

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

FILED

OCT 15 2014

10-15-14

UNDER SEAL

MAGISTRATE JUDGE MARIA VALDEZ
UNITED STATES DISTRICT COURT

In the Matter of the Search of:

The residence located at 4641 South Washtenaw
Avenue, Chicago, Illinois, further described in
Attachment A

Case Number: **14 M 553**

APPLICATION AND AFFIDAVIT FOR A SEARCH WARRANT

I, Josh E. Sadowsky, a Special Agent of the Federal Bureau of Investigation, request a search warrant and state under penalty of perjury that I have reason to believe that on the following property or premises:

See Attachment A

located in the Northern District of Illinois, there is now concealed:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is evidence and instrumentalities.

The search is related to a violation of:

Code Section

Offense Description

Title 18, United States Code, Sections 371, 1030(a), 1037, 1343, and 2319, and Title 17, United States Code, Section 506(a)	Conspiracy, computer fraud, fraud in connection with email, wire fraud, and copyright infringement
---	--

The application is based on these facts:

See Attached Affidavit,

Continued on the attached sheet.

Applicant's Signature

JOSH E. SADOWSKY, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: October 15, 2014

Judge's signature

City and State: Chicago, Illinois

MARIA VALDEZ, U.S. Magistrate Judge

Printed name and title

①

UNITED STATES DISTRICT COURT)
)
NORTHERN DISTRICT OF ILLINOIS)

AFFIDAVIT

Introduction and Agent Background

I, Josh E. Sadowsky, being duly sworn, state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation and have been so employed since 2009. I am currently assigned to the Cybercrimes Unit in Los Angeles, California, where I specialize in the investigation of computer and high-technology crimes, including computer intrusions, denial of service attacks and other types of malicious computer activity. During my career with the FBI, I have participated in numerous computer crime investigations. In addition, I have received both formal and informal training from the FBI and other institutions regarding computer-related investigations and computer technology. Prior to my work in the FBI, I was a self-employed computer consultant and Internet business owner for eight years.

2. This affidavit is made in support of an application for a warrant to search the residence located at 4641 South Washtenaw Avenue, Chicago, Illinois, 60632, described further in Attachment A (the "Subject Premises"), for evidence and instrumentalities described further in Attachment B, concerning violations of Title 18, United States Code, Sections 371 (conspiracy), 1030(a) (computer fraud and abuse), 1037 (fraud and related activity in connection with electronic mail), 1343 (wire fraud), and 2319 and Title 17, United States Code, Section 506(a)

(criminal copyright infringement)¹ (the “**Subject Offenses**”). The statements in this affidavit are based on my personal knowledge, and on information I have received from other law enforcement personnel and from persons with knowledge regarding relevant facts. Because 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. I have set forth facts that I believe are sufficient to establish probable cause to believe that evidence and instrumentalities of violations of the **Subject Offenses** are located at the **Subject Premises**.

FACTS SUPPORTING PROBABLE CAUSE TO SEARCH

Definitions

3. I know from my training and experience that the following definitions apply to the activity discussed in this affidavit:

a. *IP Address*: The Internet Protocol address (or simply “IP” address) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic to and from that computer may be properly directed from its source to its destination.

¹ Copyright protection attaches to “original works of authorship fixed in any tangible medium of expression,” Title 17, United States Code, Section 102, including photographs.

b. *Server*: A server is a computer that provides services to other computers. Examples include web servers which provide content to web browsers and e-mail servers which act as a post office to send and receive e-mail messages.

c. *Phishing*: Phishing occurs when a fraudulent e-mail or text message was sent to the victim claiming to be from a legitimate Internet provider seeking the victim's login and password information. The victim is then directed to an illicit website, or is asked to respond with their username and password, which the criminal then uses to gain access to the victim's account.

4. I know from my training and experience that Apple, located in Cupertino, California, operates computers used by subscribers all over the world in interstate and foreign commerce and communications. One of the services that Apple provides to its customers is "iCloud," a "cloud" computing back-up system for subscriber data. Photos and videos taken on Apple iPhones can be automatically backed up to the iCloud, making them accessible to users on the Internet.

5. I know from my training and experience that Google, located in Northern California, operates computers used by subscribers all over the world in interstate and foreign commerce and communications. One of the services that Google provides to its customers is Gmail, an e-mail service.

Overview

6. The FBI is currently investigating online leaks of private photographs, including nude and sexually explicit photographs of dozens of female celebrities—

including victims A.S., C.H., H.S., J.M., O.W., A.K., E.B., and A.H.—that began on or about August 31, 2014, and which are ongoing. Based on interviews with several victims, the FBI currently believes that many of the photographs were obtained without authorization from the Apple iCloud account of either the victim or his/her significant other. Based on victim account records obtained from Apple, one or more computers used at the **Subject Premises** accessed or attempted to access without authorization multiple celebrities' e-mail and iCloud accounts over the course of several months. As further described below, person(s) using one or more computers are believed to be violating the **Subject Offenses** from the **Subject Premises**.

Summary of the Evidence

Celebgate

7. Beginning on or about August 31, 2014, I read news reports about the leak of private photographs of female celebrities and conducted Google searches to discover that nude and sexually explicit photographs of numerous female celebrities were posted online. Some victims' photographs were posted on or about August 31, 2014, to the websites 4chan.org and Reddit.com. Throughout the month of August, 2014, and continuing to October, 2014, numerous other victims' private photographs were posted online without their permission. This leak of private photographs was labeled online as "Celebgate" or "The Fappening."

8. On September 22, 2014, I interviewed victim A.S. and learned the following information:

a. A.S. is a female celebrity who has appeared in several movies and TV shows.

b. A.S. first learned she may have been a victim of the photo leaks on or about August 31, 2014, when the media was reporting her as a victim. Although she could not find any photos of herself initially, several weeks later several photos and two videos were posted online. Some of the photos were taken between October and November 2013, and the others between April and May 2014. All photos were taken with her iPhone and sent through iMessage to her boyfriend. The two videos were also taken with her phone during the same time frame. At the time of the leaks, the videos were still stored in her phone. The morning after her private information was leaked, the media contacted her for a statement.

c. Between April and May 2014, A.S. recalled getting locked out of her online accounts, and her password wasn't working. A.S. used iCloud on her phone, as well as Gmail for her e-mail.

9. On September 25, 2014, I interviewed victim A.H. and learned the following information:

a. A.H. is a female celebrity who has appeared in several movies.

b. On or about August 31, 2014, A.H. learned that she was on a "master list" of victims who had their private photographs leaked online, although she did not see any photos online. On or about September 21, 2014, she received a call from her publicist that TMZ (a media outlet that focuses on tabloid reporting)

wanted to get a statement about the leak of her photos. She then learned that approximately 54 private photographs of her were leaked online. The photos were taken with her iPhone between November 2012 and May 2014. A.H. advised that while some of the photos were sent to her fiancé, others were never sent and only stored on her phone.

c. At the time of the leaks, A.H. used iCloud services on her iPhone, but soon after called a person familiar with computers who showed her how to remove the iCloud features from her phone and turn off iCloud backups.

10. On or about October 10, 2014, I reviewed AT&T Internet subscriber information for the IP address 99.133.149.163 (the "Subject Premises IP"), which showed that for the period of May 14, 2013, through October 10, 2014, the Subject Premises IP was assigned to Emelio Herrera at the Subject Premises. The "MemberID" was listed as emilioherreradiatz@att.net, and the preferred e-mail on the account was emilio.herrerra.diaz@gmail.com.

11. Between on or about September 4 and October 12, 2014, FBI Special Agent Jeff Kirkpatrick and I reviewed Apple records related to the Subject Premises IP and learned the following:

a. Between on or about May 31, 2013, and August 31, 2014, the Subject Premises IP was used to access approximately 572 unique iCloud accounts. Many of the accounts were accessed numerous times, and in total, the unique iCloud accounts were accessed 3,263 times from the Subject Premises IP.

b. Of the accounts that were accessed from the **Subject Premises IP**, a number of them were accounts of celebrities who had photos leaked online. The following are celebrities who had their account accessed from the **Subject Premises IP** and had photos leaked online: A.S., C.H., H.S., J.M., O.W., A.K., E.B., and A.H.

c. The majority of the other accounts accessed from the **Subject Premises IP** were accounts of celebrities, models or their friends and families.

d. In addition to accessing the above-referenced accounts during the time period of on or about May 31, 2013, and August 31, 2014, the **Subject Premises IP** was used to attempt to reset 1,987 unique iCloud account passwords, approximately 4,980 times.

e. The computer type listed for the password resets was "Windows_7."

12. Based on my training and experience, it is common for hackers to use various tools to assist in downloading and storing victims' iCloud data, including their photos and videos. At least two subjects who I have investigated in the past, who have also hacked celebrity iCloud accounts, used a tool called Elcomsoft Phone Password Breaker. This tool, which can be downloaded and purchased online by anyone, allows a user to download the contents of a victim's iCloud account if the username and password are known. I also know that one common way a person

would gain unauthorized access to a victim's iCloud account is by phishing. Victims usually receive the phish in the form of an e-mail, text message, or iMessage.

13. On or about October 12, 2014, FBI Special Agent Jeffrey Kirkpatrick conducted public record checks on Emilio Herrera and the **Subject Premises** and informed me of the following:

a. Emilio Herrera appeared to reside at the **Subject Premises** as recently as September, 2014.

b. Also listed as possible residents of the **Subject Premises** were Carmen Herrera, Jesus Herrera and Martin Herrera.

c. The **Subject Premises** was owned by Jesus Herrera.

d. Multiple vehicles had been registered to Emilio Herrera and Jesus Herrera at the **Subject Premises**.

e. Emilio, Carmen and Jesus Herrera all had Illinois driver's licenses with the address listed as the **Subject Premises**.

f. The **Subject Premises** appeared to be a single-family home with a single mailbox in the front of the house.

g. The property had a detached garage behind the home.

h. All of the addresses listed for the **Subject Premises**, including utilities, driver's licenses, vehicle registrations and billing addresses, indicate the **Subject Premises** is a single-family home. One data source, Accurant, in some cases had a unit number listed as 1 or 2. This was the only place a unit number was

shown. Based upon the service address provided by AT&T being listed as the **Subject Premises** with no unit number, it is likely that if the single family home or the garage was converted to have a second unit, then the AT&T internet service is still being utilized by the entire property.

SPECIFICS REGARDING SEARCHES OF COMPUTER SYSTEMS

14. Based upon my training and experience, and the training and experience of specially trained computer personnel whom I have consulted, searches of evidence from computers commonly require agents to download or copy information from the computers and their components, or remove most or all computer items (computer hardware, computer software, and computer-related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Computer storage devices can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site.

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

c. In order to fully retrieve data from a computer system, the analyst needs all storage media as well as the computer. The analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard disk drives or on external media).

d. In addition, a computer, its storage devices, peripherals, and Internet connection interface may be instrumentalities of the crime(s) and are subject to seizure as such if they contain contraband or were used to carry out criminal activity.

PROCEDURES TO BE FOLLOWED IN SEARCHING COMPUTERS

15. The warrant sought by this Application does not authorize the "seizure" of computers and related media within the meaning of Rule 41(c) of the Federal Rules of Criminal Procedure. Rather the warrant sought by this Application authorizes the removal of computers and related media so that they may be searched in a secure environment.

16. With respect to the search of any computers or electronic storage devices seized from the location identified in Attachment A hereto, the search procedure of electronic data contained in any such computer may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein):

a. examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to determine whether that data falls within the items to be seized as set forth herein;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3)

contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. surveying various file directories and the individual files they contain to determine whether they include data falling within the list of items to be seized as set forth herein;

d. opening or reading portions of files in order to determine whether their contents fall within the items to be seized as set forth herein;

e. scanning storage areas to discover data falling within the list of items to be seized as set forth herein, to possibly recover any such recently deleted data, and to search for and recover deliberately hidden files falling within the list of items to be seized; and/or

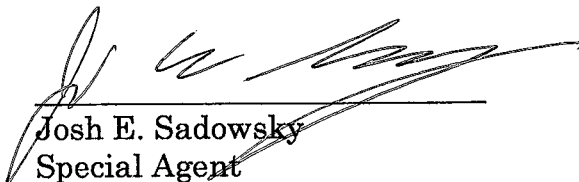
f. performing key word searches through all storage media to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B.

17. Any computer systems and electronic storage devices removed from the premises during the search will be returned to the premises within a reasonable period of time not to exceed 30 days, or unless otherwise ordered by the Court.

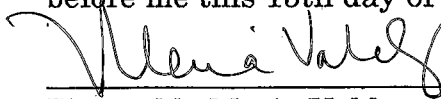
CONCLUSION

18. Based on the above information, I respectfully submit that there is probable cause to believe that violations of the **Subject Offenses** have been committed, and that evidence and instrumentalities relating to this criminal conduct, as further described in Attachment B, will be found in the **Subject Premises**, as further described in Attachment A. I therefore respectfully request that this Court issue a search warrant for the residence located at 4641 South Washtenaw Avenue, Chicago, Illinois, 60632, more particularly described in Attachment A, authorizing the seizure of the items described in Attachment B.

FURTHER AFFIANT SAYETH NOT.


Josh E. Sadowsky
Special Agent
Federal Bureau of Investigation

Subscribed and sworn
before me this 15th day of October, 2014


Honorable Maria Valdez
United States Magistrate Judge

ATTACHMENT A

DESCRIPTION OF PREMISES TO BE SEARCHED

The premises to be searched is the residence located at 4641 South Washtenaw Avenue, Chicago, Illinois, 60632 and is further described as follows: the residence is located on the east side of Washtenaw Avenue between 46th and 47th streets, two houses north of an east-west alley. The premises appears to be a one-and-a-half story single-family home with brown brick and white trim. The numbers "4641" are located immediately to the right of the front door. The home is surrounded by a black wrought-iron fence. The premises include a brown brick two-car garage, which is located behind the home off a north-south alley.

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

Evidence and instrumentalities concerning violations of Title 18, United States Code, Sections 371 (conspiracy), 1030(a) (computer fraud and abuse), 1037 (fraud and related activity in connection with e-mail), 1343 (wire fraud), and 2319 and Title 17, United States Code, Section 506(a) (criminal copyright infringement) (the “**Subject Offenses**”), as follows:

- a. Any and all records, notes, documents, and materials related to e-mail and iCloud accounts accessed by residence of the **Subject Premises** for the period of May 31, 2013, to present.
- b. Any and all records, notes, documents, and materials related to celebrities and women not affiliated with residents of the **Subject Premises**, to include:
 - i. Personally identifying information, such as date of birth and social security account number;
 - ii. Contact information, such as addresses, telephone numbers, e-mail addresses, or online account names;
 - iii. Photographs in any format; and
 - iv. Videos in any format.
- c. Any and all records, notes, documents, and materials related to “phishing,” which may include accounts with names that imply they are from Gmail, Apple, or other potential phishing accounts, and used in an attempt to have users provide login information in response to an e-mail from the account, or the content of a phishing e-mail itself, which may appear to look like a legitimate e-mail from an Internet Service Provider with the purpose of obtaining private information from a recipient.
- d. Any and all records, documents, images, logs, programs, applications and materials relating to hacking e-mail accounts, resetting e-mail password, hacking utilities, e-mail forwarding, Elcomsoft Phone

Password Breaker software, or compromising e-mail accounts or other secured Internet services.

- e. Any and all records, documents, images, logs, programs, applications and materials relating to the sharing, distributing, or posting of photographs, videos or personal information of celebrities, or person(s) that have no obvious relationship to residents of the **Subject Premises**, including victims A.S., C.H., H.S., J.M., O.W., A.K., E.B., and A.H.
- f. Evidence and contents of logs and files on a computer or storage device, such as those generated by the computer's operating system, which describes the history and use of the device, including but not limited to files indicating when files were written, were opened, were saved, or were deleted. Evidence tending to show the identity of the person using the computer at the time any actions relating to the above offenses were taken. Also, any malware resident on the computer.

The following may be seized and searched for all items listed above, and for any items specifically noted in the paragraphs below:

- a. Computer hardware, meaning any and all computer equipment. Included within the definition of computer hardware are any electronic devices capable of data processing (such as central processing units, laptop or notebook or netbook or tablet computers, personal digital assistants, gaming consoles, and wireless communication devices to include cellular telephone devices capable of internet access); peripheral input/output devices (such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media); related communications devices (such as modems, wireless routers, cables and connections); storage media, defined below; and security devices, also defined below.
- b. Computer software, meaning any and all data, information, instructions, programs, or program codes, stored in the form of electronic, magnetic, optical, or other media, which is capable of being interpreted by a computer or its related components. Computer software may also include data, data fragments, or control characters integral to the operation of computer software, such as operating systems software, applications software, utility programs, compilers, interpreters, communications software, and other programming used or intended to be used to communicate with computer components.

- c. Computer related documentation, meaning any written, recorded, printed, or electronically stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.
- d. Data security devices, meaning any devices, programs, or data -- whether themselves in the nature of hardware or software -- that can be used or are designed to be used to restrict access to, or to facilitate concealment of, any computer hardware, computer software, computer related documentation, or electronic data records. Such items include, but are not limited to, user names and passwords; data security hardware (such as encryption devices, chips, and circuit boards); data security software or information (such as test keys and encryption codes); and similar information that is required to access computer programs or data or to otherwise render programs or data into usable form.
- e. All storage media capable of collecting, storing, maintaining, retrieving, concealing, transmitting, and backing up electronic data. Included within this paragraph is any information stored in the form of electronic, magnetic, optical, or other coding on computer media or on media capable of being read by a computer or computer related equipment, such as fixed hard disks, external hard disks, removable hard disks (including micro drives), floppy diskettes, compact disks (CDs), digital video disks (DVDs), tapes, optical storage devices, laser disks, thumb drives, ipods, digital cameras, memory cards (e.g. CF or SD cards), Xboxes, flash drives, or other memory storage devices. This also includes areas with digital storage capability on devices such as printers, scanners, wireless routers, etc.

ADDENDUM TO ATTACHMENT B

Cellular Phones

With respect to the search of any information and records stored within hand-held wireless communication devices, including cellular telephones, and any related memory cards or removable storage media, law enforcement personnel will locate the information to be seized according to the following protocol:

The search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein):

- a. searching for and attempting to recover any hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein;
- b. surveying various file directories, electronic mail, text messages, contact lists, address books, call logs, calendars, notes, appointments, task lists, voice mail, audio files, video files, or pictures, including attachments thereto, to determine whether they include data falling within the list of items to be seized as set forth herein;
- c. opening or reading portions of electronic mail or text messages, and attachments thereto, in order to determine whether their contents fall within the items to be seized as set forth herein; and/or
- d. performing key word searches through all electronic mail or text messages, and attachments thereto, to determine whether occurrences of language contained in such electronic mail or text messages, and attachments thereto, exist that are likely to appear in the information to be seized described in Attachment B.

Law enforcement personnel are not authorized to conduct additional searches on any information beyond the scope of the items to be seized by this warrant.

Computer media

This warrant does not authorize the "seizure" of computers and related media within the meaning of Rule 41(c) of the Federal Rules of Criminal Procedure. Rather this warrant authorizes the removal of computers and related media so that they may be searched in a secure environment. The search shall be conducted pursuant to the following protocol:

With respect to the search of any computers or electronic storage devices removed from the premises described in Attachment A hereto, the search procedure of electronic data contained in any such computer may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein):

- a. examination of all the data contained in such computer hardware, computer software, and/or memory storage devices to determine whether that data falls within the items to be seized as set forth herein;
- b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
- c. surveying various file directories and the individual files they contain to determine whether they include data falling within the list of items to be seized as set forth herein;
- d. opening or reading portions of files in order to determine whether their contents fall within the items to be seized as set forth herein;
- e. scanning storage areas to discover data falling within the list of items to be seized as set forth herein, to possibly recover any such recently deleted data, and to search for and recover deliberately hidden files falling within the list of items to be seized; and/or

- f. performing key word searches through all electronic storage media to determine whether occurrences of language contained in such storage media exist that are likely to appear in the evidence described in Attachment B.

The government will return any computers or electronic storage devices removed from the premises described in Attachment A hereto within 30 days of the removal thereof, unless contraband is found on the removed computer and/or electronic storage device, or unless otherwise ordered by the Court.