

 ORIGINAL

FILED  
KING COUNTY, WASHINGTON

JAN 07 2015

DEPARTMENT OF  
JUDICIAL ADMINISTRATION

SUPERIOR COURT, KING COUNTY, WASHINGTON

STATE OF WASHINGTON	)	14-1-12052-1
	) ss.	NO: 14-908
COUNTY OF KING	)	AFFIDAVIT FOR SEARCH WARRANT

Special Agent Michael Larson, being first duly sworn on oath, deposes and says:

On the basis of the following, I believe there is probable cause that **Brian Richard Farrell** has/have committed, is/are committing, and/or are about to commit the below-identified crime(s) in King County, and that

- Evidence of the crime(s) of **Violation of the Uniformed Controlled Substances Act—Possession of Alprazolam (Xanax) with Intent to Deliver (RCW 69.50.401)**;
- Contraband, the fruits of a crime, or things otherwise criminally possessed;
- Weapons or other things by means of which a crime has been committed or reasonably appears about to be committed;
- A person for whose arrest there is probable cause, or who is unlawfully restrained;

is/are located in, on, at, or about the following described premises, vehicle or person:

**Premises:** The property is located at 4238 163rd Avenue SE, in Bellevue, King County, Washington (98006). The property is located on the east side of 163<sup>rd</sup> Avenue SE just south of SE 42nd Place. The property includes a two-story single-family residence and an attached garage. The house is tan in color and the exterior is finished with horizontal siding on the lower level and vertical siding on the upper level. Additionally, there is a small porch/entryway on the west side of the house which is partially enclosed with a three- to four-foot-tall brick wall. The front door is light brown in color and faces west. The house number is not visible on the exterior of the residence. The search should include the entire property, including the garage and any other outbuildings.

**Property:** The following property is secured in evidence bags and located in an access-controlled facility at the Seattle office of the Homeland Security Investigations, in King County, Washington.

1. A gray/black Apple MacBook Air laptop, serial number C02MR0RHFLCF;
2. A gray Apple iPad, SN DMPNKAQUG5W1;

3. A gray/black Apple iPhone 5S, SN 352007066546184;
4. A gray/black HTC cellphone, SN HTC6525LVW;
5. A white three-terabyte Apple Airport Time Capsule, SN C86N80KHF9H6;
6. A gray/black Sony 32-gigabyte thumb drive;
7. A black SanDisk 16-gigabyte micro SD card;
8. A black SanDisk two-gigabyte micro SD card;
9. A white O2 sim card;
10. A white Libara sim card.

On the basis of the following, I, Special Agent Michael Larson, believe there is probable cause that Brian Richard Farrell has/have committed, is/are committing, and/or are about to commit the above-identified crime(s) in King County, and that evidence of that/those crimes is/are in the above-identified location(s).

#### AFFIANT

My name is Michael Larson and I have been a law enforcement officer for over 16 years. I am currently a Special Agent with the Department of Homeland Security, United States Immigration and Customs Enforcement, Homeland Security Investigations; assigned to the Office of the Special Agent in Charge, Seattle, Washington. I have been employed as a Special Agent since July 2009 and I am currently assigned to the Border Enforcement Security Task Force (BEST). BEST Seattle is comprised of members from Homeland Security Investigations; U.S. Customs and Border Protection's Office of Field Operation; the U.S. Secret Service; the U.S. Coast Guard Investigative Service; the U.S. Postal Inspection Service; the Seattle Police Department; and the Port of Seattle Police Department. BEST Seattle investigates smuggling and related crimes and combats criminal organizations seeking to exploit vulnerabilities at the Seattle and Tacoma-area airports, seaports, and adjacent waterways.

During my career, I have participated in investigations and search warrants involving theft, fraud, money laundering, smuggling, import and export violations, counterfeit goods, crimes against persons, and drug trafficking. I am a graduate of the Federal Law Enforcement Training Center's Criminal Investigator Training Program in Brunswick, Georgia, as well as the U.S. Immigration and Customs Enforcement Special Agent Training Program. During my participation in these two programs, I completed over 2,000 hours of basic and specialized law enforcement training.

Prior to my employment with Homeland Security Investigations, I worked for the U.S. District Court for eleven years as a U.S. Probation Officer and U.S. Probation Officer Assistant in both the Western District of Michigan and Western District of Washington. Additionally, I am a graduate of Michigan State University in East Lansing, Michigan, where I received Bachelor's degrees in International Relations and Criminal Justice from James Madison College and the School of Criminal Justice, respectively.

Based on my training and experience, I am familiar with the identification of various illegal controlled substances, the field-testing of those illegal controlled substances, the proper

1 terminology that is used to identify and make reference to certain illegal controlled substances,  
2 and techniques for conducting drug trafficking investigations.

3 I have conversed with drug users and drug dealers about illegal controlled substances. I have  
4 verified information received from drug users and drug dealers through independent sources such  
5 as police reports, other agents and officers, reliable informants, and from evidence gathered  
6 during searches. Thus, I am familiar with the methods and ways of drug users and dealers.

7 I have participated in the service of search warrants and consent searches where illegal controlled  
8 substances were located. I am familiar with both the appearance and odor of illegal controlled  
9 substances from enforcement activities, as well as from training classes in which illegal  
10 controlled substances were introduced to familiarize officers with their physical characteristics. I  
11 have also become familiar with how illegal controlled substances are normally packaged for sale.

12 Based on my training, experience, participation in narcotics investigations, and my conversations  
13 with other experienced narcotics investigators, who I am associated with, I know:

- 14 • That individuals involved in the acquisition, transportation, consumption, and sale of  
15 illegal controlled substances, commonly keep paraphernalia and supplies for weighing,  
16 packaging, and consuming their illegal controlled substances. Such paraphernalia  
17 includes, but is not limited to, razor blades, pipes, scales, cutting and diluting agents,  
18 packaging materials, and plastic baggies. The aforementioned items are usually  
19 maintained in a suspect's residence, including outbuildings and vehicles, for ready access  
20 and concealment from law enforcement detection.
- 21 • That individuals involved in the acquisition, transportation, and sale of illegal controlled  
22 substances often use cellular telephones, telephonic pagers, telephone answering  
23 machines, voice mail systems, and even computer generated electronic messaging  
24 systems (e-mail) to communicate with suppliers, customers, and accomplices. On  
25 occasion, persons will "code" their messages in order to transmit information securely  
26 and avoid law enforcement detection. For instance, drug dealers often assign "codes" to  
27 their customers who can then "page" them and enter their coded identity and/or a  
28 particular coded drug request. Most cellular telephones, telephonic pagers, answering  
machines, voice mail systems, and computers have the capability to store completed  
messages which detectives can retrieve upon seizing a particular item.
- That individuals involved in the acquisition, transportation, and sale of illegal controlled  
substances are often in possession of dangerous weapons. These weapons may include,  
but are not limited to, firearms, knives, and swords. Said weapons are used to protect and  
secure a drug dealer's property. Such property may include, but is not limited to, illegal  
controlled substances, records, monies, and other assets. The aforementioned weapons  
are usually maintained in a suspect's residence, including outbuildings and vehicles, for  
ready access.

- 1 • That individuals involved in the acquisition, transportation, and sale of illegal controlled  
2 substances, often take, or allow to be taken, photographs and video recordings of  
3 themselves, their associates, their property, and their illegal controlled substances. The  
4 aforementioned photographs and video recordings are usually maintained in a suspect's  
5 residence and vehicles for their enjoyment.
- 6 • That individuals involved in the acquisition, transportation, and sale of illegal controlled  
7 substances, routinely maintain records regarding their illegal activities. Their records are  
8 typically related to the ordering, transportation, acquisition, possession, and sale of their  
9 illegal controlled substances. These records reflect the names, addresses, and telephone  
10 numbers of their criminal associates, as well as other locations under their control, such  
11 as additional residences and storage units. Drug dealers almost always keep records of  
12 their drug transactions and the payments and debts owed to them. These records are  
13 commonly  
14 • referred to as pay/owe sheets. Drug dealers maintain these records in books, ledgers, and  
15 computers or on computer data storage media, note pads, and scrap papers. The  
16 aforementioned records are usually maintained in a suspect's residence, including  
17 outbuildings and vehicles, for ready access and concealment from law enforcement  
18 detection.
- 19 • That individuals involved in the sale and distribution of illegal controlled substances,  
20 almost always maintain amounts of money, financial instruments, jewelry, and other  
21 assets which are proceeds from or intended to be used to facilitate drug transactions. All  
22 such items, in addition to being evidence of drug trafficking violations, are forfeitable  
23 under Washington State law. Because of this, drug dealers will attempt to conceal the  
24 proceeds of drug sales in secure locations within their residence, including outbuildings  
25 and vehicles, for ready access and concealment from law enforcement detection.
- 26 • That individuals involved in the sale and distribution of illegal controlled substances,  
27 profit from the sale of these drugs and then attempt to legitimize those profits. I know  
28 that to accomplish this task, these individuals often utilized false and fictitious business  
records, cashier checks, accounts in foreign and domestic banks, and often transfer to  
third persons or purchase in another person's name, real and personal property. Also,  
since the government's efforts at seizing and forfeiting drug-related assets have been  
widely publicized, individuals involved in the sale and distribution of illegal controlled  
substances often place assets in the name of others to avoid detection and subsequent  
asset seizure. Records of such activity are often located in a person's residence for ready  
access and concealment from law enforcement detection.
- That individuals involved in the distribution of illegal narcotics often keep locations in  
lieu of or in addition to their own homes in order to store items related to their illegal  
activities, for the intended purpose of keeping these items safe from potential theft and  
hidden from the detection of law enforcement.

1 INVESTIGATION

2 **Silk Road Background**

(Homeland Security Investigations)

3 Based on reading FBI and HSI law enforcement documents and on speaking with agents familiar  
4 with this investigation, I know that SR2 is the successor site to the original Silk Road, which was  
5 taken down by law enforcement in 2013. SR2 operates in the same manner as Silk Road. SR2 is  
6 an anonymous underground web site that has an infrastructure similar to well-known online  
7 marketplaces such as Amazon Marketplace or eBay, allowing sellers and buyers to conduct  
8 transactions online. However, unlike legitimate websites, the SR2 website is designed to  
9 facilitate illegal commerce by ensuring absolute anonymity on the part of both buyer and seller.  
10 SR2 is a platform that facilitates the sale of illicit goods and services, primarily illegal drugs,  
11 including, but not limited to, MDMA (Ecstasy), LSD, cannabis, hashish, cocaine and heroin.  
12 SR2 operates as a middleman or escrow account, holding the digital currency during the  
13 transaction and taking a commission ranging from 8 to 15 percent from the vendor. SR2 vendors  
14 advertise that they ship to and from countries around the world, including the United States,  
15 Netherlands, Germany and the United Kingdom.

16 Based on my knowledge and the knowledge of other law enforcement agents familiar with this  
17 investigation, I know that SR2 is not limited to selling controlled substances. Some of the other  
18 products listed for sale include weapons, fake identification cards, drug paraphernalia,  
19 counterfeit merchandise, stolen identity/credit cards, malicious software and computer  
20 equipment consistent with hacking such as password stealers, key loggers and remote access  
21 tools. SR2 emerged as one the most sophisticated and extensive criminal marketplaces on the  
22 Internet to date.

23 The primary means by which SR2 protects the user's identity is by operating on "The Onion  
24 Router" (hereinafter "TOR") network, which is a special network of computers distributed  
25 around the world designed to conceal the true Internet Protocol (hereinafter "IP") addresses of  
26 the users on the network. Every communication sent through TOR is bounced through numerous  
27 relays within the network and wrapped in a layer of encryption at each relay, such that the end  
28 recipient of the communication has no way of tracing the communication back to its true  
originating IP address. TOR also enables web sites to operate on the network in a manner that  
conceals the true IP address of the computer server hosting the website.

29 On October 1, 2013, HSI Chicago working in conjunction with the Federal Bureau of  
30 Investigation (FBI), New York (NY) arrested Ross Ulbricht, Also Known As (AKA) Dread  
31 Pirate Roberts (DPR), in San Francisco, CA. DPR owned and operated the Silk Road and shortly  
32 after his arrest and the Silk Road dismantlement, SR2 was created, which also operates on TOR.  
33 Silk Road operated from approximately February 2011 up until the listed DPR arrest date.  
34 Thereafter, SR2 came online, and it offered the same or similar services, in the same or similar  
35 manner as Silk Road.

36 In order to access SR2, a user has to first download TOR, which is available from a web site  
37 called [www.torproject.org](http://www.torproject.org), (there are also other versions available). The user then needs to  
38

1 establish a Bitcoin account, which is another means used to anonymize users' identities. SR2  
2 requires that all transactions be paid for through the use of "Bitcoins," which are a virtually  
3 untraceable, decentralized, peer-to-peer form of electronic digital currency having no association  
with banks or governments.

4 I know that, based on conversations with agents familiar this investigation, a Bitcoin user  
5 typically purchases Bitcoins from a Bitcoin "exchanger." Currently a user could go to  
6 www.coinbase.com, a Bitcoin exchanger, open a Bitcoin account and purchase Bitcoins. Once a  
7 user has his or her Bitcoin account and TOR program, the user can then enter the SR2 Uniform  
8 Resource Locator (URL), also known as a web address, and sign up for a SR2 account. During  
9 the SR2 sign up process the user provides their Bitcoin account number to use for their  
10 transactions. Many users take additional precautions to mask their transactions by funneling their  
Bitcoin transactions through several other sites before payment or withdrawals are made. Once a  
user has set up his or her Bitcoin account and SR2 user name, the user can navigate through the  
site, which operates much like any other on-line marketplace. Products are advertised with a full  
description and vendors are rated by other users on the site.

11 From January 2014 to July 2014, a FBI NY Source of Information (SOI) provided reliable IP  
12 addresses for TOR and hidden services such as SR2, which included its main marketplace URL  
13 (silkroad6ownowfk.onion), its vendor URL (vx3w763ohd256iyh.onion), its forum URL  
14 (silkroad5v7dywlc.onion) and its support interface (uz434sei7arqunp6.onion). The SOI's  
information ultimately led to the identification of SR2 servers, which led to the identification of  
at least another seventeen black markets on TOR.

15 The SOI also identified approximately 78 IP addresses that accessed a vendor .onion address. A  
16 user cannot accidentally end up on the vendor site. The site is for vendors only, and access is only  
17 given to the site by the SR2 administrators/moderators after confirmation of a significant amount  
18 of successful transactions. If a user visits the vendor URL, he or she is asked for a user name and  
password. Without a user name and password, the vendor web site cannot be viewed.

### 19 **Current Investigation**

20 On July 30, 2014, Homeland Security Investigations <sup>(HSI)</sup> Seattle received information that a user  
21 associated with IP address 67.182.142.24 accessed the vendor portal of SR2. Records reveal the  
22 IP address was associated with a Comcast internet account registered to Steve Phelps at 4238  
163rd Avenue SE – Bellevue, WA 98006.

23 On August 8, 2014, the Washington Department of Licensing reported the following vehicle and  
24 driver information for that address:

- 25 1. Registered to Steve Phelps:
  - 26 a. 2005 Blue Volkswagen Beetle, WA Plate 221YJR;
  - 27 b. 2004 Black Yamaha XVS11ASC Motorcycle, WA Plate 7B3364;
  - 28 c. 1992 Black Honda VT1100CL Motorcycle, WA Plate 967140.

1 2. Registered to Brian Farrell:

- 2 a. 2006 White Mini Cooper, WA Plate ARF0500;  
3 b. 1992 White BMW 325, WA Plate ANK1380;  
4 c. 1991 White Chevrolet Camero, WA Plate 871ZJJ.

5 On August 13, 2014, Homeland Security Investigations initiated surveillance activities on the  
6 above address, further observing the blue Volkswagen Beetle, and the white Chevrolet Camero.  
7 At approximately 2:09 p.m., a white male matching the physical description of Steve Phelps was  
8 observed leaving the residence in the blue Volkswagen Beetle.

9 On August 25, 2014, Homeland Security Investigations agents initiated surveillance activities on  
10 4238 163rd Avenue SE, further observing Brian Farrell's white Mini Cooper.

11 On October 10, 2014, Homeland Security Investigations, assisted by a U.S. Postal Inspector,  
12 visited several U.S. Post Offices near 4238 163rd Avenue SE, Bellevue, WA 98006. During  
13 these visits, postal employees were interviewed and shown photographs of several individuals to  
14 include Steve Phelps and Brian Farrell. While at the Issaquah Branch located at 400 NW Gilman  
15 Boulevard, one employee recognized the photograph of Brian Farrell, stating that he might have  
16 come into the post office several times in the past. While at the Crossroads Branch located at  
17 15731 NE Eighth Street, another employee stated that he recognized Brian Farrell as someone  
18 who may have come into the post office several times in the past. Another employee at the same  
19 location recognized the photograph of Steve Phelps, further stating he may have dropped off a  
20 tub of letters for mailing and he drove a blue station wagon.

21 On October 20, 2014, Homeland Security Investigations initiated surveillance activities on 4238  
22 163rd Avenue SE, Bellevue, WA 98006; further observing two vehicles not previously observed  
23 at the residence including a Volkswagen Passat station wagon, bearing WA Plate ARX9262,  
24 registered to Margarita Iordach; and a Toyota pickup truck, bearing WA Plate LIFTED,  
25 registered to Lesley Karen Gregory. At approximately 1:38 p.m., an individual matching Brian  
26 Farrell's physical description was observed leaving the residence in his white Mini Cooper. At  
27 approximately 2:55 p.m., Brian Farrell was pulled over for speeding by an officer from the Brier  
28 Police Department. During the vehicle stop, Brian Farrell admitted to the responding officer that  
he was carrying a Glock semi-automatic pistol in his glove box, further advising he possessed a  
valid concealed carry permit.

On October 27, 2014, the Washington Employment Security Department reported Brian Farrell  
was employed by CompuCom at 1756 114th Avenue, Suite 220, Bellevue, WA 98004, where he  
received wages totaling \$69,974.01 for the period covering January 1, 2013, through in or about  
June 2014. No employer or wage information was reported for Steve Phelps during that period.

On December 1, 2014, Brian Farrell departed Seatac International Airport aboard Icelandair  
Flight 680 to Keflavik International Airport. On December 20, 2014, Brian Farrell departed  
Dublin International Airport aboard Aer Lingus Flight 125 to Chicago O'Hare International  
Airport. Upon arriving in Chicago, Brian Farrell was referred for a secondary inspection where

1 he was contacted by U.S. Customs and Border Protection Officers and Homeland Security  
2 Investigations Special Agents.

3 During the secondary inspection, Brian Farrell was found to be in possession of the following  
4 computers, phones, and digital media: an Apple Airport 3TB Time Capsule, an Apple iPad, an  
5 Apple Air Laptop, an Apple iPhone 5S cell phone, an HTC cell phone, a 32 GB thumb drive, and  
6 four memory cards. When questioned regarding the nature of his travel, Brian Farrell explained  
7 that he was returning to the U.S. after visiting London, Scotland, and Ireland. Brian Farrell  
8 further explained that he previously worked for Microsoft and the he was fired from this job in  
9 September 2014. Brian Farrell explained that he purchased the Apple devices after leaving  
10 Microsoft, further stating he bought the Apple Airport 3TB Time Capsule while overseas. Brian  
11 Farrell was unable to explain why he was traveling with so many digital devices, further refusing  
12 to provide investigators with any of his passcodes. Brian Farrell also purchased a \$5,000.00  
13 Omega watch and a \$1,000.00 suit while overseas. Brian Farrell reported his roommate to be  
14 Steve Phelps. During the inspection, Brian Farrell was also found to be in possession of  
15 prescriptions for Alprazolam and Diazepam. Brian Farrell's computers, phones, and digital  
16 media were subsequently detained for further review, pursuant to the border search authority  
17 afforded to customs agents and officers. These items were securely forwarded to HSI-Seattle.

18 On December 22, 2014, Homeland Security Investigations Special Agents and Task Force  
19 Officers initiated contact with Brian Farrell and Steve Phelps at 4238 163rd Avenue SE. Upon  
20 making contact with Brian Farrell and Steve Phelps, agents identified themselves and their  
21 purpose; both men agreed to voluntary interviews.

22 During the interview of Brian Farrell, agents learned that he previously worked for Microsoft as  
23 a contract employee. Brian Farrell admitted that he was familiar with Silk Road from the news,  
24 further admitting to visiting the site within the last six months. Brian Farrell advised agents, "I  
25 deal with bitcoins," further stating Silk Road was the "shady side of bitcoins." Brian Farrell  
26 denied ever buying or selling drugs on Silk Road, stating that to the best of his knowledge no one  
27 living with him was involved in buying or selling drugs. Brian Farrell reported his roommate to  
28 be Steve Phelps, further stating they have a Comcast account which the two men share.

During the interview of Steve Phelps, agents learned that he was unemployed and currently  
receiving disability benefits related to severe diabetes. Steve Phelps stated that he has rented a  
room at the residence since 2008. During the period that he has lived there, up to four other  
individuals have lived in the lower level of the house. Currently, only Steve Phelps and Brian  
Farrell live at the residence. Steve Phelps explained that Brian Farrell rents the entire lower level  
of the residence; however, the two men share common areas in the house. Steve Phelps stated  
that Brian Farrell is a "computer wizard," and has made a number of upgrades to the computer  
network in the house. Steve Phelps advised that Brian Farrell has a computer server in the  
garage. Steve Phelps stated he learned about Silk Road and the "dark net" from Brian Farrell.  
Steve Phelps further stated that Brian Farrell showed him the Silk Road website which was full  
of drugs for sale. Brian Farrell advised Steve Phelps that he could get "anything" off the  
website. Steve Phelps described Brian Farrell as displaying great "bravado," noting that Brian  
Farrell bragged about being a hacker and being part of a hacking collective called "Anonymous."



1 Steve Phelps described Brian Farrell's drug use as being "astonishing," further stating he used all  
2 kinds of medications including Ambien, Valium, Diazepam, and other narcotics. Steve Phelps  
3 advised that Brian Phelps receives packages on a daily basis from UPS, FedEx, and USPS.  
4 Steve Phelps stated Brian Farrell "obsessively" tracks his packages online and "babysits" the  
5 mailbox. Steve Phelps recalled one occasion where he opened a suspicious package addressed to  
6 Brian Farrell and found it to contain a bag of Xanax pills. When asked about what he did about  
7 the pills, Steve Phelps stated that he held on to them, further agreeing to surrender them to  
8 agents. Steve Phelps stated he first spoke to Brian Farrell about Silk Road within the last six to  
9 eight months.

7 On December 23, 2014, Homeland Security Investigations Special Agents met with Steve Phelps  
8 who signed a Notice of Abandonment and Assent to Forfeiture of Prohibited or Seized  
9 Merchandise for the Xanax pills. At the time Mr. Phelps signed the notice, he surrendered 107  
10 Xanax pills to agents. The pills were subsequently seized, counted, and a logged into evidence.

#### 10 **Technical Foundation Regarding Digital Devices Seized or to Be Seized**

11 I know from training and experience that people own cellular telephones for the purpose of being  
12 able to use them wherever they are, and as such carry them virtually constantly, or are nearly  
13 always within the near vicinity of their cell phones and/or portable devices. Criminals often use  
14 cellular phones to communicate with accomplices and will sometimes store accomplice's contact  
15 or identity information in contact lists, speed dial lists, or other areas of the phone. The  
16 communications can occur in many ways, including through typical cellular phone calls, instant  
17 messaging, text messages, SMS communications, chat sessions, email and social networking  
18 websites. I know that criminals use cellular phones to document and share information about  
19 criminal activities through phone calls, email, text messages, instant messages, SMS  
20 communications, photographs, videos, notes, and digital or voice memos that depict, discuss, or  
21 identify crime scenes, contraband, proceeds, victims, accomplices, or other evidence. Some of  
22 these communications are directed to another person or persons. Others are posted and shared  
23 more publicly, as happens with chat sessions and social networking websites. Cellular phone  
24 users can also use their phones for calendar items, web surfing, and obtaining directions to  
25 locations. A cellular telephone typically stores, without action by the user, evidence of this use  
26 and activity of the phone in its memory and other onboard or external storage such as SIM card  
27 or Micro SD card, as well as information, such as call logs, address books, messages sent and  
28 received, images, audio and video files, personal calendars, documents, as well as IP addresses  
(unique numeric identifiers assigned when a device accesses the internet) and profiles for  
wireless networks to which they have been connected using wired or Wi-Fi connectivity, which  
include location as well as internet activity information (files viewed via the internet are  
typically automatically downloaded onto a computer). These evidentiary records,  
communications, and images can be retrieved from a cellular telephone, and will also often  
indicate the date, time, and physical location at which the activity occurred (cell site data and/or  
GPS coordinates for the phone). As such, a person's use of the phone will reveal where a person  
has been at particular dates and times relevant to the crimes under investigation in this case, a  
person's activity at relevant dates and times, and/or places where a person frequents at which that

1 person is likely to be found for arrest or at which the suspect stored or inadvertently left evidence  
2 behind.

3 Based on my training and experience, I know that cellular telephones can store such information  
4 for long periods of time, and that the above-reference information can often be retrieved by a  
5 trained forensic examiner months or even years after the data was stored on the phone, even  
6 when it has purportedly have been erased or deleted from the phone. Forensic evidence on the  
7 phone can also establish how the phone was used, by whom, and when, and the purposes for  
8 which it was used. Whether some data on the phone is evidence may depend on other  
9 information stored on the phone, and the application of an examiner's knowledge about how a  
10 cellular telephone behaves. Therefore, contextual information is necessary to understand the  
11 other evidence that falls within the scope of the warrant. Sometimes it might be possible to find  
12 data, records, or location information within a cell phone that can be used to corroborate details  
13 of an alibi. Other categories of exculpatory evidence might also be available that can help  
14 investigators to rule out an individual as a suspect.

15 One form in which evidence of or pertaining to the above-listed crimes might be found is  
16 digital—stored on a digital device or digital storage media. The terms “digital device” and  
17 “device” include devices capable of capturing and/or storing digital data, such as computers,  
18 cameras, personal assistants, iPods, portable media players, tablet computers like iPad, gaming  
19 consoles, video cameras, DVRs (digital video recorders), web cams or other video capture  
20 devices, modems, routers, firewalls, wireless access points, printers, cellular telephones, GPS  
21 navigation devices, etc. Digital data storage media (hereafter “media”) include solid state drives  
22 (SSDs), hard disk drives (HDDs), compact discs, DVDs, Blu-Ray discs, flash media such as  
23 thumb drives, Secure Digital (SD) cards, Micro Secure Digital (MicroSD) cards, backup drives,  
24 and the like. Data stored on digital devices and media can be easily transferred from one device  
25 or storage media to another.

26 I know from training and experience and that of my fellow officers that digital devices and media  
27 can be used for a wide variety of activities in connection with criminal activity; typically retain  
28 some evidence of all activity taken on or in the device or media; and, as such, are both  
intentional and/or unintentional storage devices that could contain evidence of crime. Digital  
devices and media can contain evidence of planning, preparation, commission of, efforts to  
conceal, and/or to sell or dispose of the proceeds of criminal activity. Examples of this evidence,  
places, and types of data in which this evidence may be found include: The identity of  
accomplices, victims and others -- which can be stored in files such as photographs, address  
books or contact lists, as well as in records of communications with accomplices, victims and  
others through means such as email, instant messaging, social media, Voice Over IP, and  
videoconferencing. Traces, or even the full contents, of these files and communications can  
remain on the digital device or media for indefinite periods of time after the communication  
originally took place, even if the user deleted the communication. Additional examples of  
evidence that may be found in digital devices and media include but are not limited to records  
regarding the loading, creation, modification, storage, deletion, copying, and/or sending of files  
such as documents, images, or recordings pertaining to the criminal activity or items, persons, or  
places of interest; financial transactions such as with financial institutions, businesses, or

1 individuals; purchases and sales of items or services; research through "web surfing;" use of the  
2 internet for other activities such as gaming; back up storage to a remote location, such as "the  
3 cloud;" database inquiries; use of social media; access to websites and services that produce  
4 directions, maps, or overhead imagery.

4 Wholly apart from user-generated files and data, digital devices and media typically store, often  
5 without any conscious action by the user, electronic evidence pertaining to virtually all actions  
6 taken on the digital device. This includes, for example, information regarding the identity of the  
7 device user(s) (the actual or assumed identity used by the person or persons using the digital  
8 device or media (user profile)). (This is analogous to a search for indicia of occupancy or  
9 dominion and control while executing a search warrant at a residence and can be found in  
10 numerous locations and formats within the device.) Additional examples of the type of data that  
11 analysis of digital devices and media can reveal include the date, time, and geographic location  
12 at which the device or media were used; evidence regarding the purpose of and actual use of the  
13 device and media; and evidence related to devices that have been connected, via wire or  
14 wirelessly, to the device being searched, which can include evidence of remote storage, synching  
15 of devices to one another, uploading or saving data to other devices, pointers to, and/or  
16 information pertaining to evidence that was transferred to and/or is stored at other locations such  
17 as web-based email accounts, network accessible services, social networking websites, and cloud  
18 storage. Digital device users typically do not erase or delete this evidence, because special  
19 software is typically required for the task. However, it is technically possible to delete this  
20 information. The data can be found in numerous locations, and formats. These types of  
21 information will be important to the forensic examiner's ability to piece together and recognize  
22 evidence of the above-listed crimes, when it is found in the digital device(s) or digital storage  
23 media.

17 Evidence can also be embedded into unlikely files for the type of evidence, such as a photo  
18 hidden within a document or vice versa, or files stored on an external device in an effort to  
19 conceal their existence. Information stored in digital devices and on media can be stored in  
20 random order; with deceptive file names; can be hidden from normal view; can be encrypted or  
21 password protected; and can be stored on unusual devices for the type of data, such as routers,  
22 printers, scanners, game consoles, or other devices that are similarly capable of storing digital  
23 data. Additionally, a computer router may store information about a user's internet access and  
24 could reveal unknown connected digital or remote storage devices or capability; a scanner or  
25 printer may store information that would identify the digital device with which it was used.  
26 Whether some data on the digital device(s) or media is evidence may depend on other  
27 information stored on the digital device(s) and media, and the application of an examiner's  
28 knowledge about how digital device(s) and media behave. A person who has appropriate  
familiarity with how a digital device works, and relevant contextual information from a  
particular device, can draw conclusions about how the devices and media were used, by whom,  
where, and when. This information is sometimes necessary to identify and understand the other  
evidence that falls within the scope of the warrant. Further, in finding evidence of how a digital  
device or media was used, the purpose of its use, who used it, where, and when, it is sometimes  
necessary to establish that a particular thing is not present on the device or media.

1 Based on my training and experience, I know that digital device(s) and digital storage media can  
2 store the above-referenced information for long periods of time, and that the information can  
3 often be retrieved by a trained forensic examiner months or even years after the data was stored  
4 on the digital device(s), even when it purportedly has been erased or deleted from the device(s).  
5 Deleted data remains accessible to a forensic examiner until the memory space at which it is  
6 stored is needed for new data. Thus, the ability to retrieve residue of a deleted electronic file  
7 from a hard drive depends less on when the file was created, downloaded, viewed, or deleted,  
8 than on a particular user's operating system, storage capacity, and computer habits. A forensic  
9 examiner can usually retrieve the above referenced evidentiary material from digital devices and  
10 media.

11 Digital device programs frequently require passwords, user names, and/or pass phrases to  
12 operate. Those may be kept inside a device, or outside the device in some other area known to  
13 the user. So, in addition to searching a digital device for evidence of the above-listed crime(s),  
14 investigators will need to search both the premises searched, and the digital device for evidence  
15 identifying the user(s) of the device and for passwords, user names, and/or pass phrases needed  
16 to operate the device. Further, due to the wide variety of digital devices and their operating  
17 systems, the forensic examiner may also need the following items in order to conduct a thorough  
18 and accurate search of the devices: computer hardware, software, peripherals, internal or  
19 external storage devices, power supplies, cables; internet connection and use information;  
20 security devices; software; manuals; and related material.

21 Depending on the quantity of available data storage, search of digital devices and media is  
22 anticipated to take anywhere between several hours and weeks to complete. A single megabyte  
23 of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of  
24 storage space (1,000 megabytes) is the equivalent of 500,000 double-spaced pages of text.  
25 Storage devices capable of storing terabytes of data are now commonplace. Just duplicating  
26 such a hard drive in a manner that ensures an accurate forensic copy takes a minimum of several  
27 hours, and can take days, to complete.

28 Due to the length of time required to search digital devices and digital storage media; the need to  
ensure that the devices cannot be altered or wiped via a remote command or destructive codes  
that a user may have embedded in the system; the need to ensure the evidence within the devices  
is correctly handled, which often requires use of forensic equipment in a laboratory environment;  
officer safety concerns; and so that law enforcement can release the search location back to its  
occupants much sooner than would otherwise occur, I request authority to remove from the  
search location all digital devices and media that could contain evidence authorized for seizure  
under the warrant for subsequent search pursuant to the terms of the warrant. To further ensure a  
complete and accurate analysis of the digital device(s) and digital storage media, the computer  
examiner may also need to have available all digital device related items such as software,  
hardware, attached devices such as printers, scanners and the like, power supplies, and cables,  
manuals, and instructions. Thus, I seek authority to also remove these items to the police  
department for later search.

I also request authority to obtain assistance from a technical specialist, to review the digital

1 device(s) and digital media for the best and least intrusive method of securing digital evidence that  
2 this warrant authorizes for seizure, and to assist in securing such evidence.

### 3 CONCLUSION

4 Based on all the foregoing information, there is probable cause to believe that evidence of the  
5 above-listed crimes exists at the above-described premises and that there is probable cause to  
6 search the above identified premises for the following items:

- 7 ➤ Items in whatever form that are fruits, evidence, or that were/are being used in the course  
8 of preparing to commit, committing, disposing of proceeds or evidence, and/or efforts to  
9 conceal the above-listed crimes, including;
  - 10 ▪ Alprazolam (Xanax), and any other unlawfully possessed controlled
  - 11 ▪ packaging materials, equipment, scales, containers, paraphernalia, and any
  - 12 ▪ other items used in the consumption, distribution or manufacturing of
  - 13 ▪ controlled substances;
  - 14 ▪ Documents which show the acquisition and distribution of illegal drugs;
  - 15 ▪ Financial documents which show the distribution of proceeds from illegal
  - 16 ▪ drug transactions;
  - 17 ▪ Literature, books, magazines, and photographs pertaining to controlled
  - 18 ▪ substances;
  - 19 ▪ Any weapons possessed in violation of Chapter 9.41 RCW;
  - 20 ▪ Monies or assets deemed to be proceeds of illegal drug transactions;
- 21 ➤ Items in whatever form evidencing dominion and control of the premises;
- 22 ➤ Evidence of use of devices that are capable of containing evidence of the listed crimes  
23 between July 30, 2014, and December 31, 2014, to access black-market trading sites  
24 and/or to communicate with criminal associates or others about or pertaining to the  
25 above-listed crime(s), via incoming or outgoing calls, missed calls, chat sessions, instant  
26 messages, text messages, voice memo, voice mail, SMS communications, internet usage,  
27 and the like;
- 28 ➤ Other evidence of or pertaining to use of digital device(s) and digital storage media in  
connection with the above-listed crime(s), in whatever form, including storage media,  
peripherals and other items used in conjunction with digital devices or media to further  
commission or concealment of the crime, or which may be found in printed material such  
as documents, images, videos, contact lists, address lists, records or notes of internet  
searches;
- Information identifying, tending to identify, or relevant to identifying the digital device  
user at the date and time the things described in the warrant were created, edited,  
accessed or deleted; between the above-stated dates; and/or tending to identify the  
possessor of the device at those dates and times, and/or establishing dominion and control  
of the device at those dates and times;
- Any of the following that are capable of containing evidence, in whatever form, of the  
above-listed crime(s), and of dominion and control over the digital device and media and  
of dominion and control over the physical location searched. These items may be

1 subsequently searched for said evidence, and for evidence showing ownership and/or  
2 identifying the users of said equipment: Any and all computer hardware, software,  
3 peripherals, internal or external storage devices, power supplies, and cables. The  
4 following may also be searched for and seized to facilitate search of the above-listed  
5 items: user names, passwords, pass phrases, internet connection and use information,  
6 security devices, software, manuals and related materials.

- 7 ➤ Other evidence of or pertaining to use of the device in connection with the above-listed  
8 crime(s), which may be found in call logs, photographs, images, videos, documents,  
9 contact lists, address lists, internet searches, or other data storage within the device;
- 10 ➤ All information that can be used to calculate the position of the phone between the above-  
11 listed dates, including location data, cell tower usage, GPS satellite data, and GPS  
12 coordinates for routes and destination queries between the above-listed dates which is or  
13 pertain to evidence of the above-listed crime(s);
- 14 ➤ Data, documents, records, images, videos, or other items in whatever form, tending to  
15 identify the subscriber of the device, the user of the device, and/or the possessor of the  
16 device, and/or dominion and control of the device between the above-listed dates.

17 I certify under penalty of perjury under the laws of the State of Washington that the foregoing is  
18 true and correct.

19 Signed this 30<sup>th</sup> day of December, 2014, at Seattle, WA.

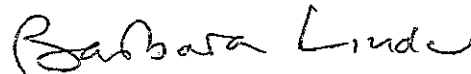
20 

21 \_\_\_\_\_  
22 Special Agent Michael J. Larson  
23 United States Department of Homeland Security  
24 Immigrations and Customs Enforcement  
25 Homeland Security Investigations

26 Subscribed and sworn to before me this 30 day of Dec, 2014.

27   
28 \_\_\_\_\_  
29 SUPERIOR COURT JUDGE

30 Issuance of Warrant Approved:<sup>1</sup>  
31 DANIEL T. SATTERBERG  
32 King County Prosecuting Attorney



33 **Approved Electronically on December 30, 2014**

34 By: Jeremy T. Lazowska, WSBA #39272  
35 Deputy Prosecuting Attorney  
36 Criminal Division

37 \_\_\_\_\_  
38 <sup>1</sup> If affiant is a Federal Agent, issuance of warrant is also requested by the signing King County Prosecuting Attorney.