet can use compromised computers or commercial services to conceal their true originating IP address and thereby intentionally inhibit their identification. Getting IP address and other information directly from the computer being used by the subject can defeat such techniques.

9. The NIT will cause the above-described information to be sent over the Internet to a computer controlled by the FBI located in [jurisdiction] [and then relayed to investigators in this District].

10. Based upon the information above, I have probable cause to believe that the computer that receives the NIT is [an instrumentality and contains evidence] of violations of Title 18, United States Code, Section [crime]. I further submit that there is probable cause to believe that using a NIT in conjunction with the target address will assist in identifying the activating computer, its location and the individual(s) using the activating computer to commit these violations of the United States Code. By this affidavit and application, I request that the Court issue a search warrant authorizing the use of the NIT described herein.

11. Because notice as required by Rule 41(f)(3) of the Federal Rules of Criminal Procedure would jeopardize the success of the investigation, and because the investigation has not identified an appropriate person to whom such notice can be given, I hereby request authorization to delay such notice for 30 days from the sending of the NIT.

12. Because there are legitimate law enforcement interests that justify an unannounced use of the NIT and review of the messages generated by the activating computer in this case, I ask this Court to authorize the proposed use of a NIT without the prior announcement of its use. One of these legitimate law enforcement interests is that announcing the use of the NIT would assist a person using the activating computer to defeat the activation of the NIT.

13. Rule 41(e)(2) of the Federal Rules of Criminal Procedure requires that the warrant command the law enforcement officer (a) “to execute the warrant within a specified time no longer than 14 days” and (b) to “execute the warrant during the daytime unless the judge for good cause expressly authorizes execution at another time” The government seeks permission to deploy the NIT at any time of day or night within 14 days of the date the warrant is authorized. There is good cause to allow such a method of execution as the time of deployment causes no additional intrusiveness or inconvenience to anyone. The government also seeks to read any messages generated by the activating computer as a result of a NIT at any time of day or night during the execution of the warrant. This is because the individuals using the activating computer may activate the NIT after 10:00 PM or before 6:00 AM and law enforcement would seek to read the information it receives as soon as it is aware of the NIT response.

14. The government does not currently know the exact configuration of the computer that may be used to access the NIT. Variations in configuration, e.g., different operating systems, may require the government to send the target address more than one communication in order to get the NIT to activate properly. Accordingly, I request that this Court authorize the government to continue to send communications to the target

address for up to 14 days after this warrant is authorized, until the NIT has returned the information authorized to be collected by this warrant.

15. To the extent that use of a NIT to obtain the information described herein can be characterized as a seizure of an electronic communication or electronic information under 18 U.S.C. § 3103a(b)(2), such a seizure is reasonably necessary for the reasons described herein.

16. Accordingly, it is respectfully requested that this Court issue a search warrant authorizing the following:

- A. the use of multiple communications until the NIT has returned the information authorized to be collected by this warrant, without prior announcement, within 14 days from the date this Court issues the requested warrant;
- B. the NIT may cause an activating computer wherever located to send to the government in [location], [and thereafter to the government in this District,] network level messages containing information that may assist in identifying the computer;
- C. that the government may receive and read, at any time of day or night, within 14 days from the date the Court authorizes of use of the NIT, the information that the NIT causes to be sent to the computer controlled by the [server owner, typically the investigating agency];
- D. that, pursuant to 18 U.S.C. § 3103a(b)(3), to satisfy the notification requirement of Rule 41(f)(3) of the Federal Rules of Criminal Procedure, the government may delay providing a copy of the search

warrant and the receipt for any property taken for thirty (30) days from the sending of the NIT unless notification is further delayed by court order.

- E. that provision of a copy of the search warrant and receipt may, in addition to any other methods allowed by law, be effectuated by electronic delivery of true and accurate electronic copies (e.g., Adobe PDF file) of the fully executed documents in the same manner as the NIT is delivered.

17. I further request that this Application and the related documents be filed under seal. The information to be obtained is relevant to an on-going criminal investigation. Premature disclosure of this Application and related materials may jeopardize the success of the above-described investigation. Further, this affidavit describes a law enforcement technique in sufficient detail that disclosure of the technique could assist others in thwarting its use in the future. Accordingly, I request that the affidavit remain under seal until further order of the Court.

WHEREFORE, Affiant respectfully requests that a warrant described above be issued.

[affiant]

Subscribed and sworn to me before me
this day of ,

HON. [judge]
U.S. Magistrate Judge

Attachment A

Place to Be Searched

The portion of the computer activating the NIT that may assist in identifying the computer, its location, other information about the computer, and the user of the computer.

Attachment B

Things To Be Seized

Information that may assist in identifying the computer and its location, which is evidence of violations of Section [crime] of Title 18, United States Code ([crime]).

Attachment C

IT IS ORDERED that the government is authorized to use multiple communications until the NIT has returned the information authorized to be collected by this warrant, without prior announcement, within 10 days from the date this Court issues the requested warrant;

IT IS ORDERED that the NIT may cause an activating computer wherever located to send to the government in [location], [and thereafter to the government in this District,] network level messages containing information that may assist in identifying the computer and its location;

IT IS ORDERED that provision of a copy of the search warrant and receipt may, in addition to any other methods allowed by law, be effectuated by electronic delivery of true and accurate electronic copies (e.g., Adobe PDF file) of the fully executed documents in the same manner as the NIT is delivered.