

AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the
District of Colorado

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

Case No. 12-sw-05086-CBS

The Facebook account for user Horun Asrorov

APPLICATION FOR A SEARCH WARRANT

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

See Attachment A attached hereto and incorporated by reference

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

See Attachment B attached hereto and incorporated by reference

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

- [x] evidence of a crime;
[] contraband, fruits of crime, or other items illegally possessed;
[x] 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:

Table with 2 columns: Code Section, Offense Description. Row 1: Title 18, United States Code, Sections 2339A, 2339B and 956; Provision of Material Support to Terrorists; Provision of Material Support to a Designated Foreign Terrorist Organization; and, Conspiracy to Kill, Maim, or Injure Persons or Damage Property in a Foreign Country

The application is based on these facts: See Affidavit attached hereto and incorporated by reference

- [x] Continued on the attached sheet.
[] Delayed notice of \_\_\_ days (give exact ending date if more than 30 days: \_\_\_ ) is requested
under Fed. R. Crim. P. 41(f)(3) and 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Sworn to before me and signed in my presence.

Date: 2/2/12 at 11:20am

City and state: Denver, CO

Donald E. Hale, Special Agent
Applicant's signature
Printed name and title

Craig B. Shaffer, United States Magistrate Judge
Judge's signature
Printed name and title



**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to information associated with the Facebook user IDs and/or account address: Horun Asrorov that are stored at premises owned, maintained, controlled, or operated by Facebook, a company headquartered at 151 University Avenue, Palo Alto, California, 94301.

**ATTACHMENT B**

**Particular Things to be Seized**

**I. Information to be disclosed by Facebook**

To the extent that the information described in Attachment A is within the possession, custody, or control of Facebook, Facebook is required to disclose the following information to the government for each user ID and/or account address listed in Attachment A:

- (a) All contact information, including full name, user identification number, birth date, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers; and, group identification number, a list of users currently registered to the group, and Group Contact Info, including all contact information for the creator and/or administrator of the group and a PDF of the current status of the group profile page.
- (b) All Photoprints, including all photos uploaded by that user ID and all photos uploaded by any user that have that user tagged in them;
- (c) All Neoprints, including profile contact information; Mini-Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected

“Friend” requests; comments; gifts; pokes; tags; and information about the user’s access and use of Facebook applications;

- (d) All other communications and messages made or received by the user, including all private messages and pending “Friend” requests;
- (e) All IP logs, including all records of the IP addresses that logged into the account;
- (f) All information about the user’s access and use of Facebook Marketplace;
- (g) The length of service (including start date), the types of service utilized by the user, and the means and source of any payments associated with the service (including any credit card or bank account number);
- (h) All privacy settings and other account settings;
- (i) All records pertaining to communications between Facebook and any person regarding the user or the user’s Facebook account, including contacts with support services and records of actions taken.

**II. Information to be seized by the government**

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, Sections 2339A, 2339B, and 956 involving Jamshid MUHTOROV, a/k/a Abumumin Turkistony, a/k/a Abu Mumin, a/k/a Horun Asrorov, since January 1, 2009, including, for each user ID identified on Attachment A, information pertaining to the following matters:

- (a) Any evidence of threats (real or otherwise), communications, planning, financing, instruction, providing false information, hoaxes or other acts pertaining to terrorist activities.
  
- (b) Records relating to who created, used, or communicated with the user ID, including records about their identities and whereabouts.

**AFFIDAVIT**

1. I, Donald E. Hale, Special Agent (SA) assigned to the Federal Bureau of Investigation (FBI), Department of Justice, being duly sworn, hereby state:
  
2. Your affiant is a Special Agent with the FBI, having been so for approximately 9 years. I have completed the FBI's Special Agent training course at Quantico, VA. Subsequently my duties have included assignments to investigate a variety of criminal violations to include federal terrorism offenses. Your affiant currently investigates violations of federal law associated with terrorism related offenses, including material support of foreign terrorist organizations, arson and explosives crimes, firearms offenses, and other associated violations. Your affiant is authorized to carry firearms, execute warrants, make arrests for offenses against the United States, and to perform other duties as authorized by law.
  
3. This affidavit is made in support of applications for the following search warrants: (1) for a gray roller style bag; (2) for a Facebook account with the user name Horun Asrorov; (3) for two iPhones and a GPS device recovered from Jamshid MUHTOROV; (4) for the YouTube account with the "channel" horun30; and (5) for TCF Bank account number 4877241421. For the Facebook and YouTube accounts, this application seeks search warrants under Title 18, United States Code, Sections 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Facebook and YouTube to disclose to the government records and other information in their possession pertaining to the subscriber or customer associated with the accounts, including the contents of communications. These warrants

are related to an investigation into Jamshid MUHTOROV, a/k/a Abumumin Turkistony, a/k/a Abu Mumin, year of birth 1976, for potential violations of Title 18, United States Code Sections 2339A (Provision of Material Support to Terrorists), 2339B (Provision of Material Support to a Designated Terrorist Organization) and 956 (Conspiracy to Kill, Injure or Damage Property in a Foreign Country). The statements set forth in this affidavit are based upon my training and experience, consultation with other experienced investigators and agents, and investigative reports and other documents. This affidavit is intended to set forth probable cause in support of a criminal complaint and search warrants and does not purport to set forth all of the affiant's knowledge regarding the investigation.

#### **BACKGROUND**

4. The Islamic Jihad Union ("IJU", also known as al-Djihad al-Islami, Dzhamaat Modzhakhedov, and the Islamic Jihad Group of Uzbekistan) is an extremist organization that splintered from the Islamic Movement of Uzbekistan ("IMU") in the early 2000s. The IJU adheres to an anti-Western ideology, opposes secular rule in Uzbekistan, and seeks to replace the current regime with a government based on Islamic law.
5. The IJU first conducted attacks in April of 2004, targeting a popular bazaar and police at several roadway checkpoints. These attacks killed approximately 47 people, including 33 terrorists, some suicide bombers. The IJU claimed responsibility for these attacks on multiple militant Islamic websites and denounced the leadership of Uzbekistan.

6. In July 2004 the IJU conducted simultaneous suicide bombings of the US and Israeli Embassies and the Uzbekistani Prosecutor General's Office in Tashkent, Uzbekistan. In claiming responsibility for these attacks, the IJU stated that their martyrdom operations would continue. The IJU also claimed the attacks were committed in support of their Palestinian, Iraqi and Afghan brothers in the global insurgency.
  
7. In September 2007, German authorities arrested three IJU operatives, disrupting a plot against unidentified US or Western facilities in Germany. The IJU operatives had acquired about 700 kg of hydrogen peroxide and an explosives precursor, which was enough raw material to make the equivalent of about 1,200 pounds of TNT. The IJU claimed responsibility for the foiled plot.
  
8. The IJU has claimed responsibility for attacks targeting Coalition forces in Afghanistan in 2008, including a March 2008 suicide attack against a U.S. military post purportedly carried out by a German-born Turk.
  
9. In April 2009, Turkish authorities seized weapons and detained extremists with ties to the IJU. The IJU has also claimed responsibility for a May 2009 attack in Uzbekistan and numerous attacks in Afghanistan against Coalition forces. It is believed that members of both the IJU and IMU have trained with and provided support to Al Qaida.
  
10. The website [www.sodiqlar.com](http://www.sodiqlar.com) is an Uzbek language website that hosts operational claims and statements from the IJU. The website administrator for [www.sodiqlar.com](http://www.sodiqlar.com) is



known by the alias "Abu Muhammad." Public reporting shows that [www.sodiqjar.com](http://www.sodiqjar.com) is affiliated with the IJU and is suspected to be owned and operated by the IJU.

11. The Islamic Jihad Union is a designated terrorist organization, designated by the Secretary of State, and continuously designated since June 12, 2005 (under the name Islamic Jihad Group). Notification of its designation appears at 70 F. Reg. 35332-01 (June 17, 2005), amended to include name "Islamic Jihad Union" on April 29, 2008, published in the 73 F. Reg 30443-01 (May 27, 2008).

#### **FACTS OF THE CASE**

12. The FBI has been investigating Jamshid MUHTOROV based on his communications with [www.sodiqjar.com](http://www.sodiqjar.com) website administrator and Islamic Jihad Union ("IJU") facilitator "Muhammad." "Muhammad" is known as "Abu Muhammad." (Hereafter referred to as *Muhammad in this "Facts of the Case" section*) MUHTOROV communicated with Muhammad using at least two email addresses through the IJU-affiliated email address [sodiqjar@gmail.com](mailto:sodiqjar@gmail.com). MUHTOROV's two email addresses are [horun30@gmail.com](mailto:horun30@gmail.com) and [mjams3476@gmail.com](mailto:mjams3476@gmail.com). Pursuant to court authorization, the FBI obtained the email communications for both of these accounts. Additionally, pursuant to court authorization, the FBI obtained communications originating from MUHTOROV's phone lines. FBI lawful search and surveillance has shown that the email address [horun30@gmail.com](mailto:horun30@gmail.com) is associated with and used by Jamshid Muhtorov. The FBI lawfully discovered that these email accounts are regularly accessed through a Sony Vaio laptop computer with a Toshiba hard drive, serial number 600YT5PKT. Additionally,

through legally authorized methods, the FBI learned that the mobile phone used by MUHTOROV is an Android Blackberry with the telephone number (720) 775-8484.

13. On February 5, 2011, using the new email address of mjams3476@gmail.com, MUHTOROV emailed Muhammad. FBI lawful search and surveillance has shown that the email address mjams3476@gmail.com is associated with and used by Jamshid Muhtorov.
  
14. On March 8, 2011, MUHTOROV received a phone call from a known associate. MUHTOROV told the associate that the "wedding house" sends greetings. MUHTOROV then read the associate parts of a message from the IJU, calling them "our guys over there." MUHTOROV told the associate that the IJU said they need material support. MUHTOROV asked the associate if the associate remembered Juma Namangani (a founder of the IMU who was killed in 2001 in Afghanistan by a U.S. airstrike). The associate said he remembered Namangani very well. The associate then warned MUHTOROV to be careful talking about Namangani and other sensitive information while on the phone. The associate warned MUHTOROV about surveillance. Both MUHTOROV and the associate then cursed whoever might be listening in on their conversations and called upon Allah to punish those who do so.
  
15. On March 22-23, 2011, MUHTOROV updated Muhammad by email on his efforts and intentions. MUHTOROV committed himself to Bay'ah – an allegiance to the IJU. MUHTOROV told Muhammad the he [MUHTOROV] was "ready for any task, even

with the risk of dying.” [Muhammad later acknowledges that the Bay’ah has been passed on to the group leadership.]

16. On April 2, 2011, MUHTOROV emailed Muhammad and explained that an associate sent money for a “wedding gift.” Muhammad told MUHTOROV to wait, and promised to find out how the IJU wanted the money to be sent. MUHTOROV asked to be invited to the wedding, expressing his willingness to help with “the wedding” and to hear from the “master of ceremonies” about plans for “the wedding.”

17. Muhammad responded to MUHTOROV’s email on April 4, 2011 explaining that the “master of ceremonies” was busy and unable to communicate with MUHTOROV directly. On May 4, 2011, MUHTOROV wrote Muhammad saying that he was disappointed that he was not “invited to the wedding.” MUHTOROV wrote to Muhammad that even though he [MUHTOROV] was not invited to “the wedding,” he [MUHTOROV] will still travel to Istanbul before the “hot season,” and that he [MUHTOROV] will bring a “wedding gift.”

18. Based upon training and experience, your affiant knows that the term “wedding” is used as code for a terrorist event or attack. Further, your affiant knows that the practice of Bay’ah is an allegiance to a particular group or person in Islamic tradition.

19. MUHTOROV began searching online for flights from Denver to Istanbul, Turkey on May 3, 2011. Using a number of different web sites, MUHTOROV looked at a number

of one-way flights departing between June 15-17, 2011. However, he did not purchase a ticket.

20. During the months of June, July and August of 2011, MUHTOROV significantly increased the amount of hours he was working for the vehicle transport company, delivering vehicles to a number of far ranging locations including Vermont, Illinois, and Arizona.
21. On July 8, 2011, MUHTOROV told his wife Nargiza by phone that Arizona looks just like Jizzak, and that they should move there. MUHTOROV's wife laughed and said "Didn't you want to go to Turkey?"
22. On July 20, 2011, MUHTOROV's wife Nargiza called MUHTOROV and explained that she had tickets for her and their children to fly to Bishkek, Kyrgyzstan. She explained that the flight was on July 25<sup>th</sup> at 3:20 from Denver-Chicago-Istanbul-Bishkek, and asked MUHTOROV if he would be home before they left. MUHTOROV told her that he might be home, and said "Why don't you buy one more ticket to Istanbul for me?" Nargiza told him that it was too late, they already purchased their tickets. She complained "I told you we're going to buy tickets, why didn't you tell me you want to fly out too, I would've planned accordingly." MUHTOROV insisted that it was still possible for her to get a ticket for him as well. Nargiza reminded MUHTOROV that she has no money. She also commented that MUHTOROV always changes his mind. Nargiza then searched the internet for another plane ticket on the same flight she had booked with the option to get off in Istanbul. She told MUHTOROV that there was one ticket for \$988 but it was a different flight. MUHTOROV said he will not take a different flight.

23. On July 22, 2011, MUHTOROV and his wife fight during a phone call. MUHTOROV tells Nargiza Muhtorov to "choose – me [MUHTOROV] or your mother." Nargiza retorts "How about you? Didn't you want to leave us for Turkey?"
24. In a phone conversation on July 25, 2011, MUHTOROV told his young daughter that he would never see her again; but, if she was a good Muslim girl, he will see her in heaven.
25. On August 1, 2011, MUHTOROV told his father that he'll leave for his "studies" in September after his family returns.
26. MUHTOROV received an email from Muhammad on August 19, 2011 telling MUHTOROV that it was good that MUHTOROV told Muhammad about a person named "Sahwii". Muhammad asked MUHTOROV let him know if MUHTOROV had any more detailed information about "Sahwii." Muhammad also asked MUHTOROV to provide details about a person named "Talib". Muhammad told MUHTOROV that if "Talib" is bad mouthing Mujaheddin, they will have to find a way to frighten him. MUHTOROV responded by email on August 26, 2011 explaining that he hasn't seen "Talib" for a long time. MUHTOROV wrote that he scolded "Talib" really hard; and, that since then "Talib" had been keeping away. MUHTOROV also wrote that the clever answers posted on your site [sodiqlar] quieted him ["Talib"] down a lot.
27. On September 1, 2011 Muhammad sent MUHTOROV an email comparing "Sahviy" and "Talib" to viruses that erode the Islamic community from the inside while enemies attack from the outside. Muhammed continued, telling MUHTOROV that "to get rid of them,

we need an antivirus." Muhammed explained that there "are two ways antivirus cleans files -- fixes or quarantines the corrupted files, or wipes the viruses out completely." Muhammed wrote that they will try to fix "Sahviy" and "Talib", otherwise they will do jihad against them as prescribed by Allah. Muhammad told MUHTOROV that Allah permits jihad against hypocrites and ignorant people the same way the jihad against the infidels is being done. On September 4, 2011 MUHTOROV replied to Muhammad that "As for the antivirus, we have the most powerful antivirus -- the book of Allah and teachings of our Prophet, Peace be upon Him."

28. On January 3, 2012 MUHTOROV called his wife Nargiza and told her that he was leaving the United States for Istanbul, Turkey on January 15, 2012. Subsequently, MUHTOROV has continued to have conversations with Nargiza planning his impending travel. On January 6, 2012 MUHTOROV asked her to find his passport and other documents necessary for travel.
  
29. On or about January 7, 2012, MUHTOROV told an associate he was leaving the United States on January 17, 2012. MUHTOROV informed the associate that his last day at the trucking job would be January 15, 2012 and that he would return home to Colorado on that day, find his passport and then return to Chicago and fly to Istanbul, Turkey on January 17, 2012.

30. MUHOTORV resigned from his job driving trucks on or about January 1, 2012. He provided his employer with two weeks notice, indicating his last day on the job would be January 15, 2012.
31. On January 3, 2012 MUHTOROV used his phone to browse the internet for flights to Istanbul, Turkey. MUHTOROV, using the web site CheapTickets.com, focused on Turkish Airlines flight 6 leaving O'Hare Airport in Chicago, Illinois on January 18, 2012.
32. On January 16, 2012, MUHTOROV went online and purchased a ticket through CheapTickets.com on LOT Polish Airlines from Chicago, Illinois to Istanbul, Turkey. This flight is scheduled to depart on January 21, 2012 at 5:25 pm CST. The flight connects through Warsaw, Poland via Polish Airlines flight number 2, arriving in Istanbul, Turkey on Polish Airlines flight number 135.
33. On January 21, 2012, agents watched MUHTOROV as he travelled to Chicago O'Hare Airport. Agents watched MUHTOROV in possession of three pieces of luggage: a red bag with handles, a brown bag, and a dark backpack/shoulder style bag. Agents also watched MUHTOROV in possession of and using a tablet style computer device (such an iPad type tablet).
34. Upon arriving at the Chicago O'Hare Airport on January 21, 2012, agents watched MUHTOROV go to the ticket counter and check in for his flight. In addition to the aforementioned luggage (the red bag, brown bag and dark backpack/shoulder style bag),

MUHTOROV also had a gray roller style bag and a second backpack/shoulder style bag. After checking his luggage (including the red bag and gray roller) and obtaining a boarding pass, agents arrested MUHTOROV on a Criminal Complaint.

35. In searching MUHTOROV incident to arrest, agents found MUHTOROV in possession of \$2,865 in cash, the aforementioned iPad tablet, two iPhones, and a GPS device.

36. Further investigation has revealed that MUHTOROV used a Facebook account with the user name "Horun Asrorov". MUHTOROV also used a YouTube account with the user "channel" of horun30. Agents also discovered MUHTOROV opened an account at TCF Bank with the account number 4877241421.

#### **SEARCHING COMPUTERS**

37. As described above and in Attachment B for the search warrants, this affidavit is in support of an application seeking permission to search and seize records, computers, and electronic storage media (including cellular phones or other personal media devices) that have been found in Jamshid MUHTOROV's possession. Some of these electronic records might take the form of files, documents, and other data that is user-generated. Some of these electronic records, as explained below, might take a form that becomes meaningful only upon forensic analysis.

38. For example, based on knowledge, training, and experience, your affiant knows that a powered-on computer maintains volatile data. Volatile data can be defined as active



*information temporarily reflecting a computer's current state including registers, caches, physical and virtual memory, network connections, network shares, running processes, disks, floppy, tape and/or CD-ROM and printing activity. Collected volatile data may contain such information as opened files, connections to other computers, passwords used for encryption, the presence of anti-forensic tools, or the presence of programs loaded in memory that would otherwise go unnoticed. Volatile data and its corresponding evidentiary value is lost when a computer is powered-off and unplugged.*

39. *Based on knowledge, training, and experience, your affiant knows that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because 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 storage medium until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space-that is, in space on the storage medium that is not currently being used by an active file-for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.*

40. *Also, again based on training and experience, wholly apart from user-generated files, computer storage media-in particular, computers' internal hard drives-contain electronic evidence of how a computer has been used, what it has been used for, and who has used*

it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information. Data on the storage medium not currently associated with any file can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

41. As further described in Attachment B for the search warrants, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for evidence that establishes how computers were used, the purpose of their use, who used them, and when.
42. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.” The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only

overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

43. "User attribution" evidence can also be found on a computer and is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, and correspondence (and the data associated with the foregoing, such as file creation and last accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.
44. Searching computers for the evidence described in the attachment may require a range of data analysis techniques. For example, information regarding user attribution or Internet use is located in various operating system log files that are not easily located or reviewed. Or, a person engaged in criminal activity will attempt to conceal evidence of the activity by "hiding" files or giving them deceptive names. As explained above, because the warrant calls for records of how a computer has been used, what it has been used for, and who has used it, it is exceedingly likely that it will be necessary to thoroughly search storage media to obtain evidence, including evidence that is not neatly organized into files or documents. *Just as a search of a premises for physical objects requires searching the entire premises for those objects that are described by a warrant, a search of this premises for the things described in this warrant will likely require a search among the data stored in storage media for the things (including electronic data) called for by this warrant. Additionally, it is possible that files have been deleted or edited, but that*

remnants of older versions are in unallocated space or slack space. This, too, makes it exceedingly likely that in this case it will be necessary to use more thorough techniques.

45. Based upon knowledge, training and experience, your affiant knows that a thorough search for information stored in storage media often requires agents to seize most or all storage media to be searched later in a controlled environment. This is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. Additionally, to properly examine the storage media in a controlled environment, it is often necessary that some computer equipment, peripherals, instructions, and software be seized and examined in the controlled environment. This is true because of the following:

- a. The nature of evidence. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable.
- b. The volume of evidence. Storage media can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process

can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.

- c. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on-site. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
  
- d. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

46. Based on training and experience, your affiant further states that if evidence located on a computer as described on Attachment B for the search warrants appears to relate to criminal acts other than those outlined in this affidavit, those items will not be further examined unless and until a search warrant is applied for and issued for evidence of any such separate criminal acts.

## FACEBOOK ACCOUNTS

47. Facebook owns and operates a free-access social networking website of the same name that can be accessed at <http://www.facebook.com>. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written views, photographs, videos, and other information with other Facebook users, and sometimes with the general public.
48. Facebook asks users to provide basic contact information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, contact email addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites and other personal identifiers. Facebook also assigns a user identification number to each account.
49. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, to all Facebook users, or to anyone with access to the Internet, including non Facebook users. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

50. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request". If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for the purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "Mini-Feed", which highlights information about the user's "Friends", such as profile changes, upcoming events, and birthdays.

51. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host and a guest list. A particular user's profile page also includes a "Wall", which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

52. Facebook has a Photos application, where users can upload an unlimited number of albums and photos. Another feature of the Photos application is the ability to "tag" (i.e. label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook's purposes, a user's "Photoprint" includes all photos uploaded by that user that

have not been deleted, as well as all photos uploaded by any user that have that user tagged in them.

53. Facebook users can exchange private messages on Facebook with other users. These messages, which are similar to email messages, are sent to the recipient's "Inbox" on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile.
54. Facebook Notes is a blogging feature available to Facebook users, and it enable susers to write and post notes or personal web logs (blogs), or import their blogs from other services, such as Xanga, LiveJournal and Blogger.
55. The Facebook Gifts feature allows users to send virtual gifts to their friends that appear as icons on the recipient's profile page. Gifts cost money to purchase, and a personalized message can be attached to each gift. Facebook users can also send each other "pokes," which are free and simple result in a notification to the recipient that he or she has been "poked" by the sender.
56. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items in the Marketplace.



57. In addition to the applications described above, Facebook also provided users with access to other applications on the Facebook platform. When a Facebook user accesses or used one of these platforms, an update about the user's use of that application may appear on the user's profile page.

58. Some Facebook pages are affiliated with groups of users, rather than one individual user. Membership in the group is monitored and regulated by an administrator, or head of the group, who can invite new members or reject or accept requests by users to enter. Facebook can identify all users who are currently registered to a particular group and can identify the creator of the group. Facebook also assigns a group identification number to each group. Facebook uses the term "Group Contact Info" to describe the contact information for the group's creator and/or administrator.

59. Facebook uses the term "Neoprint" to describe an expanded view of a given user profile. The Neoprint for a given user can include the following information from the user's profile: profile contact information; MiniFeed information; status updates; links to videos, photos, articles or other items; Notes; Wall postings; friend lists, including friends' user identification numbers; groups and networks of which the user is a member; group identification numbers; future and past event postings; rejected "friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications.

60. Facebook also retains Internet Protocol (“IP”) logs for a given user ID or IP address.

These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, date and time of the action, and the user ID and IP address associated with the action.

61. Social networking providers like Facebook typically retain additional information about their users’ accounts, such as information about the length of service (including start date), types of service utilized, and the means and source of any payments associated with the service. In some cases, users may communicate directly with Facebook about issues related to their account, such as technical problems or complaints from other users. Social networking providers typically retain records about such communications, including records of contact with users.

62. Therefore, the computers of Facebook are likely to contain all the material described, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information and account application.

### **CONCLUSION**

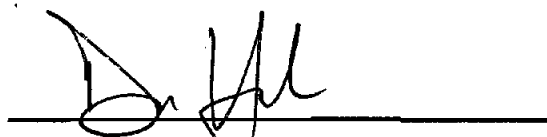
63. Based upon the foregoing, your affiant believes there is probable cause to issue search warrants: (1) for a gray roller style bag; (2) for a Facebook account with the user name Horun Asrorov; (3) for two iPhones and a GPS device recovered from Jamshid

MUHTOROV; (4) for the YouTube account with the "channel" horun30; and (5) for TCF Bank account number 4877241421.

64. Specifically as to the Facebook and YouTube warrants, it is anticipated that they will be executed under the Electronic Communications Privacy Act, in particular Title 18, United States Code, Sections 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Facebook and YouTube to disclose to the government copies of the records and other information (including the content of communications) particularly described in Attachment B. This Court has jurisdiction to issue the requested warrants for these accounts because it is a "court of competent jurisdiction" as defined by Title 18, United States Code, Section 2711. Specifically, the Court is a district court of the United States ... that - has jurisdiction over the offense being investigated. 18 U.S.C. Section 2711(3)(A)(i).

65. Pursuant to Title 18, United States Code, Section 2703(g), the presence of a law enforcement officer is not required for the service or execution of the Facebook or YouTube account warrants.

**I, Donald E. Hale, being duly sworn according to law, depose and say that the facts stated in the foregoing affidavit are true and correct to the best of my knowledge, information and belief.**

A handwritten signature in black ink, appearing to read "D. Hale", is written over a solid horizontal line.

**Donald E. Hale, Special Agent**

**Federal Bureau of Investigation, Joint Terrorism Task Force**

Sworn to and subscribed before me this 29 day of February, 2012.



**UNITED STATES MAGISTRATE JUDGE**  
**UNITED STATES DISTRICT COURT**  
**DISTRICT OF COLORADO**