

UNITED STATES DISTRICT COURT

for the
District of ColoradoIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)Yahoo! Inc.
701 First Avenue
Sunnyvale, CA 94089

Case No.

10-sw-5056-MEH
-BATB

APPLICATION FOR A SEARCH WARRANT

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

The email addresses described in Attachment A, which are in the possession of or under control of Yahoo! Inc., 701 First Avenue, Sunnyvale, CA 94089.

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized):

See Attachment B, which is attached and incorporated in the Application and Affidavit.

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

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of _____ 18 _____ U.S.C. § _____ 1037(a)(4) _____, and the application is based on these facts:

The facts to support a finding of probable cause for issuance of a search warrant are set forth in the affidavit of FBI Special Agent Jason Myszkiewicz, which is attached hereto and incorporated herein.

☒ Continued on the attached sheet.

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

Jason Myszkiewicz FBI SA
Applicant's signature

Jason Myszkiewicz, Special Agent, Federal Bureau of Investigation
Printed name and title

Sworn to before me and signed in my presence.

Date:

1/25/2010

Michael E. Hegarty
Judge's signature

City and state:

Michael E. Hegarty
United States Magistrate Judge
Denver, Colorado

Printed name and title

ATTACHMENT A

DESCRIPTION OF LOCATION TO BE SEARCHED

The following e-mail accounts which are in the possession of or under the control of the E-mail and Internet Service Provider YAHOO! INC. whose office is located at 701 First Avenue, Sunnyvale, California 94089:

abadilladebbie@yahoo.com
abbittmanuel@yahoo.com
abbottbrendaa@yahoo.com
abrahamheathr@yahoo.com
allan.merida@yahoo.com
angelabadq95@yahoo.com
azucenabustmante@yahoo.com
baltazarloza@yahoo.com
beverlyburnett19@yahoo.com
billijilli@yahoo.com
bowergary@yahoo.com
brandonharris_23@yahoo.com
castillkim@yahoo.com
chandraabakah@yahoo.com
cherylabdu@yahoo.com
craftdona@yahoo.com
cynthiabledsoe_14@yahoo.com
dancabral_14@yahoo.com
deborah_kepner@yahoo.com
delwahab@yahoo.com
dennbelly@yahoo.com
elenachavez19@yahoo.com
florencioaffholder@yahoo.com
gingsdidley@yahoo.com
grt.tony@yahoo.com
hintonal_8@yahoo.com
huppmarkk@yahoo.com
james2548798@yahoo.com
jennettlaura@yahoo.com
johnabate5@yahoo.com
jonathanabdelwahab@yahoo.com
jonmike43@yahoo.com
karelagudelo@yahoo.com

knowles.donna@yahoo.com
maryedmonds23@yahoo.com
meitousanser@yahoo.com
mujidatabbott@yahoo.com
nanrodriguez17@yahoo.com
peeleralice@yahoo.com
riendeaumaurence@yahoo.com
robertgirififth@yahoo.com
robertyson_21@yahoo.com
rushbrian_03@yahoo.com
sharonabdelhaq@yahoo.com
smithtina_25@yahoo.com
stapleton.donna@yahoo.com
veronicahill_07@yahoo.com
wardale_18@yahoo.com
williamlundbohum@yahoo.com
wisebenny_30@yahoo.com

ATTACHMENT B
ITEMS TO BE SEARCHED AND SEIZED

Pursuant to 18 U.S.C. § 2703, YAHOO! INC. whose office is located at 701 First Avenue, Sunnyvale, California 94089 (the PROVIDER) is hereby ordered as follows:

I. SEARCH PROCEDURE

a. The search warrant will be presented to personnel of the PROVIDER, who will be directed to isolate those accounts and files described in Section II below;

b. In order to minimize any disruption of computer service to innocent third parties, the PROVIDER'S employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the computer accounts and files described in Section II below, including an exact duplicate of all information stored in the computer accounts and files described therein;

c. The PROVIDER'S employees will provide the exact duplicate in electronic form of the accounts and files described in Section II below and all information stored in those accounts and files to the agent who serves the search warrant; and

d. Law enforcement personnel will thereafter review all information and records received from the PROVIDER'S employees to determine the information to be seized by law enforcement personnel specified in Section III.

**II. FILES AND ACCOUNTS TO BE COPIED BY THE PROVIDER'S
EMPLOYEES**

a. All electronic mail stored and presently contained in, or on behalf of, subscribers, including but not limited to the accounts associated with the e-mail addresses identified in Attachment A ("SUBJECT ACCOUNTS") including received messages, sent messages, deleted messages, and messages maintained in trash or other folders;

b. All existing printouts from original storage of all of the electronic mail described above in Section II(a);

c. All transactional information of all activity of the SUBJECT ACCOUNTS described above in Section II(a), including log files, dates, times, methods of connecting, ports, dial-ups, and/or locations;

d. All business records and subscriber information, in any form kept, pertaining to the SUBJECT ACCOUNTS described above in Section II(a), including applications, subscribers' full names, all screen names associated with the subscribers and/or accounts, all account names associated with the subscribers, methods of payment, telephone numbers, addresses, and detailed billing records; and

e. All records indicating the services available to subscribers of the SUBJECT ACCOUNTS described above in Section II(a).

**III. INFORMATION TO BE SEIZED BY LAW ENFORCEMENT
PERSONNEL**

a. The following electronic mail, attachments and related computer files and account information regarding the SUBJECT ACCOUNTS from **September 1, 2008** to the date of the execution of the search warrant -- which constitute evidence and instrumentalities of violations of Title 18, United States Code, Section 1037(a)(4)— prohibiting the registration of five or more electronic mail accounts or two or more domain names with information falsely identifying the actual registrant in connection with transmitting multiple commercial electronic mail messages:

1. All electronic mail, attachments and related computer files that identify the account user, individuals or correspondents engaged in the transmission of commercial electronic mail messages, that identifies the means or methods used regarding such transmission or other violations of Title 18, United States Code, Section 1037;
2. All electronic mail, attachments and related computer files that evidences or identifies the means of payment or financing the transmission of commercial electronic mail messages or other violations of Title 18, United States Code, Section 1037;
3. All "address books" or other lists of correspondents.
4. All saved "chat" transcripts that identify the transmission of commercial electronic mail messages and/or violations of 18 U.S.C. § 1037;
5. All of the records and information described above in Sections II(c), (d), and (e), including:

- a. Names and associated e-mail addresses; physical address and location information; records of session times and durations; length of service (including start date) and types of service utilized; telephone or instrument

number or other subscriber number or identity, including any temporarily assigned network address; the means and source of payment for such service (including any credit card or bank account number); and Internet Protocol addresses used by the subscriber to register the account or otherwise initiate service.

- b. User connection logs for the SUBJECT ACCOUNTS for any connections to or from the SUBJECT ACCOUNTS which should include the following:
Connection time and date; disconnect time and date; method of connection to system (e.g., SLIP, PPP, Shell); data transfer volume (e.g., bytes); the IP address that was used when the user connected to the service, connection information for other systems to which user connected via the SUBJECT ACCOUNTS; and any address to which the wire or electronic mail was or is to be forwarded from the SUBJECT ACCOUNTS or e-mail address.

IV.PROVIDER PROCEDURES

- a. The PROVIDER shall deliver the information set forth above within **10 days** of the service of this warrant and the PROVIDER shall send the information via facsimile or United States mail, and where maintained in electronic form, on CD-ROM or an equivalent electronic medium, to:

Special Agent J. A. Myszkiewicz
FBI – Denver Field Office
1961 Stout Street, Suite 1823
Denver, Colorado 80294

- b. Pursuant to 18 U.S.C. § 2703(g) the presence of an agent is not required for service or execution of this warrant.

AFFIDAVIT

I, J. A. Myszkiewicz, being duly sworn, hereby depose and state the following:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have held the position for two and a half years. I am currently assigned to a Computer Crime squad, wherein my duties and responsibilities include the investigation of criminal violations involving fraud and related activity in connection with commercial electronic mail, including Title 18, United States Code, Section 1037(a)(4) (prohibiting the registration of five or more electronic mail accounts or two or more domain names with information falsely identifying the actual registrant in connection with transmitting multiple commercial electronic mail messages). Prior to joining the FBI, I had eight years of professional work experience in the technology industry where I was responsible for such tasks as computer and website programming, database development, and systems administration.
2. This affidavit is in support of an application for a warrant to search the e-mail accounts identified in Attachment A ("SUBJECT ACCOUNTS"), there being probable cause to believe that in the SUBJECT ACCOUNTS are evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 1037(a)(4)(as more particularly described on Attachment B).
3. The information contained within the affidavit is based on my training and experience, as well as information imparted to me by other law enforcement officers involved in this investigation. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this

investigation but have set forth only the facts that I believe are necessary to establish probable cause that evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 1037(a)(4) *et. seq.*, are present at the location described.

RELEVANT STATUTES

4. This investigation concerns alleged violations of 18 U.S.C. Section 1037(a)(4), relating to commercial electronic mail messages.
5. 18 U.S.C. Section 1037(a) provides: “Whoever, in or affecting interstate or foreign commerce, knowingly” – (4) “registers, using information that materially falsifies the identity of the actual registrant, for five or more electronic mail accounts or online user accounts or two or more domain names, and intentionally initiates the transmission of multiple commercial electronic mail messages from any combination of such accounts or domain names “[shall in violation of law].
6. 18 U.S.C. Section 1037(d)(3) defines “Multiple” as “more than 100 electronic mail messages during a 24-hour period, more than 1,000 mail electronic mail messages during a 30-day period, or more than 10,000 electronic mail messages during a 1-year period.”

DEFINITIONS

7. The following additional definitions apply to this Affidavit and Attachment B to this Affidavit.
8. Domain name: Used within e-mail, web, and other addresses to identify an organization on the Internet. For example, the domain name of the addresses <http://www.gmail.com/> and john DOE@gmail.com would be gmail.com.
9. DomainTools (www.domaintools.com): A private company which retains historical WHOIS

and hosting records.

10. E-mail address: An e-mail address is composed of a user name and a domain name. The address uses the format “<user name>@<domain name>,” e.g. johndoe@gmail.com.
11. Google Apps: A Google service for using custom domain names with several Google products, including e-mail receipt and storage. For example, a user could create a custom Google Apps domain name, such as “customdomain.com” and multiple e-mail addresses associated with that domain, such as johndoe@customdomain.com. Any e-mail sent to johndoe@customdomain.com would be received by a server owned and maintained by Google and stored on that server. This service allows users and small companies to offload the burden of server management to Google for free or for a nominal cost, depending on the specific account type. Google Apps, through its “Google Docs” service also allows users to store and edit documents online. These documents are stored on Google’s servers.
12. Hosting company / records: A company that sells space on their servers to a lessee. The hosting company generally owns the physical computers and any space / overhead associated with those computers. The lessee pays to use these resources for various purposes. In most cases, the lessee can configure the servers for a variety of uses, such as data storage, transmission of e-mail, or hosting of websites. A hosting record contains information which associates a hosting company with a server or IP address.
13. Proxy server: An intermediary server that accepts requests from clients (such as a Web browser) and forwards them to other proxy servers, the origin server, or services (such as a Web site). A proxy server could be used to conceal a client's true source IP address and location in order to “anonymize” or obfuscate a user’s visit to a Web site. For example, a

proxy server could be used by an individual in India to make it appear that the individual is located in the United States.

14. User name: Used within e-mail addresses to define a specific individual, group, or entity.

For example, the user name of the address johndoe@gmail.com would be johndoe.

15. WHOIS: A service used for querying databases in order to determine the registrant or assignee of Internet resources, such as a domain name or IP address. The service is free, open to the public, and is accessible through various websites and tools. Information about a registrant usually includes organization (if applicable), name, address, telephone number, and e-mail address. The information is reported by the registrant and is generally not verified or authenticated.

BACKGROUND REGARDING THE INTERNET

16. As part of my training, I have become familiar with the Internet (also commonly known as the World Wide Web), which is a global network of computers and other electronic devices that communicate with each other using various means, including standard telephone lines, high-speed telecommunications links (e.g., copper and fiber optic cable), and wireless transmissions, including satellite. Due to the structure of the Internet, connections between computers on the Internet routinely cross state and international borders, even when the computers communicating with each other are in the same state. Individuals and entities use the Internet to gain access to a wide variety of information; to send information to, and receive information from, other individuals; to conduct commercial transactions; and to communicate via electronic mail ("e-mail"). An individual who wants to use Internet e-mail must first obtain an account with a computer that is linked to the Internet – for example,

through a university, an employer, or a commercial service – which is called an “Internet Service Provider” or “ISP” (see definition of “Internet Service Provider” below). Once the individual has accessed the Internet, that individual can use an e-mail account provided by their ISP or they can use the Internet to connect to web-based e-mail services (such as those provided by America Online and Microsoft Hotmail) to send and receive e-mail. Web-based e-mail services provide e-mail accounts that may be accessed from any computer that has access to the world wide web. In addition, the individual can access websites using web browsers (computer programs that permit users to navigate through pages of information that are stored on remote computers, such as Microsoft’s Internet Explorer and Mozilla’s Firefox) to view or download content, or make purchases. The Internet may also be used to access e-groups (websites that require users to subscribe, and permit subscribers to post messages, chat electronically, post and transfer files and share information), newsgroups (that permit posting of e-mail messages regarding specific topics) and video conferencing.

17. E-mail Provider:

- a. In my training and experience, I have learned that YAHOO! provides a variety of on-line services, including electronic mail (“e-mail”) access, to the general public. Subscribers obtain an account by registering with YAHOO! During the registration process, YAHOO! asks subscribers to provide basic personal information. Therefore, the computers of YAHOO! are likely to contain stored electronic communications (including retrieved and unretrieved e-mail for YAHOO! subscribers) and information concerning subscribers and their use of YAHOO! services, such as account access information, e-mail transaction information, and account application

information.

- b. In general, an e-mail that is sent to a YAHOO! subscriber is stored in the subscriber's "mail box" on YAHOO! servers until the subscriber deletes the e-mail, or until a preservation letter is sent to the e-mail provider. If the subscriber does not delete the message, or if the e-mail provider preserves the content of the account pursuant to a preservation letter, the message can remain on YAHOO! servers indefinitely.
- c. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to servers maintained by YAHOO!, and then transmitted to its end destination. YAHOO! often saves a copy of the e-mail sent. Unless the sender of the e-mail specifically deletes the e-mail, or if the e-mail provider preserves the content of the account pursuant to a preservation letter, the e-mail can remain on the system indefinitely.
- d. YAHOO! subscribers can also store files, including e-mails, address books, contact or buddy lists, pictures, and other files, on servers maintained and/or owned by YAHOO!

18. Internet Service Providers ("ISPs"):

- a. ISPs are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line (DSL) or cable television,

dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, that the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an “e-mail address,” an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and personal password.

- b. ISPs maintain records (“ISP records”) pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often times in the form of log files), e-mail communications, information concerning content uploaded and/or stored on or via the ISP’s servers, and other information, which may be stored both in computer data format and in written or printed record format. ISPs reserve and/or maintain computer disk storage space on their computer system for their subscribers’ use. This service by ISPs allows for both temporary and long-term storage of electronic communications and many other types of electronic data and files. Typically, e-mail that has not been opened by an ISP customer is stored temporarily by an ISP incident to the transmission of that e-mail to the intended recipient, usually within an area known as the home directory. Such temporary, incidental storage is defined by statute as “electronic storage,” see 18 U.S.C. § 2510(17), and the provider of such a service is

an “electronic communications service.” An “electronic communications service,” as defined by statute, is “any service which provides to users thereof the ability to send or receive wire or electronic communications. 18 U.S.C. § 2510(15). A service provider that is available to the public and provides storage facilities after an electronic communication has been transmitted and opened by the recipient, or provides other long term storage services to the public for electronic data and files, is defined by statute as providing a “remote computing service.” 18 U.S.C. § 2711(2).

19. **Internet Protocol Address (IP Address):** Every computer or device on the Internet is referenced by a unique Internet Protocol address the same way every telephone has a unique telephone number. An IP address is a series of four numbers separated by a period, and each number is a whole number between 0 and 254. An example of an IP address is 192.168.10.102. Each time an individual accesses the Internet, the computer from which that individual initiates access is assigned an IP address. A central authority provides each ISP a limited block of IP addresses for use by that ISP’s customers or subscribers. Most ISP’s employ dynamic IP addressing, that is they allocate any unused IP address at the time of initiation of an Internet session each time a customer or subscriber accesses the Internet. A dynamic IP address is reserved by an ISP to be shared among a group of computers over a period of time. The ISP logs the date, time and duration of the Internet session for each IP address and can identify the user of that IP address for such a session from these records. Typically, users who sporadically access the Internet via a dial-up modem will be assigned an IP address from a pool of IP addresses for the duration of each dial-up session. Once the session ends, the IP address is available for the next dial-up customer. On the other hand,

some ISPs, including most cable providers, employ static IP addressing, that is a customer or subscriber's computer is assigned one IP address that is used to identify each and every Internet session initiated through that computer. In other words, a static IP address is an IP address that does not change over a period of time and is typically assigned to a specific computer. A modem is an electronic device that allows one computer to communicate with another.

20. A host computer is one that is attached to a dedicated network and serves many users. These host computers are sometimes commercial online services, such as America On-line (AOL), which allow subscribers to dial a local number and connect to a network, which is in turn connected to their host systems. These service providers allow electronic mail service between their own subscribers, and those of other networks or individuals on the Internet.
21. Some of these systems offer their subscribers the ability to communicate publicly or privately with each other in real time in the form of "chat rooms." Contact with others online can be either open and anonymous, or private and personal in the form of person-to-person instant messages.

BACKGROUND OF INVESTIGATION

22. On May 4, 2009, SA Matthew I. Braverman was notified by Wegmans Food Markets (hereafter Wegmans) located in Rochester, New York that between March 13, 2009 and March 29, 2009, unsolicited commercial e-mail messages had been sent to Wegmans employees at their corporate e-mail addresses. The messages all arrived from addresses containing the user name "worldsu.per-food" from approximately 201 different domain names. All of the messages were similar in style, form, and substance. During this 17-day

time period, approximately 567 unique Wegmans employee e-mail accounts were sent a total of approximately 3,630 e-mails associated with the "worldsu.per-food" user name.

23. Wegmans reported to SA Braverman that on March 29, 2009, Wegmans employees were sent approximately 448 of the "worldsu.per-food" e-mails. These 448 e-mails were sent with e-mails servers using the root domain names filtercommands.net, pinkfair.net, and durationthinker.com. Based on my training and experience, I know that a root domain name identifies the entity that controls the name (e.g., emailserver.gmail.com, "gmail" is the root domain name).

24. SA Braverman utilized the software tool "www.domaintools.com" to conduct an historical 'whois' query to identify the registrant as of March, 29, 2009, for the domain names filtercommands.net, pinkfair.net, and durationthinker.com. The domain names had been registered by an individual who had identified himself/herself as Kristi Harbold, South Valley Marketing, PO Box 17587, Baltimore, MD 21297, Phone (410)630-1247. Based on my training and experience, I know that the software tool "www.domaintools.com" reflects historical information that does not change and will reveal registrant information as of a specific date.

- a. SA Braverman contacted the United States Postal Inspection Service (USPIS) and determined that the Post Office Box 17587, Baltimore, MD 21297 had been closed since 2007.

25. On multiple occasions Wegmans employees and SA Braverman attempted to contact Kristi Harbold via telephone at (410)630-1247 but could only reach an automated phone menu system and were unable to speak to an individual or leave a message. No company name or

further details were provided on the recording. Wegmans employees and SA Braverman also attempted to research South Valley Marketing using Internet resources but were unsuccessful in locating any further information.

26. SA Braverman utilized the software tool "www.domaintools.com" to conduct a hosting history query to identify the host, as of March 29, 2009, for the domain name filtercommands.net. At that time, that domain name was hosted by the IP address 128.168.160.2.
27. SA Braverman utilized the software tool "www.domaintools.com" to conduct a 'whois' query for the IP address 128.168.160.2. This IP address was associated with the internet service provider DATA102. The 'whois' data indicated that South Valley Marketing, 40 Warren Street, 3rd Floor, Charlestown, Massachusetts used a subset of DATA102's IP address space, between 128.168.160.0 and 128.168.175.255.
 - a. SA Braverman determined that the address 40 Warren Street, 3rd Floor, Charlestown, Massachusetts is the location of the business named Regus, a company offering virtual office services which operates the website "www.regus.com." According to this website, a virtual office is "a great value alternative to having a full time office and can be set up virtually overnight."
28. On June 9, 2009, DATA102 provided subscriber information for the IP address space 128.168.160.0 to 128.168.175.255. Around April 2008, DATA102 sold the IP address space 128.168.128.1 to 128.168.255.254 to Corporate Investment & Holdings (CIH) of Las Vegas, as owned and operated by Chris de Diego, e-mail address chris@go-pulsemarketing.com. DATA102 identified an affiliated business owned by de Diego as Pulse Marketing, 8350

Wilshire Blvd., Suite 300, Beverly Hills, California. SA Braverman determined the address 8350 Wilshire Blvd., Suite 200, Beverly Hills California 90211-2348 is the location of the business Access Office Inc., a business offering virtual office services which operates the website "www.accessofc.com."

29. In November 2009, SA Braverman utilized the Accurint, Choicepoint, and Dunn & Bradstreet services to conduct a search of national business databases for records pertaining to the business name "South Valley Marketing" and the name "Kristi Harbold" as it was associated with P.O. Box 17587, Baltimore, Maryland 21297 with negative results for any active companies. SA Braverman also utilized the Dunn & Bradstreet service to conduct a search of any Maryland, Colorado, and California businesses associated with an individual named Kristi Harbold. For this search, no businesses named South Valley Marketing were identified. SA Braverman also searched the Colorado, California, and Maryland Secretaries of State databases for South Valley Marketing with negative results.

- a. Other than 'whois' registrant information, open source Internet searches on Google.com returned negative results for search terms "Kristi Harbold" and either "South Valley Marketing" or "Pulse Marketing."

30. On June 26, 2009, Wegmans reported to SA Braverman an unsolicited commercial e-mail message which had been sent to several Wegmans employees at their corporate e-mail addresses on June 22, 2009. The messages all shared the subject line "Complete Body Cleanse with Acai Pure." Wegmans' network log files indicated that the message was sent to 40 distinct e-mail accounts belonging to Wegmans.

- a. The e-mails appeared to originate, as determined by the "FROM:" line

contained within the e-mail header, from the following e-mail addresses:

- i. hottestdiet@powellbrbecause.net
- ii. rated1superfoodonoprah@practisedstumbledvirtuous.net
- iii. hottestdiet@prevailinglyingfights.net
- iv. rated1superfoodonoprah@prevelanceorrinraimentbr.net
- v. rated1superfoodonoprah@proclaimedphantoms.net
- vi. hottestdiet@puzzlinglyneigh.net

31. SA Braverman utilized the software tool "www.domaintools.com" to conduct an historical 'whois' query to identify the registrant as of June 22, 2009, of each of the domain names, for the aforementioned e-mail addresses, namely: powellbrbecause.net, practisedstumbledvirtuous.net, prevailinglyingfights.net, prevelanceorrinraimentbr.net, proclaimedphantoms.net, and puzzlinglyneigh.net. Each of the aforementioned domain names had been registered by an individual who had identified himself/herself as Paul Beck, Epatriot Data, P.O. Box 17587, Baltimore, Maryland 21297, telephone (410)630-1247. This is the same address and telephone number used for South Valley Marketing.

32. On multiple occasions Wegmans employees and SA Braverman attempted to contact Paul Beck telephonically at (410)630-1247 but could only reach an automated phone menu system and were unable to speak to an individual or leave a message. No company name or further details were provided on the recording. Wegmans employees and SA Braverman also attempted to research Epatriot Data using Internet resources but were unsuccessful in locating any further information.

33. In November 2009, SA Braverman utilized the Accurint, Choicepoint, and Dunn &

Bradstreet services to conduct a search of national business databases for records pertaining to the business name "EPatriot Data" and the name "Paul Beck" as it was associated with P.O. Box 17587, Baltimore, Maryland 21297 with negative results. SA Braverman also utilized the Dunn & Bradstreet service to conduct a search of any Maryland, Colorado, and California businesses associated with an individual named Paul Beck. For this search, no businesses named EPatriot Data were identified. SA Braverman also searched the Colorado, California, and Maryland Secretaries of State databases for EPatriot Data with negative results.

- a. Other than 'whois' registrant information, open source Internet searches on Google.com returned negative results for search terms "Paul Beck" and either "EPatriot Data" or "Pulse Marketing."

34. On July 3, 2009, SA Braverman reviewed one of the aforementioned e-mail messages which had been received by Wegmans. SA Braverman determined the e-mail message had originated from the IP address 209.101.177.172 on June 22, 2009 at 5:55 a.m. EDT.

35. On July 3, 2009, SA Braverman utilized the software tool "www.domaintools.com" to conduct a 'whois' query to identify the registrant of the IP address 209.101.177.172 as Mega Colocation, 631 N. Stephanie Street, Suite 231, Henderson, Nevada 89014, a division of Big Sky Services, Inc., 1197 East Los Angeles Avenue, Suite C-215, Simi Valley, California 93065.

36. On July 28, 2009, Big Sky Services advised that the subscriber to IP address 209.101.177.172 on June 22, 2009 at 5:55 a.m. EDT was Pulse Marketing, 8350 Wilshire Blvd., Suite 200, Beverly Hills California 90211-2348.

- a. Wegmans reported to SA Braverman that its e-mail servers are located in its main data center located at 100 Wegmans Market Street, Rochester, NY. SA Braverman tracked the location of IP address 209.101.177.172 to California. Therefore, SA Braverman determined that the electronic mail messages received by Wegmans employees on June 22, 2009 traveled interstate.

37. SA Braverman reviewed the website "www.spamhaus.org," for information pertaining to Pulse Marketing. The website is operated by The Spamhaus Project, which is an international non-profit organization whose mission is to track the Internet's spam operations. The Spamhaus Project identified an active spammer named Levi Beers, who was described as the Chief Technology Officer of Pulse Marketing. The Spamhaus Project identified Beers' e-mail address as "levibeers@gmail.com."
38. SA Braverman conducted a search of the website "www.facebook.com," and located a profile pertaining to Levi Beers. The Facebook profile indicated that he was married to Tracy Stotler Beers. It also contained a link to the website "www.babyaidensjourney.com."
39. SA Braverman conducted a search of the website "www.babyaidensjourney.com" and the website identified an e-mail address for Levi Beers as "levibeers@gmail.com."
40. On August 6, 2009, Google provided subscriber information for the e-mail address "levibeers@gmail.com" to be Levi Beers. The account was created on March 5, 2005. A secondary e-mail address of "levibeers@hotmail.com" was provided.
41. SA Braverman conducted a mail server lookup for the domain go-pulsemarketing.com and identified that e-mail for go-pulsemarketing.com was managed through Google Apps.
42. On August 6, 2009, Google provided subscriber information for the e-mail address

“chris@go-pulsemarketing.com” to be Chris de Diego.

43. On August 21, 2009, the United States District Court, Western District of New York issued a Search Warrant on Google Inc., 1600 Amphitheatre Parkway, Mountain View, California for the content of the e-mail accounts "levibeers@gmail.com" and "chris@go-pulsemarketing.com," including all Google Apps content. Google Apps includes a "Google Docs" service which allows users to store and edit documents online on Google's servers.
44. On August 31, 2009, Google Inc. responded to the Search Warrant and provided the requested records. I have reviewed the following information that was obtained from the records provided by Google Inc.:

- a. On September 16, 2008, de Diego sent an e-mail to Beers and Pulse Marketing contractor, Praveen Marella, with a subject line of "Yahoo Project." The message included the following: "Please create 50 new Yahoo accounts as soon as possible. Then we are going to take an offer and I want to send this offer from these yahoo accounts to our Yahoo file. Need to test how many per hour one of your guys can do. My goal would be 3-5 per min. 8 hours per day."
- b. On September 17, 2008, Marella sent an e-mail to de Diego and Beers with a subject line of "Re: Yahoo Project." The message included the following: "Please find as attachment 50 fresh yahoo email IDs created for you." Attached to the message was the file, "Yahoo_50.xls." The file was a spreadsheet document that included 50 Yahoo IDs. Twenty-five of those Yahoo IDs make up half of the SUBJECT ACCOUNTS.

- c. On September 19, 2008, de Diego sent an e-mail to Marella with a subject line of "Re: Yahoo Plan – How we can make it work." The message included the following: "Please continue to set up new Yahoo accounts, as much as possible. Try to use the new proxy server, if it shows up in a language you can't read, just re-load the page, it will grab a new IP, just keep going to Yahoo.com until it is in English."
- d. On September 20, 2008, Marella sent an e-mail to de Diego and Beers with a subject line of "Yahoo Mailing Plan for Weekend." The message included the following: "We are planning to use 100 yahoo accounts and mail to 15K data on Saturday and Sunday. Over the weekend we will increase the Yahoo account numbers and try to reach 150K to 200K target."
- e. On April 28, 2009, Beers sent an e-mail to de Diego and Marella with a subject line of "Praveen and today, Monday 4/27." The message included the following: "...[Marella] submitted [IP address information] under Paul Beck from epatriotdata.com."
- f. On June 23, 2009, Marella sent an e-mail to de Diego and Beers with a subject line of "Yahoo Accounts....500 per day." The message included the following: "I just made an review with the team members and we can create 500 yahoo accounts per day. This includes creating them and using the accounts to send emails to keep them active."
- g. On June 24, 2009, Beers received an e-mail from the abuse department of Big Sky Services with a subject of "IMPORTANT – 12 COMPLAINTS." The e-

mail notified Pulse Marketing that an e-mail message sent by Pulse Marketing on June 22, 2009 at approximately 5:01 a.m. EST with the "From:" address, "hottestdiet@prevailingfights.net," and the subject line, "Complete Body Cleanse with Acai Pure," had been flagged as spam. The sending e-mail address and subject line matched those from unsolicited messages received by Wegmans employees on the same date, June 22, 2009.

- h. A document entitled "Pulse_Weekly_Report Q-3 2008" was found in Beers' Google Apps account. The document appeared to be a multi-page spreadsheet with daily details of Pulse Marketing's e-mailing activity in 2008 and 2009. An entry indicated that on June 22, 2009, Pulse Marketing successfully mailed 3,082,097 e-mail addresses for an offer entitled "Acai Pure Trial Offer." The mailing was executed between 3:20 a.m. EST and 8:30 a.m. EST. Another entry indicated that on March 29, 2009, Pulse Marketing distributed an offer entitled "Acai Pure Trial Offer."
- i. On June 25, 2009, Marella sent an e-mail to de Diego and Beers with a subject line of "Today's Update on emails creation – 25th June 2009." The message included the following: "Yahoo: 575 new email IDs were created in last 24 hrs and checking the working of the IDs is on"; "Google Docs was updated with the email accounts created"; "Yahoo - 6978 Working IDs."
- j. On June 25, 2009, de Diego sent an e-mail to Marella and Beers with a subject line of "Re: Today's Update on emails creation – 25th June 2009." The message included the following: "Try to create as many yahoo accounts as

possible every day”; “Most important is that we get to 50,000 yahoo accounts as soon as possible.”

- k. On June 28, 2009, Beers sent an e-mail to Pulse Marketing General Manager, Terry Schriener, with a subject of “AOL FL’s.” The message included the following: “I was incorrect, we are using Paul Beck, my phone for the classes.”
- l. On July 1, 2009, Beers sent an e-mail to Marella with a subject line of “change the google doc.” The message included the following:
“Yahoo_Hotmail_Gmail project is being published to everyone.”
- m. A document entitled “Yahoo_Hotmail_Gmail - IDs” was found in Beers’ Google Apps account. The document was a multi-page spreadsheet with a list of user IDs created at Yahoo, Gmail, and Hotmail. The spreadsheet included 8,615 Yahoo IDs. Twenty-five of those Yahoo IDs make up half of the SUBJECT ACCOUNTS.
- n. On July 29, 2009, Beers sent an e-mail to de Diego with a subject line of, “Yahoo AutoLogin.” The message included the following: “I have 5 servers (semi-dedicated) to running the yahoo accounts.... they can deliver mail at any time.”
- o. On August 19, 2009, Beers received an e mail from a Pulse Marketing contractor with a subject line of “Things I need.” The message included the following: “Ability to send e mails from admin@epatriotdata.com so I can respond to screams and stem complaints.”

45. Based on the investigation to date and my discussions with SA Braverman, it appears that:

- a. Several thousand Yahoo electronic mail accounts were created by Pulse Marketing employees using false information.
- b. "Kristi Harbold" and "South Valley Marketing" are fictitious names used by Pulse Marketing and/or its associates to register one or more domain names with false registrant information.
- c. "Paul Beck" and "Epatriot Data" are fictitious names used by Pulse Marketing and/or its associates to register six or more domain names with false registrant information.
- d. Thereafter, multiple commercial electronic mail messages affecting interstate commerce have been sent between March 2009 and June 2009 with the assistance of these falsely registered domain names and falsely created Yahoo electronic mail accounts.

EVIDENCE

46. Based on training and experience, I know that the complete contents of e-mail accounts may be important to establishing the actual user who has dominion and control of an e-mail account at a given time. E-mail accounts may be registered in false names or screen names from anywhere in the world with little or no verification by the service provider. They may also be used by multiple people. Therefore, the content of a given account, including the e-mail accounts that send messages to a given SUBJECT ACCOUNT often provides important evidence regarding the actual

user's dominion and control of an e-mail account.

47. Your Affiant knows from training and experience that the complete contents of e-mail accounts may contain a history of sent and received messages, as well as retrieved and unretrieved messages, which can provide important evidence regarding how and for what purpose an e-mail account was used.

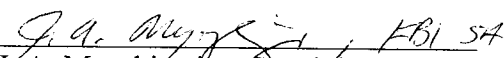
48. Your Affiant knows from training and experience that criminals discussing their criminal activity may use slang, short forms (abbreviated words or phrases such as "lol" to express "laugh out loud"), or code words (which require entire strings or series of e-mail conversations to determine their true meaning) when discussing their crimes. They can also discuss aspects of the crime without specifically mentioning the crime involved. In the electronic world, it is even possible to use pictures, images and emoticons (images used to express a concept or idea such as a happy face inserted into the content of an e-mail or the manipulation and combination of keys on the computer keyboard to convey an idea, such as the use of a colon and paren "(:)" to convey a smile or agreement) to discuss matters. Keyword searches would not account for any of these possibilities, so actual review of the contents of an e-mail account by law enforcement familiar with the identified criminal activity is necessary to find all relevant evidence within the account.

CONCLUSION

49. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A).

50. Based on the aforementioned factual information, probable cause exists to believe that evidence, fruits, and instrumentalities of 18 U.S.C. § 1037(a)(4) (as further described on Attachment B) will be located within the e-mail accounts identified in Attachment A. The usage of the e-mail accounts in Attachment A is relevant to establish whether PULSE MARKETING INC. falsified information in registering the e-mail accounts for the purpose of transmitting unsolicited commercial electronic mail. I, therefore, respectfully request that the attached warrant be issued authorizing the search and seizure of the items listed in Attachment B. I further state that if evidence located within the e-mail accounts identified in Attachment A appear 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.

I declare under penalty of perjury the foregoing is true and correct to the best of my knowledge and belief.


J. A. Myszkiewicz, Special Agent
Federal Bureau of Investigation

SUBSCRIBED and SWORN before me this 25th day of January, 2010.


UNITED STATES MAGISTRATE JUDGE