

AO 91 (Rev. 02/09) Criminal Complaint

UNITED STATES DISTRICT COURT
for the
District of Colorado

United States of America)
v.)
1. BAKHTIYOR JUMAEV,)
_____)
Defendant

Case No. 12-mj-01039-KLM

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date of 03/08/2011 in the county of Denver in the State and District of Colorado, the defendant violated 18 U. S. C. § 2339B, an offense described as follows:

See Attachment A attached hereto and herein incorporated by reference

This criminal complaint is based on these facts:

See Affidavit attached hereto and herein incorporated by reference

Continued on the attached sheet.



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

Sworn to before me and signed in my presence.

Date: 03/14/2012



Judge's signature

City and state: Denver, CO

KRISTEN L. MIX
Printed name and title
U.S. MAGISTRATE JUDGE
DISTRICT OF COLORADO

ATTACHMENT A

Bakhtiyor Jumaev, the defendant herein, together with others both known and unknown but not charged herein; did knowingly conspire, combine, confederate, cooperate and agree with each other to provide material support and resources, in violation of Title 18, United States Code, Section 2339(a)(1), to a foreign terrorist organization, namely the Islamic Jihad Union, and the Islamic Jihad Union was continuously designated a terrorist organization since June 12, 2005 as amended April 29, 2008, knowing that this organization had engaged in and was engaging in terrorist activity and terrorism; and the offense occurred in whole or in part within the United States; and further there was interdependency among the members of the conspiracy.

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 a criminal complaint alleging that Bakhtiyor JUMAEV, a/k/a Abu Bakr, year of birth 1966, violated Title 18, United States Code Section 2339B, Conspiracy to Provide Material Support to a Designated Terrorism Organization, specifically the Islamic Jihad Union ("IJU"). This affidavit is also in support of three search warrants: (1) for a residence located at 3131 Richmond Street, Philadelphia, Pennsylvania; (2) any and all computers (including portable computer devices) located at 3131 Richmond Street, Philadelphia, PA 19134, to include a Sony Vaio laptop computer, model number VGN-F8690, service tag of R5170004, and (3) for a T-Mobile cellular telephone assigned telephone number (267) 597-1321. 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 the criminal complaint and search warrants and does not purport to set forth all of the affiant's knowledge regarding the investigation. All conversations set forth in this affidavit are related in substance and in part.

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 IMU was founded by Tohir Yuldashev and Juma Namangani in or around 1998. The IJU is believed to have split from the Islamic Movement of Uzbekistan (IMU) in late 2001 shortly after the death of Namangani. 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, and 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 U.S. and Israeli Embassies and the Uzbekistani Prosecutor General's Office in Tashkent. 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 U.S. 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 the explosive, 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 is an Uzbek language website that hosts operational claims and statements from the IJU. The website administrator for www.sodiqlar.com is known by the alias "Abu Muhammad." Public reporting shows that [sodiqlar.com](http://www.sodiqlar.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

Conspiracy to Provide Material Support to the IJU

12. The FBI has been investigating Jamshid MUHTOROV based on his communications with Islamic Jihad Union ("IJU") website administrator and facilitator "Muhammad." "Muhammad" is known as "Abu Muhammad."
13. The FBI has also been investigating JUMAEV, a close friend of MUHTOROV. JUMAEV provided his mobile telephone number, (267) 597-1321, to the Department of Homeland Security Immigration and Customs Enforcement after being arrested for immigration charges in February 2010. Upon obtaining appropriate authority, the FBI has lawfully searched and obtained information through various investigative techniques. As a result the FBI has been able to determine that the mobile phone used by JUMAEV is a T-Mobile mobile phone. Moreover, there exists incriminating communications originating from JUMAEV's mobile phone, many of which are set forth below. The FBI has also determined that JUMAEV resides at 3131 Richmond Street, Philadelphia, Pennsylvania, and that he has kept a Sony Vaio laptop computer, model number VGN-F8690, service tag of R5170004 at that residence.

14. On or about March 5, 2011, MUHTOROV emailed Abu Muhammad and stated that he delivered Abu Muhammad's hello to JUMAEV. MUHTOROV stated that JUMAEV was very happy and sent many greetings to Abu Muhammad as well. MUHTOROV stated that JUMAEV promised to send money to Abu Muhammad and the IJU through MUHTOROV.

15. On or about March 6, 2011, Abu Muhammad emailed MUHTOROV and instructed him [MUHTOROV] to say hello to the brothers again, and asked that Allah accept their deeds. Abu Muhammad told MUHTOROV that the IJU was in desperate need of money at the moment. Abu Muhammad repeated that the brothers say hello to all of you.

16. On or about March 8, 2011, MUHTOROV received a phone call from JUMAEV. MUHTOROV read JUMAEV parts of a message from the IJU, calling them the "brothers from the wedding house." MUHTOROV told JUMAEV that the "brothers from the wedding house are saying hi to you again." MUHTOROV told JUMAEV that "they say to you - may Allah accept the associations you made on the way of Allah." MUHTOROV told JUMAEV that the IJU said they need support. JUMAEV told MUHTOROV that help will go to them and that it will not be the first time, nor will it be the last time.

17. During the same conversation on March 8, 2011, JUMAEV asked MUHTOROV is this "the group of our brother?" MUHTOROV told JUMAEV "it is the second group." In order to clarify, MUHTOROV asked JUMAEV if he remembered Juma Namangani. JUMAEV said he remembered Namangani very well. MUHTOROV told JUMAEV that

it is the people of that brother, who after the martyrdom of Namangani started their own group. In response, JUMAEV agrees and tells MUHTOROV that they are with this group. JUMAEV then warned MUHTOROV to be careful talking about Namangani and other sensitive information while on the phone. JUMAEV warned MUHTOROV about surveillance. Both MUHTOROV and JUMAEV then cursed whoever might be listening in on their conversations and called upon Allah to punish those who do so. JUMAEV told MUHTOROV that if he sends "it" tomorrow, then he should get "it" by Friday.

18. On or about March 16, 2011, MUHTOROV received a call from JUMAEV. JUMAEV told MUHTOROV about an article he had recently read at the ferghana.ru website. According to JUMAEV, the article concerns the capture of two members of sodiqlar.com. JUMAEV refers to them as two "second rate sportsmen." JUMAEV additionally states that he hopes it is not true and that it is just one of the tricks "they use to destroy our faith." JUMAEV informed MUHTOROV of difficulties he experienced in accessing the sodiqlar.com website, but JUMAEV confirmed that he is able to access furqon.com. JUMAEV and MUHTOROV also discuss cell phones. MUHTOROV asked whether a new phone would work at "the wedding house" in case MUHTOROV travels there. JUMAEV stated that this issue should be confirmed with "the sportsmen brothers."

19. On or about March 22-23, 2011, MUHTOROV updated Muhammad 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 acknowledged having passed on MUHTOROV’s *Bay’ah* to the IJU leadership.

20. On or about July 12, 2011, during a telephone conversation, MUHTOROV told JUMAEV that “the wedding hosts” from “the wedding house” are concerned that Muhtorov had not arrived. MUHTOROV stated that he told them that he will come to “the wedding.” JUMAEV told MUHTOROV that he received a letter to be fingerprinted in order to obtain his work authorization, but he was not excited because he did not really want to stay in the United States. JUMAEV stated that he wanted to join “the wedding” like MUHTOROV and that he envied MUHTOROV. JUMAEV said that if he [JUMAEV] went to “the wedding,” then upon his arrival MUHTOROV could come to meet him. MUHTOROV agreed.

21. On or about July 15, 2011, during a telephone conversation MUHTOROV told JUMAEV that the brothers from the “wedding house” say hi to you. JUMAEV then asked MUHTOROV to send his [JUMAEV’s] best wishes to them.

22. On or about October 9, 2011, JUMAEV told MUHTOROV that a known associate warned him [JUMAEV] not to have any sincere conversations on the phone or over the internet. JUMAEV stated that all communications were being monitored. MUHTOROV agreed with JUMAEV, noting that authorities know everything being said on the phone.

23. On or about October 28, 2011, during a telephone conversation, MUHTOROV explained that religious restriction toward Muslims in the western world will get only worse. MUHTOROV cited a restriction on *Sharia* (Islamic law) somewhere in Denmark.

JUMAEV stated that Western countries allow one to do anything in terms of lifestyle and business except for being a Sunni extremist. JUMAEV explained that he watched a video of the *mujahidin* (holy warriors) in the Afghanistan/Pakistan region and that he cried some, laughed some, and prayed some. JUMAEV said that he took advice from the videos and explained that the *mujahidin* are in another world and are the dear ones.

24. Between March 2011 and January 2012, during telephone conversations, JUMAEV and MUHTOROV utilized several different code words to discuss IJU activities, IJU videos on the internet, and MUHTOROV's intent to travel overseas to join the IJU.

25. On or about December 2, 2011, JUMAEV called a known associate and told him that they better meet sooner rather than later, as the associate may not see JUMAEV in this world anymore. JUMAEV says that they would see each other in the other world, but in this world they cannot be certain.

26. On or about January 7, 2012, during a telephone conversation, JUMAEV and MUHTOROV discussed MUHTOROV's inability to find his passport. Using code, JUMAEV stated that MUHTOROV will not be able to join the IJU if he does not find the passport. JUMAEV states that there is so much to discuss with MUHTOROV, but they cannot speak freely on the phone.

27. On or about January 21, 2012, MUHTOROV was arrested on a federal warrant at O'Hare International Airport while attempting to travel overseas. MUHTOROV was arrested based on a violation of Title 18, United States Code Section 2339B: Provision of Material Support to a Designated Terrorist Organization, specifically provision and attempted

provision of personnel to the IJU. MUHTOROV was carrying approximately \$2,800 in cash when he was arrested. Immediately following his arrest MUHTOROV was interviewed by the FBI. During the interview MUHTOROV admitted to communicating with Abu Muhammad at the sodiqlar.com web site. MUHTOROV stated that sodiqlar.com is the website for the IJU, a combat organization that fights NATO forces in Afghanistan, to include U.S. forces. MUHTOROV also described the IMU as another Uzbek terrorist organization.

28. On or about January 24, 2012, during a telephone conversation with a known associate, JUMAEV discussed the arrest of MUHTOROV. JUMAEV stated that MUHTOROV's phone will be checked and that JUMAEV's name will come up. JUMAEV told the associate that he is consulting with him to coordinate the story they will tell authorities should they interview them. JUMAEV stated that they should be on the same page when asked about MUHTOROV.

29. On or about January 25, 2012, YouTube records were obtained from Google, Inc. for JUMAEV's YouTube account. These records display that JUMAEV has commented on approximately eight YouTube videos since on or about July 27, 2011. Several of the videos contained violent action by terrorists and featured footage of the IMU co-founder Yuldashev. Many of JUMAEV's comments espoused support for the terrorists and/or Yuldashev. For example, on or about July 27, 2011, JUMAEV posted a comment on an approximately 10 minute video showing several males in traditional Islamic dress, in a mountain region that appears to be Afghanistan or Pakistan, carrying rifles, and firing rockets and other weaponry. The video indicated that it was produced by Jundullah

Studios, which according to open source reports is the official media wing of the IMU.

In response to the video, JUMAEV left a comment encapsulating a desire for Allah to be pleased with these individuals.

30. Based upon training and experience, your affiant knows that the term “wedding” or “wedding activities” in the instances above is used as code for terrorist activities, terrorist events or terrorist attacks.

Overt Acts in Furtherance of the Conspiracy

31. On or about March 5, 2011, MUHTOROV emailed Abu Muhammad and stated that he delivered Abu Muhammad’s hello to JUMAEV. MUHTOROV stated that JUMAEV was very happy and sent many greetings to Abu Muhammad as well. MUHTOROV stated that JUMAEV promised to send money, \$300, to Abu Muhammad and the IJU through MUHTOROV.
32. On or about March 8, 2011, in a lengthy conversation discussing support for the “second group” of Juma Namangani (i.e., the IJU), JUMAEV told MUHTOROV that if he sends “it” tomorrow, then MUHTOROV should get “it” by Friday.
33. On or about March 15, 2011, JUMAEV called MUHTOROV. JUMAEV asked MUHTOROV whether he received the “wedding gift,” which JUMAEV sent last week. MUHTOROV replied that he had not received it yet, but that he had not yet checked his mail.

34. On or about April 2, 2011, MUHTOROV emailed Muhammad and explained that a brother sent me \$300 as a “wedding gift” for you. Muhammad told MUHTOROV that he would 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.”

35. Bank records have been obtained which display that a \$300 check dated on or about March 10, 2011 was made out to MUHTOROV by a known associate of JUMAEV. The check was thereafter cashed by MUHTOROV’s wife on or about April 8, 2011. FBI investigation determined that the associate had a close relationship with JUMAEV. Moreover, JUMAEV has previously used the associate’s name to register for utility services. For example, JUMAEV’s home telephone and internet service at 3131 Richmond Street, Philadelphia, Pennsylvania is registered under the associate’s name, despite the associate not being a resident of 3131 Richmond Street.

36. On January 21, 2012, MUHTOROV was arrested at Chicago O’Hare International Airport, carrying, amongst other things, about \$2,800 in U.S. currency.

37. On or about February 14, 2012 and on or about February 24, 2012, JUMAEV was interviewed by the FBI at his residence. During the interviews, JUMAEV stated that he was friends with MUHTOROV and he had communicated with MUHTOROV utilizing his T-Mobile mobile phone and a computer program known as Skype. During the

interview, FBI agents observed a Sony Vaio laptop computer in JUMAEV's residence with the Skype application running. JUMAEV confirmed that he had no roommates and was the only person residing at 3131 Richmond Street. JUMAEV confirmed that he had known of the IMU and the IJU since at least 2005 and that he had been aware since President Bush's presidency (some time prior to 2008) that both groups were designated terrorist organizations. He also stated that that he knew that both the IMU and IJU were fighting U.S. soldiers in Afghanistan. JUMAEV acknowledged that he knew that it was illegal to send any financial support to either the IMU or IJU. JUMAEV stated that the names Yuldashev and Namangani were synonymous with the IMU and that assisting either of them would mean that you would be assisting the IMU. JUMAEV denied he sent money to the IMU or IJU. JUMAEV confirmed however that he had sent a \$300 check to MUHTOROV by using a known associate's checking account on or about March 10, 2011. JUMAEV stated that it was his handwriting on the check and that he personally mailed the check to MUHTOROV. JUMAEV claimed that the \$300 was repayment of a debt.

38. Your Affiant has applied his experience and knowledge to the evidence gathered during the aforementioned investigation to conclude that JUMAEV conspired with MUHTOROV to provide money to the IJU while knowing that the IJU was a terrorist organization. The conversations between JUMAEV and MUHTOROV, as well as the conversations between MUHTOROV and Muhammad, display that JUMAEV sent \$300 to MUHTOROV through a known associate. This was confirmed by JUMAEV himself. The \$300 represents the money that MUHTOROV told Muhammad that a brother

promised to send to him [Muhammad] and the IJU on March 5, 2011. The conversations between MUHTOROV and JUMAEV establish that JUMAEV is aware of the IJU as well as the fact that they are engaged in terrorist behavior. This was also confirmed by JUMAEV himself. The conversations between JUMAEV and MUHTOROV also display an agreement to provide help to the IJU. The \$300 represents material support that JUMAEV attempted to provide to the IJU through MUHTOROV. MUHTOROV told Muhammad about JUMAEV's intent to send money on March 5, 2011, JUMAEV stated he would send the money to MUHTOROV on March 8, 2011, and JUMAEV confirmed that he had sent the money to MUHTOROV on March 15, 2011.

SEARCHING COMPUTERS

39. As described above and in Attachment B, 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 might be found at Bakhtiyor JUMAEV's residence, located at 3131 Richmond Street, Philadelphia, Pennsylvania or within Bakhtiyor JUMAEV'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.

40. 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.

41. 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.

42. 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.

43. As further described in Attachment B, 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.

44. 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.

45. "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.
46. 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.

47. 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:

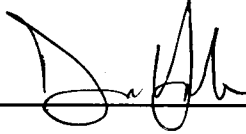
- a. The nature of evidence. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could 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.

48. Based on training and experience, your affiant further states that if evidence located on a computer as described on Attachment B 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.

49. Based upon the foregoing, your affiant believes there is probable cause to search: (1) the residence located at 3131 Richmond Street, Philadelphia, Pennsylvania; (2) any and all computers (including portable computer devices) located at 3131 Richmond Street, Philadelphia, PA 19134, to include a Sony Vaio laptop computer, model number VGN-F8690, service tag of R5170004, and (3) a T-Mobile cellular telephone assigned telephone number (267) 597-1321.

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.



Donald E. Hale, Special Agent

Federal Bureau of Investigation, Joint Terrorism Task Force

Sworn to and subscribed before me this 14th day of March, 2012.



UNITED STATES MAGISTRATE JUDGE

UNITED STATES DISTRICT COURT

DISTRICT OF COLORADO