UNITED STATES DISTRICT COURT

for the

DISTRICT OF OREGON

Portland Division

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

Vehicles as described in Attachment A

Case No. '14-MC-301-C

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

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

as described in Attachment A which is attached hereto and incorporated herein by this reference.

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:
The information and items set forth in Attachment B which is attached hereto and incorporated herein by this reference.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before August 14, 2014
(not to exceed 14 days)

☑ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

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

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

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

Date and time issued: July 31, 2014 @ 3:54 p.m.

Judge's signature

City and state: Portland, Oregon

John V. Acosta, U.S. Magistrate Judge
Printed name and title

AO 93 (Rev. 12/09) **OREGON VERSION (Rev. 4/10)** Search and Seizure Warrant (Page 2)

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
2660-PO-5300220	Aug 6, 2014 0830	Cody M Rushel

Inventory made in the presence of :

John Sorensen

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

No Items taken

Certification

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

8/15/2014
Date

Executing officer's signature

SA Peter Summers
Printed name and title

Subscribed, sworn to, and returned before me this date.

8/15/14
Date

Judge's signature

ATTACHMENT A

PLACE TO BE SEARCHED

SUBJECT 1- The person of Greg Michael Reynolds, white male, date of birth 08/17/1973

SUBJECT PREMISES 1 – located at 35612 SE Macinnes Road, Corbett Oregon, 97019, and is the residence of Greg Michael Reynolds.

Appears to be a single-floor home, which abuts a small hill. The residence is located at the end of a declined driveway, and has a brown exterior. Maroon canopies provide sun covering over the main entry door, and some of the windows facing the driveway. The front door is reached by stairs which lead from the driveway area to what appears to be a wooden deck.

SUBJECT VEHICLE 1 - a 2004 Ford Ranger, Oregon license plate number CA21276, and vehicle identifications number 1FTZR45E85PA21069. Located at SUBJECT PREMISES 1.

SUBJECT VEHICLE 2 – a 2002 Chevy Astro van, Oregon license plate number K7ZZY, and vehicle identification number 1GNEL19XX2B122592. Located at SUBJECT PREMISES 1.

ATTACHMENT B

Items to be Searched For, Seized, and Examined

The following records, documents, and items that constitute evidence, contraband, fruits and/or instrumentalities of violation of 18 USC § 875 (c), Interstate communications.

a) Documents to include notices, bills, letters, and written communications ;

b) Any handgun or firearm ammunition, written documents relating to firearms, cleaning kits, holsters, targets, spent cartridges, gun cases or safes;

c) Cellular telephones to include smart phones;

d) Computers, laptops, and electronic media storage devices;

e) Usernames or passwords pertaining to computer access, electronic mail accounts greynolds@portlandstate.org, greynolds73@gmail.com, reynoldsvs.psu@gmail.com, and cellular telephones related thereto.

f) Contact lists or documents associated with Portland State University.

UNITED STATES DISTRICT COURT

for the

District of Oregon

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Vehicles as described in Attachment A

Case No. '14-MC-301-C

APPLICATION FOR A SEARCH WARRANT

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

as described in Attachment A which is attached hereto and incorporated herein by this reference.

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

The information and items set forth in Attachment B which is attached hereto and incorporated herein by this reference.

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:

Code Section	*Offense Description*
Title 18 U.S.C 875 (c)	Interstate Communication

The application is based on these facts:
See affidavit which is attached hereto and incorporated herein by this reference.

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

Applicant's signature

Special Agent Peter Summers
Printed name and title

Sworn to before me and signed in my presence.

Date: July 31, 2014 @ 3:55 p.m.

Judge's signature

City and state: Portland, Oregon

John V. Acosta, United States Magistrate Judge
Printed name and title

STATE OF OREGON)
) ss. AFFIDAVIT OF
County of Multnomah) Peter Summers

I, Peter Summers, being first duly sworn, do hereby depose and say:

1. I am a Special Agent (SA) of the Federal Bureau of Investigation (FBI) and have been so employed for approximately three years. I am trained in investigating a wide variety of violations of federal criminal law. I am currently assigned to and work on the Joint Terrorism Task Force (JTTF).

2. I have been a Special Agent for three years. I am currently assigned to the FBI's Portland office. I am authorized, and presently assigned, to investigate Domestic Terrorism, specifically anti-government extremists, and crimes related to these groups. I am currently investigating a violation of Title 18, United States Code, Section 875(c) Interstate Communications (commonly known as threatening communications). I have received training in Domestic Terrorism, the laws, investigations and violations pertaining to Domestic Terrorism at the FBI's Counterterrorism Investigations and Operations course located at Manassas, Virginia.

3. I have also acquired knowledge and information about the groups, organizations, motivations and various means and methods: formal and informal training, other law enforcement officers and investigators, informants, persons whom I have arrested and/or interviewed, and my participation in numerous other investigations.

4. I know the following statute provides for criminal violation:

- 18 U.S.C. § 875(c) Interstate Communications, makes it unlawful for any person to:

  (c) Transmit in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another.

5. This affidavit is made in support of a search warrant for the premises, including the dwelling, outbuildings, curtilage, and vehicles thereon, located at 35612 SE Macinnes Road, Corbett, Oregon 97019, as well as the person and vehicles of Greg Michael Reynolds. This warrant is being sought in connection with an investigation relating to violation of federal laws governing interstate communications by Greg Michael Reynolds in the Judicial District of Oregon.

HISTORY OF SUBJECTS INVOLVED

6. Greg Michael Reynolds, date of birth 08/17/1973, is a convicted felon. I have reviewed documents showing that Greg Michael Reynolds was convicted of the following felony, punishable by more than one year in prison:

- Delivery of Controlled substance (Schedule I) to a Minor, in violation of Ore.Rev.Stat. § 475.995, on or about February 15, 1994, in Jackson County, Circuit Court, case number 1093110439.

It appears that, pursuant to Ore.Rev.Stat. § 166.270(4)(a) and the age of the conviction, Reynolds may legally possess firearms in Oregon.

7. Oregon Department of Motor Vehicles records show that Greg Michael Reynolds has an Oregon State Driver's License, number 4836765, listing 35612 SE Macinnes Rd, Corbett, Oregon, as his current residence. Moreover, I have attempted to interview REYNOLDS once at the address 35612 SE Macinnes Rd, Corbett, Oregon, most recently on July 24, 2014. My partner Special Agent Jake Green had previously interviewed REYNOLDS, Both times REYNOLDS was present at the address. During both visits it was evident REYNOLDS resided at the address.

RELEVANT FACTS

8. The following information, facts, and occurrences are the result of my personal knowledge and investigation, my conversations with other law enforcement officers, and from my review of their reports relative to this investigation.

9. On April 9, 2014, Cody Michael Kuschel was interviewed. KUSCHEL stated he has been in an intimate relationship with REYNOLDS for three years. The two of them live together at REYNOLDS' residence located at 3516 SE Macinnes Rd, Corbett, Oregon. KUSCHEL stated that REYNOLDS told him that there is a Glock firearm in the house (aforementioned address in Corbett) and that the firearm is locked in a key/combination lock box. Kuschel stated he never personally saw the Glock in the house but was told by REYNOLDS where it was kept.

10. On July 21, 2014, at approximately 6:33 a.m. an email was sent from **reynoldsvs.psu@gmail.com** to balzerj@pdx.edu, an email account assigned to Jackie Balzer, the former Vice President for Enrollment Management & Student Affairs at Portland State University. The email was also sent to specific employees of Portland State University, news organizations, and others. The verbatim email content is as follows (with misspellings in original):

> Dear Jackie:
>
> Now that you have violated my constitutional and civil rights and the Multnomah County DA's office, the US Department of Education, Governor John Kitzhabers office, the entire US Senate and the entire PSU Board of Trustees have authorized me to shoot you with a Glock 17 9mm are you prepared to accept your fate as you have without due

process have forced to me accept mine? I have done nothing to anyone that PSU did not, in violation of the law do to me first. I am simply upholding PSU's Code of Conduct.

I am prepared deliver your sentence as also accepted by the Circuit Courts of the State of Oregon, Multnomah County.

Have a nice day. I look forward to seeing you soon.

Greg Reynolds

11. On July 18, 2014, at approximately 6:50 a.m., an email was sent from both **reynolds@portlandstate.org** and **greynolds73@gmail.com** (known email addresses used repeatedly by Greg Michael Reynolds) to nancy.cozine@opds.state.or.us, an email account assigned to Nancy Cozine, the Executive Director for the Oregon State Public Defender's office. The email was also sent to specific employees of Portland State University, news organizations, and others. The verbatim email content is as follows (with misspellings in original):

Dear Nancy Cozine and the Oregon Public Defenders Office:

Now that you are a witness to the fact the the laws of this nation and the Constitution do no apply to me, you must understand that in lieu of due process Portland State University has determined I am "permenently and irreversibly" expelled from all rights and obligations under all state and federal laws. This has been confirmed along with my right to shoot those in the face with a Glok 17 9mm for violating my rights and denial of due process. This may include you per the Portland State University record and all board of trustees members, our great dictator Osama Bin Kitzhaber, the Oregon Department of Justice (Chrystal M. Bader), the US Department of Education, the Multnomah County DA's office (Kristen Snowden), the Oregon Appellate Clerks office, each and every

member of the US Senate, the Office of the President, Mutnomah County Sheriff Dan Stanton, the ACLU Oregon, Project Respond, Disability Rights Oregon Gregory Kaufory, Dominic Thomas, Michelle Toppe and Earl Blumenauer.

In lieu of due process I have been authorized to take further actions as necessary.

Sincerely

Greg M. Reynolds

12. On July 23, 2014, at approximately 7:55 a.m., an email was sent from **reynolds@portlandstate.org** and **greynolds73@gmail.com** to an account assigned to Dominic Thomas, Director of Student Conduct, and an email account assigned to Michelle Toppe, Dean of Student Life, both at Portland State University. The email was also sent to specific employees of Portland State University, news organizations, and others. The email content is as follows (with misspellings in original):

Date: Wed, 23 Jul 2014 07:55:22 -0700

Subject:

Dear Dominic Thomas and Michelle Toppe:

Since I have been authorized by the US Senate, Governor, Board of Trustees, Multnomah County DA (Kristen Snowden), and the Oregon Department of Justice (Chrystal M. Bader) to shoot you with a Glock 17 9mm for violating my Constitutional and Civil Rights, you should ask yourselves, are prepared to die today?

In the name of Jesus, Justice and the PSU Code of Conduct. Amen.

Sincerely

Greg M. Reynolds

13. On June 9, 2014, at approximately 6:08 a.m., an email was sent from **reynoldsvs.psu@gmail.com** to whittenc@pdx.edu, an email account assigned to Craig Whitten, a Lieutenant with Portland State University Security. The email was also sent to other people at Portland State University, government and law enforcement organizations. The email verbatim content is as follows :

Dear Craig Whitten, Craig Baker and Chief of Campus Public Safety:

I was tried and convicted by your department. You have violated my constitutional and civil rights without question. As of today that changes forever. As ordered by Jackie Balzer and PSU and has been universally accepted as law by each and every member of the US Senate, the office of the President of the United States, the PSU Board of Trustees, Jim Fransceoni, Commissioner Kaufry, Gregory Kafury, Governor John Kitzhaber, the Oregon Attorney Generals office, the Multnomah County Sheriff's office, the Circuit Courts of the State of Oregon cases 120970073, 140201438, the Social Security Administration, the US Department of Justice, the FBI, Disability Rights Oregon, Congressman Blumenauer case 00504061-74463, Oregon BAR TWJ1400136, as well on the approval of Kristen Snowden Multnomah County DA's office and Chrystal M. Bader with the Oregon Department of Justice hereby affirm that the law does not apply to Greg Reynolds, you are allowed to entrap people and impersonate police officers without consequence and I am fully authorized by the courts as of 15 May 2014, to shoot you in the face with a Glock 17 9mm in defense of the rights your criminal activities have denied me. I have yet to see a day in court as guaranteed by Senator Wyden, but you criminals run free. I intend to defend myself by any means necessary in lieu of application of the law.

This is war.

Sincerely

Greg M. Reynolds

14. Based on the threatening verbage and explicit threats, I have probable cause to believe REYNOLDS has violated 18 U.S.C § 875(c). I know from personal experience and research that email servers, particularly gmail, are located outside the State of Oregon and that email transmissions within Oregon necessarily travel outside the state. On July 24, 2014, writer and Special Agent Jake Green attempted to interview REYNOLDS at his home located at 35612 SE Macinnes Rd, Corbett, Oregon 97019. REYNOLDS declined to be interviewed. About 10 to 15 minutes after writer departed the residence, an email was sent via **reynolds@portlandstate.org** to numerous persons, many of whom have received threats from Reynolds, specifically Dominic Thomas and Michelle Toppe. The verbatim email content is as follows:

> Dear Dominic and Michelle:
>
> The FBI was just here. They tore up my driveway on video as they were leaving because they once again came here without a warrant. You have violated my constitutional and civil rights, the most you can do is lick my pussy. Kind of like how you treated me when you broke the law.
>
> Sincerely
>
> Greg M. Reynolds
>
> Record of this visit was also record by 911 phone call to report the threats made to me at my residence without due process or warrants.

15. On July 30, 2014, writer spoke with Chief of Public Safety at Portland State University (PSU) Phillip Zerzan, who stated, in addition to being expelled, Reynolds was barred for two years from PSU property prior to the emails quoted in this affidavit.

16. On July 29, 2014, a federal grand jury in this District returned a sealed indictment charging REYNOLDS with two counts of interstate threatening communications, in violation of 18 U.S.C. § 875(c), regarding two of the aforementioned threats to Portland State University employees.

17. Based on emails from REYNOLDS claiming to have access to a firearm, specifically a Glock 17, and a named associate stating REYNOLDS claims to have a Glock firearm in his home, I have probable cause to believe Greg Michael Reynolds is in possession of a firearm.

18. Based on my training and experience, I know that firearms and firearms accessories are valuable commodities and are kept for long periods of time. I know from training and experience that it is common practice among persons who possess firearms either legally or illegally for them to secrete the firearms and firearms accessories upon their person, upon the persons of co-conspirators, within their vehicles, within their residence, and within the boundaries of the curtilage of their residences. Secreting of the firearms and firearms accessories outside the residence, but within the boundaries of the residential curtilage, and within their vehicles, is a practice of persons who possess firearms, and is an attempt on their part to prevent the firearms and firearms accessories from being stolen by persons in the criminal community, and to prevent their firearms and firearms accessories from being discovered by law enforcement in the event of the service of a search warrant. I also know from training and experience that it is

common practice among persons who possess firearms, to have several firearms in their possession, and to collect firearms, due to their value.

19. Based on my training and experience, I know that people who have firearms have other various components related to firearms, such as cleaning kits, spare parts for firearms, holsters, ammunition, magazines and other ammunition storage devices, bullets, shell casings, primers, powders, reloading equipment, firearm boxes/cases, lockboxes, trigger locks, scopes, laser sights and other gun-related optics, receipts, memoranda and/or notes pertaining to the acquisition, receipt, purchase, repair or disposition of firearms, books, diagrams, manuals, photographs both in print and on digital media, undeveloped film and videos, and gun safes. These items can be stored on their person, in their vehicle or a vehicle that they are driving, and/or in their residence, outbuildings and curtilage.

20. Based on my training and experience, I know as a law enforcement officer that, during the course of most searches pursuant to a search warrant, items of identification, such as letters, bills, rent receipts, checks, check stubs, driver's licenses, keys, identification cards, miscellaneous documents, paperwork with names and numbers and the like are discovered, and are relevant to the possession, dominion, and control of the vehicle or property where evidence is located, and therefore should be seized as evidence. Additionally, I know from training and experience that firearms purchased legally may wind up being possessed by other persons, and that documentation of this control such as photographs, handwritten notes, videos, and other miscellaneous documents can record this possession, or transfer.

21. Based on my training and experience, I know that people involved in the possession of firearms often use vehicles. I know through training and experience those items of value including firearms and the records of the sale or purchase of the firearms are often kept in

automobiles by persons who possess firearms. Such items are seized regularly from vehicles located at the scene of search warrants.

22. Based on training and experience, I know that people often carry evidence of their own true identity in their vehicles. These items of identification include, but are not limited to, vehicle registration forms, driver's licenses or identification cards, credit card receipts, mail, proof of automobile insurance, and tools engraved or marked with the identifying numbers or names of persons owning a vehicle.

23. Based on training and experience, I know people involved in illegal activity have a need to communicate with other persons in order to facilitate their illegal activity. Equipment frequently used by these individuals includes cell phones and answering machines, and that the information stored in these devices contains items of evidentiary value. This information often includes phone numbers, coded messages, text messages, identification of callers, photographs of co-conspirators, and other related information. I know that subjects who possess firearms often take photos of these firearms and store them in the electronic memories of cell phones

Probable Cause With Respect To Electronic Items to be Seized

24. The seized items fall into the following categories: (1) computers; (2) cell phones, (3) electronic storage media (thumb drives, CDs, storage cards), (4) mail items. With respect to mail and other documents, these are relevant to show dominion and control over the premises where other evidence was found, and may also include communications, records, plans, or other evidence relevant to the crimes.

Probable Cause For Digital Evidence To Be Seized

25. With respect to computers, from his training and experience, SA Summers knows that criminals in general use computers to plan and coordinate activities by creating documents,

communicating via electronic methods such as e mail and by accessing the Internet to communicate and obtain information. SA Summers has reviewed numerous postings and emails to show computer usage. Also, electronic communications such as e-mails are likely to leave evidence of their being sent on the computer. Address books and contact lists are also fruitful sources of evidence, as they commonly reveal names and other information about victims or potential victims. Address books and contact lists are often stored on computers.

26. With respect to cell phones, from his training and experience, SA Summers knows that many cellular telephones especially "smart phones" have the same capability of computers and therefore may contain evidence similar to that of a computer.

27. With respect to the seized digital cameras and media/storage cards from digital cameras, SA Summers knows, from his training and experience that evidence relevant to criminal investigations is commonly found on digital cameras and camera storage cards. Photographs stored on the digital cameras and cards from digital cameras may help to identify the owner's associates and conspirators. The digital cameras and media cards from digital cameras may include photographs of past criminal actions, or evidence of a crime. In this instance REYNOLDS has documented almost 100 hundred images on his personal Facebook account. Some of these images are photographs of emails he has sent to various individuals related to this search warrant.

28. With respect to the seized electronic storage devices such as thumb drives, DVDs, and CDs, SA Summers knows, from his training and experience that a wide variety of evidence may be found on these devices. Data from cell phones, cameras, and other devices can easily be transferred and stored to thumb drives, DVDs, and CDs. Thus, any evidence that one can expect

to find on a cell phone, camera, or other device may also be found stored on thumb drives, DVDs, and CDs.

Search and Seizure of Digital Data

29. This application seeks permission to search for and seize evidence of the crime described above, including evidence of how computers, digital devices, and digital storage media were used, the purpose of their use, and who used them.

30. Based upon my training and experience, and information related to me by agents and others involved in the forensic examination of computers and digital devices, I know that data in digital form can be stored on a variety of systems and storage devices, including hard disk drives, floppy disks, compact disks, magnetic tapes, flash drives, and memory chips. Some of these devices can be smaller than a thumbnail and can take several forms, including thumb drives, secure digital media used in phones and cameras, personal music devices, and similar items.

Removal of Data Storage Devices

31. I know that a forensic image is an exact physical copy of a data storage device. A forensic image captures all data on the subject media without viewing or changing the data in any way. Absent unusual circumstances, it is essential that a forensic image be obtained prior to conducting any search of data for information subject to seizure pursuant to the warrant. I also know that during the search of the premises it is not always possible to create a forensic image of or search digital devices or media for data for a number of reasons, including the following:

32. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. Because there are so many different types of digital devices and software in use today, it is difficult to anticipate all of the necessary technical

manuals, specialized equipment, and specific expertise necessary to conduct a thorough search of the media to ensure that the data will be preserved and evaluated in a useful manner.

33. Searching digital devices can require the use of precise, scientific procedures designed to maintain the integrity of the evidence and to recover latent data not readily apparent to the casual user. The recovery of such data may require the use of special software and procedures, such as those used in a law enforcement laboratory.

34. The volume of data stored on many digital devices is typically so large that it will be highly impractical to search for data during the execution of the physical search of the premises. Storage devices capable of storing 500 gigabytes of data are now commonplace in desktop computers. It can take several hours, or even days, to image a single hard drive. The larger the drive, the longer it takes. Depending upon the number and size of the devices, the length of time that agents must remain onsite to image and examine digital devices can become impractical.

Laboratory Setting May Be Essential For Complete And Accurate Analysis Of Data

35. Since digital data may be vulnerable to inadvertent modification or destruction, a controlled environment, such as a law enforcement laboratory, may be essential to conduct a complete and accurate analysis of the digital devices from which the data will be extracted. Software used in a laboratory setting can often reveal the true nature of data. Therefore, a computer forensic reviewer needs a substantial amount of time to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband, or an instrumentality of a crime.

36. Analyzing the contents of a computer or other electronic storage device, even without significant technical difficulties, can be very challenging, and a variety of search and

analytical methods must be used. For example, searching by keywords, which is a limited text-based search, often yields thousands of hits, each of which must be reviewed in its context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant hit does not end the review process. The computer may have stored information about the data at issue which may not be searchable text, such as: who created it; when and how it was created, downloaded, or copied; when it was last accessed; when it was last modified; when it was last printed; and when it was deleted. The relevance of this kind of data is often contextual. Furthermore, many common email, database, and spreadsheet applications do not store data as searchable text, thereby necessitating additional search procedures. To determine who created, modified, copied, downloaded, transferred, communicated about, deleted, or printed data requires a search of events that occurred on the computer in the time periods surrounding activity regarding the relevant data. Information about which users logged in, whether users shared passwords, whether a computer was connected to other computers or networks, and whether the users accessed or used other programs or services in the relevant time period, can help determine who was sitting at the keyboard.

Latent Data:

a) Searching digital devices can require the use of precise, scientific procedures designed to maintain the integrity of the evidence and to recover latent data. The recovery of such data may require the use of special software and procedures. Data that represents electronic files or remnants of such files can be recovered months or even years after it has been downloaded onto a hard drive, deleted, or viewed via the Internet. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools.

b) Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in space on the hard drive or other storage media that is not allocated to an active file. In addition, a computer's operating system may keep a record of deleted data in a swap or recovery file or in a program specifically designed to restore the computer's settings in the event of a system failure.

Contextual Data:

a) In some instances, the computer "writes" to storage media without the specific knowledge or permission of the user. Generally, data or files that have been received via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to such data or files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve artifacts of electronic activity from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer usage.

b) Logs of access to websites, file management/transfer programs, firewall permissions, and other data assist the examiner and investigators in creating a "picture" of what the computer was doing and how it was being used during the relevant time in question. Given the interrelationships of the data to various parts of the computer's operation, this information cannot be easily segregated.

37. Digital data on the hard drive that is not currently associated with any file may reveal evidence of a file that was once on the hard drive but has since been deleted or edited, or it

could reveal a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, email programs, and chat programs store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Such data may also lead to exculpatory evidence.

38. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be learned from the absence of particular data on a digital device. Specifically, the lack of computer security software, virus protection, malicious software, evidence of remote control by another computer system, or other programs or software may assist in identifying the user indirectly and may provide evidence excluding other causes for the presence or absence of the items sought by this application.

39. Additionally, since computer drives may store artifacts from the installation of software that is no longer active, evidence of the historical presence of the kind of software and data described may have special significance in establishing timelines of usage, confirming the identification of certain users, establishing a point of reference for usage and, in some cases, assisting in the identification of certain users.

40. This data can be evidence of a crime, can indicate the identity of the user of the digital device, or can point toward the existence of evidence in other locations. Such data may

also lead to exculpatory evidence. Evidence of the absence of particular data on the drive is not generally capable of being segregated from the rest of the data on the drive.

Search Procedure

41. In searching for data capable of being read, stored, or interpreted by a computer or storage device, law enforcement personnel executing the search warrant will employ the following procedure:

a) On-site search, if practicable. Law enforcement officers trained in computer forensics (hereafter, "computer personnel"), if present, may be able to determine if digital devices can be searched on-site in a reasonable amount of time and without jeopardizing the ability to preserve data on the devices. Any device searched on-site will be seized only if it contains data falling within the list of items to be seized as set forth in the warrant and in Attachment B.

b) On-site imaging, if practicable. If a digital device cannot be searched on-site as described above, the computer personnel, if present, will determine whether the device can be imaged on-site in a reasonable amount of time without jeopardizing the ability to preserve the data.

c) Seizure of digital devices for off-site imaging and search. If no computer personnel are present at the execution of the search warrant, or if they determine that a digital device cannot be searched or imaged on-site in a reasonable amount of time and without jeopardizing the ability to preserve data, the digital device will be seized and transported to an appropriate law enforcement laboratory for review.

d) Law enforcement personnel will examine the digital device to extract and seize any data that falls within the list of items to be seized as set forth in the warrant and in

Attachment B. To the extent they discover data that falls outside the scope of the warrant that they believe should be seized (e.g., contraband or evidence of other crimes), they will seek an additional warrant.

e) Law enforcement personnel will use procedures designed to identify items to be seized under the warrant. These procedures may include the use of a "hash value" library to exclude normal operating system files that do not need to be searched. In addition, law enforcement personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data falls within the list of items to be seized under the warrant.

f) If the digital device was seized or imaged, law enforcement personnel will perform an initial search of the original digital device or image within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If, after conducting the initial search, law enforcement personnel determine that an original digital device contains any data falling within the list of items to be seized pursuant to this warrant, the government will retain the original digital device to, among other things, litigate the admissibility/authenticity of the seized items at trial, ensure the integrity of the copies, ensure the adequacy of chain of custody, and resolve any issues regarding contamination of the evidence. If the government needs additional time to determine whether an original digital device or image contains any data falling within the list of items to be seized pursuant to this warrant, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete the search of the digital device or image within 180 days of the date of execution of the warrant. If the

government needs additional time to complete the search, it may seek an extension of the time period from the Court within the original 180-day period from the date of execution of the warrant.

g) If, at the conclusion of the search, law enforcement personnel determine that particular files or file folders on an original digital device or image do not contain any data falling within the list of items to be seized pursuant to the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the list of items to be seized pursuant to the warrant, as well as data within the operating system, file system, or software application relating or pertaining to files or data falling within the list of items to be seized pursuant to the warrant (such as log files, registry data, and the like), through the conclusion of the case.

h) If an original digital device does not contain any data falling within the list of items to be seized pursuant to this warrant, the government will return that original data device to its owner within a reasonable period of time following the search of that original data device and will seal any image of the device, absent further authorization from the Court.

Data to be Seized

42. In order to search for data that is capable of being read or interpreted by a computer, law enforcement personnel will need to seize, image, copy, and/or search the following items, subject to the procedures set forth herein:

a) Any computer equipment or digital devices that are capable of being used to commit or further the crime outlined above, or to create, access, or store contraband

or the types of evidence, fruits, or instrumentalities of such crime, as set forth in Attachment B;

b) Any computer equipment or digital devices used to facilitate the transmission, creation, display, encoding, or storage of data, including word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices, and optical scanners that are capable of being used to commit or further the crimes outlined above, or to create, access, process, or store the types of evidence, contraband, fruits, or instrumentalities of such crimes, as set forth in Attachment B;

c) Any magnetic, electronic, or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, personal digital assistants, and cell phones capable of being used to commit or further the crimes outlined above, or to create, access, or store the types of evidence, contraband, fruits, or instrumentalities of such crimes, as set forth in Attachment B;

d) Any documentation, operating logs, and reference manuals regarding the operation of the computer equipment, storage devices, or software;

e) Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

f) Any physical keys, encryption devices, dongles, or similar physical items which are necessary to gain access to the computer equipment, storage devices, or data;

g) Any passwords, password files, test keys, encryption codes, or other information necessary to access the computer equipment, storage devices, or data, and

h) All records, documents, programs, applications, or materials created, modified, or stored in any form, including in digital form, on any computer or digital device, that show the actual user(s) of the computers or digital devices during any time period in which the device was used to upload, download, store, receive, possess, or view child pornography, including the web browser's history; temporary Internet files; cookies, bookmarked or favorite web pages; email addresses used from the computer; MAC IDs and/or Internet Protocol addresses used by the computer; email, instant messages, and other electronic communications; address books; contact lists; records of social networking and online service usage; and software that would allow others to control the digital device such as viruses, Trojan horses, and other forms of malicious software.

Retention of Image

43. The government will retain a forensic image of each electronic storage device subjected to analysis for a number of reasons, including proving the authenticity of evidence to be used at trial; responding to questions regarding the corruption of data; establishing the chain of custody of data; refuting claims of fabricating, tampering, or destroying data; and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

Inventory and Return

44. With respect to the seizure of electronic storage media or the seizure or imaging of electronically stored information, the search warrant return to the Court will describe the physical storage media that were seized or imaged.

45. Based on the above, I believe there is probable cause that a firearm, and other firearms, ammunition, and other firearms-related items, as well electronic evidence related to threatening communications as described in this affidavit and in Attachment B, will be found at the residence of Greg Michael Reynolds at 35612 SE Macinnes Rd, Corbett, Oregon, or on the person of Greg Michael Reynolds, or in a Ford Ranger vehicle currently registered to REYNOLDS bearing Oregon license plate CA21276 located at 35612 SE Macinnes Rd, Corbett, Oregon, or in a Chevrolet Astro Van currently registered to REYNOLDS bearing Oregon License plate K7ZZY located at 35612 SE Macinnes Rd, Corbett, Oregon, and that said items are evidence of the crime of interstate threatening communications under Title18, United States Code, Section 875(c). I thus request that the court issue a warrant to search the premises, including dwelling, outbuildings, and curtilage, of address 35612 SE Macinnes Rd, Corbett, Oregon along with a Ford Ranger vehicle, bearing Oregon license plate CA21276, located at 35612 SE Macinnes Rd, Corbett, Oregon, a Chevrolet Astro Van bearing Oregon License plate K7ZZY located at 35612 SE Macinnes Rd, Corbett, Oregon as well as the person of Greg Michael Reynolds, for the items described in Attachment B, and to seize the same.

////

////

////

////

46. This affidavit and proposed search warrant have been reviewed by Assistant United States Attorney Stephen Peifer, who advised me that it is his opinion the affidavit demonstrates probable cause and that the search warrant is in proper order.

Peter Summers
Special Agent, FBI

SWORN AND SUBSCRIBED to before me this 31st day of July, 2014.

JOHN V. ACOSTA
United States Magistrate Judge

ATTACHMENT A

PLACE TO BE SEARCHED

SUBJECT 1- The person of Greg Michael Reynolds, white male, date of birth 08/17/1973

SUBJECT PREMISES 1 – located at 35612 SE Macinnes Road, Corbett Oregon, 97019, and is the residence of Greg Michael Reynolds.

Appears to be a single-floor home, which abuts a small hill. The residence is located at the end of a declined driveway, and has a brown exterior. Maroon canopies provide sun covering over the main entry door, and some of the windows facing the driveway. The front door is reached by stairs which lead from the driveway area to what appears to be a wooden deck.

SUBJECT VEHICLE 1 - a 2004 Ford Ranger, Oregon license plate number CA21276, and vehicle identifications number 1FTZR45E85PA21069. Located at SUBJECT PREMISES 1.

SUBJECT VEHICLE 2 – a 2002 Chevy Astro van, Oregon license plate number K7ZZY, and vehicle identification number 1GNEL19XX2B122592. Located at SUBJECT PREMISES 1.

ATTACHMENT B

Items to be Searched For, Seized, and Examined

The following records, documents, and items that constitute evidence, contraband, fruits and/or instrumentalities of violation of 18 USC § 875 (c), Interstate communications.

a) Documents to include notices, bills, letters, and written communications ;

b) Any handgun or firearm ammunition, written documents relating to firearms, cleaning kits, holsters, targets, spent cartridges, gun cases or safes;

c) Cellular telephones to include smart phones;

d) Computers, laptops, and electronic media storage devices;

e) Usernames or passwords pertaining to computer access, electronic mail accounts greynolds@portlandstate.org, greynolds73@gmail.com, reynoldsvs.psu@gmail.com, and cellular telephones related thereto.

f) Contact lists or documents associated with Portland State University.