	Case 2:13-cr-00082-KJM Docume	ent 23	Filed 12/13/13	Page 1 of 31		
1	JASON S. LEIDERMAN, SBN 203336					
2	jay@criminal-lawyer.me ERIC J. LINDGREN, SBN 288542					
3	eric@criminal-lawyer.me LAW OFFICES OF JAY LEIDERMAN					
4	5740 Ralston Street, Suite 300 Ventura, California 93003					
5	Tel: 805-654-0200 Fax: 805-654-0280					
6	TOR EKELAND, PRO HAC VICE					
7	tor@torelekand.com TOR EKELAND, P.C. 155 Water Street Brooklyn, NY 11201					
8						
9	Tel: 718-285-9279 Fax: 718-504-5417					
10	Attorneys for Defendant MATTHEW KEYS					
11						
12	UNITED STAT	ES DI	STRICT COURT			
13	EASTERN DIST	RICT	OF CALIFORNIA	A		
14			Case No.: 13-CR-0	0082 KIM		
15)		TION AND MOTION TO		
16	UNITED STATES,) S	UPPRESS EVID	DENCE; MEMORANDUM DAUTHORITIES		
17	Plaintiff,					
18	v.		Date: Jan Time: 9:0	uary 29, 2014 0 am		
19	MATTHEW KEYS,			urtroom 3		
20	Defendant.	ý				
21))				
22						
23	TO THE COURT AND THE UNITED STATES, THROUGH THE UNITED STATES					
24	ATTORNEY:					
25	PLEASE TAKE NOTICE THAT on the					
26	matter can be heard in the above designated courtroom, or such other courtroom to which said motion is					
27	assigned, Defendant Matthew Keys ("Defendant	" or "N	Ar. Keys"), by and	t through counsel, will move		
28						
	MOTION TO SUDDESS		5740 Rai	ES OF JAY LEIDERMAN Iston Street, Suite 300 ra California 93003		

MOTION TO SUPPRESS Page i

ntura, California 930 Tel: 805-654-0200 Fax: 805-654-0280 US

Case 2:13-cr-00082-KJM Document 23 Filed 12/13/13 Page 2 of 31

the court to issue an order suppressing evidence seized as a result of a search and seizure by police 2 officers, to wit:

- 1. The audio recording and any transcript of Mr. Keys' statement to investigators on October 4, 2012.
- 2. The perceptions, recollections and observations of the officers related to that taped statement.
 - 3. Mr. Keys' written statement to the government dated October 4, 2012.
 - 4. All property and information seized during the October 4, 2012 execution of a search warrant on Mr. Keys' New Jersey residence.
 - 5. Any other evidence the court finds unlawfully obtained and the fruits thereof.

This motion is made under Rule 12(b)(3)(C) of the Federal Rules of Criminal Procedure on the ground that the search and seizure violated Defendant's rights under the Fourth and Fifth Amendments to the United States Constitution.

This motion is based on the attached points and authorities, the testimony of any witnesses at the hearing, the attached declarations of Defendant's counsel, the files and records in this action, and any further evidence or argument that the Court may properly receive at or before the hearing

Dated: December 13, 2013

1

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

By: /s/ Jay Leiderman Jason S. Leiderman

Eric J. Lindgren LAW OFFICES OF JAY LEIDERMAN

By: <u>/s/ Tor Ekeland</u>

Tor Ekeland TOR EKELAND, P.C.

Attorneys for Defendant MATTHEW KEYS

TABLE OF CONTENTS 1 2 TABLE OF AUTHORITIES 3 MEMORANDUM OF POINTS AND AUTHORITIES......1 4 INTRODUCTION..... STATEMENT OF FACTS..... 5 THE SEARCH WARRANT AND AFFIDAVIT. I. 6 7 B. COMMUNICATION BETWEEN MERCER AND MR. KEYS REGARDING 8 9 ANONYMOUS..... 10 C. INTERNAL INVESTIGATION OF THE DECEMBER 14, 2010 EDITS TO THE LOS ANGELES TIMES WEBSITE..... 11 D. MR. KEYS PUBLISHED ARTICLES ACKNOWLEDGING ACCESS TO "TOP LEVEL 12 13 14 15 16 17 II. EXECUTION OF THE WARRANT. .. 10 ARGUMENT..... 18 I. THE SEARCH WARRANT AUTHORIZED AN OVERBROAD GENERAL SEARCH OF 19 ALL OF MR. KEYS' ELECTRONIC MEDIA. 10 20 A. IN ORDER TO CONDUCT WHOLESALE SEIZURES OF ELECTRONIC MEDIA. THE 21 22 GOVERNMENT MUST PRESENT A FACTUAL BASIS FOR DOING SO, IT MUST FOLLOW A SEGREGATION PROTOCOL FOR IDENTIFYING RELEVANT INFORMATION, AND IT 23 24 25 B. THE WARRANT COMPLETELY IGNORES CHIEF JUDGE KOZINSKI'S GUIDELINES 26 27

1	II. AT THE TIME ANDREWS APPLIED FOR THE WARRANT, THE FACTS				
2	SUPPORTING PROBABLE CAUSE TO BELIEVE MR. KEYS POSSESSED ANY EVIDENCE				
3	WERE STALE				
4	III. THE AFFIDAVIT CONTAINS DELIBERATE OR RECKLESS				
5	MISREPRESENTATIONS AND OMISSIONS REQUIRING A FRANKS HEARING				
6	A. ANDREWS' AFFIDAVIT CONTAINS DELIBERATE OR RECKLESSLY-MADE				
7	STATEMENTS AND OMISSIONS 19				
8	B. WITH THE FALSE STATEMENTS AND OMISSIONS CORRECTED, THE AFFIDAVIT				
9	DOES NOT SUPPORT A FINDING OF PROBABLE CAUSE				
10	IV. THE FRUIT OF THE POISONOUS TREE DOCTRINE REQUIRES SUPPRESSION OF				
11	WRITTEN AND RECORDED STATEMENTS OF MR. KEYS				
12	V. MR. KEYS' MIRANDA WAIVER WAS INVALID BECAUSE IT WAS NOT				
13	VOLUNTARY, KNOWING AND INTELLIGENT				
14	A. MR. KEYS INVOLUNTARILY WAIVED HIS <i>MIRANDA</i> RIGHTS				
15	B. MR. KEYS DID NOT KNOWINGLY AND INTELLIGENTLY WAIVE HIS MIRANDA				
16	RIGHTS				
17	CONCLUSION				
18					
19					
20					
21					
22					
23					
24					
25					
26					
27					
28					
	LAW OFFICES OF JAY LEIDERMAN 5740 Ralston Street, Suite 300 Ventura, California 93003 Page iv Tel: 805-654-0200 Fax: 805-654-0280				

Case 2:13-cr-00082-KJM Document 23 Filed 12/13/13 Page 5 of 31

1

TABLE OF AUTHORITIES

2	Federal Cases
3	Brown v. Illinois, 422 U.S. 590 (1975)
4	Chism v. Washington State, 661 F.3d 380 (9th Cir. 2011) 20
5	Colorado v. Connelly, 479 U.S. 157 (1986)
6	Colorado v. Spring, 479 U.S. 564 (1987)
7	<i>Coolidge v. New Hampshire</i> , 402 U.S. 443 (1971) 10
8	Derrick v. Peterson, 924 F.2d 813 (9th Cir. 1990)
9	Durham v. United States, 403 F.2d 190 (9th Cir. 1968) 16
10	Franks v. Delaware, 438 U.S. 154 (1978) ("Franks")
11	Gladden v. Unsworth, 396 F.2d 373 (9th Cir. 1968) 22, 23
12	In re Grand Jury Subpoenas Dated December 10, 1987, 926 F.2d 847 (9th Cir. 1991) 11
13	Jackson v. Denno, 378 U.S. 368 (1964)
14	Lucero v. Kerby, 133 F.3d 1299 (10th Cir. 1998)
15	Miranda v. Arizona, 384 U.S. 436 (1966) 22, 23, 24
16	Moran v. Burbine, 475 U.S. 412 (1986)
17	Nardone v. United States, 308 U.S. 338 (1939) 21
18	Nix v. Williams, 467 U.S. 431 (1984)
19	Payton v. New York, 445 U.S. 573 (1980) 10
20	Sample v. Eyman, 469 F.2d 819 (9th Cir. 1972)
21	Sgro v. United States, 287 U.S. 206 (1932) 16
22	<i>Tague v. Louisiana</i> , 444 U.S. 469 (1980)
23	<i>Taylor v. Maddox</i> , 366 F.3d 992 (9th Cir. 2004)
24	United States v. Chesher, 678 F.2d 1353 (9th Cir. 1982) 19
25	United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989 (9th Cir. 2009) ("CDT II") 14
26	United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162 (9th Cir. 2010) ("CDT III") 11, 13,
27	14, 15
28	United States v. DeLeon, 979 F.2d 761 (9th Cir. 1992)
	LAW OFFICES OF JAY LEIDERMAN 5740 Ralston Street, Suite 300 Ventura, California 93003 Page v Tel: 805-654-0200

Fax: 805-654-0280

Case 2:13-cr-00082-KJM Document 23 Filed 12/13/13 Page 6 of 31

1	United States v. Dozier, 844 F.2d 701 (9th Cir. 1988) 16
2	United States v. Frank, 956 F.2d 872 (9th Cir. 1991)
3	United States v. Gann, 732 F.2d 714 (9th Cir. 1984) 16
4	United States v. Grant, 682 F.3d 827 (9th Cir. 2012)16
5	United States v. Greany, 929 F.2d 523 (9th Cir. 1991) 16
6	United States v. Greathouse, 297 F.Supp.2d 1264 (D. Or. 2003) 17, 18
7	United States v. Guerrero, 847 F.2d 1363 (9th Cir. 1988)
8	United States v. Hill, 459 F.3d 966 (9th Cir. 2006) 13, 14
9	United States v. Jawara, 474 F.3d 565 (9th Cir. 2007) 19
10	United States v. Lacy, 119 F.3d 742 (9th Cir. 1997) 16, 17
11	United States v. Montoya-Arrubla, 749 F.2d 700 (11th Cir. 1985) 24
12	United States v. Smith, 638 F.2d 131 (9th Cir. 1981) 22
13	United States v. Stanert, 762 F.2d 775 (9th Cir. 1985) 19
14	United States v. Tamura, 694 F.2d 591 (9th Cir. 1982) 12, 13, 14
15	United States v. Towne, 997 F.2d 537 (9th Cir. 1993) 11
16	Wong Sun v. United States, 371 U.S. 471 (1963) 21
17	Statutes
18	18 U.S.C. § 1030
19	18 U.S.C. § 3501
20	18 U.S.C. § 371
21	Constitutional Provisions
22	U.S. Const. amend. IV 1, 11, 13, 14
23	U.S. Const. amend. V
24	
25	
26	
27	
28	
	LAW OFFICES OF JAY LEIDERMAN 5740 Ralston Street, Suite 300 Ventura, California 93003 Page vi Tel: 805-654-0200 Fax: 805-654-0280

<u>MEMORANDUM OF POINTS AND AUTHORITIES</u> <u>INTRODUCTION</u>

This case involves a seizure that goes to the very heart of what the Fourth Amendment prohibits. For no reason other than allowing the FBI to fish for electronic data, a magistrate authorized and the government executed a wholesale seizure of Defendant Matthew Keys' electronic media. The warrant was unsupported by any facts requiring such a seizure and unaccompanied by any protocol designed to prevent a general rummaging, and therefore the seizure violated the Fourth Amendment's prohibition on general warrants.

This general search led directly to a police interview of Mr. Keys, during which he involuntarily waived his Fifth Amendment right against self-incrimination. Additionally, the circumstances surrounding the interview show that Mr. Keys did not participate knowingly, voluntarily, or intelligently. As such, Mr. Keys' statements must be suppressed as violative of his Fifth Amendment rights and of the fruit of the poisonous tree doctrine.

STATEMENT OF FACTS

Mr. Keys was indicted in a three-count indictment in March 14, 2013. (Docket entry # 1.) Count 1 alleges a conspiracy to intentionally cause unauthorized damage to a protected computer via a knowing transmission of a program, information, code, and command, in violation of 18 U.S.C. §§ 371 and 18 U.S.C. §§ 1030(a)(5)(A), (c)(4)(B). Count 2 alleges a substantive violation of 18 U.S.C. §§ 1030(a)(5)(A), (c)(4)(B). And count 3 alleges a knowing attempted transmission of a program, information, code, and command with the intent to cause damage to a protected computer in violation of 18 U.S.C. §§ 1030(a)(5)(A), (b).

These charges stem from edits to one paragraph of a story on the Los Angeles Times website on December 14, 2010. That day, using the Los Angeles Times/Tribune Company's content management system ("CMS"), the user "ngarcia" allegedly altered a paragraph of a latimes.com story. The article's title and byline originally appeared as follows:

Pressure builds in House to pass tax-cut package

House Democratic leader Steny Hoyer sees 'very good things' in the tax-cut deal, which many representatives oppose. But with the bill set to clear the Senate, reluctant House Democrats are feeling the heat to pass it.

> MOTION TO SUPPRESS Page 1

LAW OFFICES OF JAY LEIDERMAN 5740 Ralston Street, Suite 300 Ventura, California 93003 Tel: 805-654-0200 Fax: 805-654-0280 By Lisa Mascaro, Tribune Washington Bureau¹

2 After the minor edits by ngarcia, the article's title and byline allegedly read:

Pressure builds in House to elect CHIPPY 1337

House Democratic leader Steny Hoyer sees 'very good things' in the deal cut which will see uber skid Chippy 1337 take his rightful place, as head of the Senate, reluctant House Democrats told to SUCK IT UP.

By CHIPPYS NO 1 FAN, Tribune Washington Bureau

The article's substantive content was not altered, and website administrators restored the original in less than an hour.

8 9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

I.

1

3

4

5

6

7

THE SEARCH WARRANT AND AFFIDAVIT.

On October 3, 2012, Special Agent Gabriel Andrews ("Andrews") submitted an "Application and Affidavit for Search Warrant" to search Mr. Keys' residence in Seacaucus, New Jersey. (Attached hereto as Def.'s Ex. A.) United States Magistrate Judge Michael A. Hammer signed the warrant. The warrant is in four parts: Attachments A, B, C, and D. Attachment A describes the place to be searched; Attachment B describes the items to be seized; and Attachment C names the alleged offenses for which the government sought evidence.

Attachment D of the search warrant is Andrews' affidavit in support thereof. (See Def.'s Ex. A, Attachment D ("Andrews Aff.").) In October 2010, Mr. Keys was employed at KTXL Fox 40 ("Fox 40") in Sacramento as a "Web Producer." (Andrews Aff. at ¶ 8.) Among other things, Mr. Keys' responsibilities included managing Fox 40's Facebook and Twitter accounts. (*Id.*) Near the end of that month, a Fox 40 employee named Brandon Mercer—referred to in the affidavit only as the "Producer"—allegedly terminated Mr. Keys' employment. (*Id.*) According to Mercer, Mr. Keys then changed the passwords to the Facebook and Twitter accounts, deleted 6,000 followers, and posted headlines from other, competing stations. (*Id.*) After four days, Mercer regained control of the accounts. (*Id.*)

¹ The original article is still available on the Los Angeles Times website, at http://articles.latimes.com/2010/dec/14/news/lapn-hoyer-tax-vote-20101215.

A. EARLY DECEMBER 2010 "SUSPICIOUS" E-MAILS.

Next, Andrews' affidavit describes some "suspicious" e-mails from a number of free e-mail accounts: foxmulder4099@yahoo.co.uk, cybertroll69x@hotmail.com, walterskinner5099@yahoo.co.uk, cancerman4099@yahoo.co.uk, and fox40truthers@gmail.com. (Andrews Aff. at ¶¶ 9-15.) These emails were related to an alleged compromise of the "P2P Server," a server owned by Tribune Media, Fox 40's parent company. (*Id.* at ¶ 7.)

On December 1, 2010, foxmulder4099@yahoo.co.uk allegedly sent Mercer a message suggesting the writer had obtained e-mail addresses of all Fox 40 customers. (Andrews Aff. at \P 9.) The two exchanged several emails, and foxmulder4099 continued to disparage Fox 40's business practices. (*Id.*)

The next day, cybertroll69x@hotmail.com sent Mercer an e-mail. (Andrews Aff. at ¶ 10.) This e-mail contained a forwarded copy of a different e-mail message, allegedly sent from Fox 40 employee "J.H." (*Id.*) The message from J.H. claimed that foxmulder4099 was Mr. Keys. (*Id.*) When questioned about the e-mail by Mercer, J.H. denied sending the message accusing foxmulder4099 of being Mr. Keys. (*Id.*) According to Andrews' affidavit, the person who created the cybertroll69x account claimed to be Mr. Keys, and registered the account using a Sacramento zip code, 95824. (*Id.* at ¶ 11.) Andrews identified IP address 98.208.49.74 as the only address used to access the account. (*Id.*) This address "resolved to a location in Sacramento, California." (*Id.*) Further attempts to identify cybertroll69x were not successful. (*Id.*)

On December 3, Fox 40 received a strange e-mail from CancerMan4099@yahoo.co.ok. (Andrews Aff. at ¶ 12.) Like the previous e-mail, CancerMan4099's e-mail contained a forwarded copy of a different message. (*Id.*) The forwarded message was from the American Cancer Society to CancerMan4099, and it indicated that CancerMan4099 had given his contact name as "Matthew Keys" to the American Cancer Society. (*Id.*) That same day a Fox 40 "customer" reported receiving an unsolicited e-mail from fox40truthers@gmail.com. (*Id.* at ¶ 13.)

Finally, on December 6, 2010, Mercer received an e-mail in the form of a press release from WalterSkinner5099@yahoo.co.uk. (Andrews Aff. at ¶ 14.) This e-mail referred to Mercer's Facebook page. (*Id.*)

Andrews' affidavit explains why he included IP address information for only the

cybertroll69x@hotmail.com account:

"Fox Mulder," "Walter Skinner," and "Cancer Man" are characters from the Fox television show "The X-Files." Subpoenas issued for these accounts determined either that the information was unavailable or that the account used was by a proxy server. Based on my training and experience, I am aware that proxy servers are used by people on the Internet to avoid having their activity traced back to them.

(Andrews Aff. at \P 15.)

Though Andrews' affidavit made no mention of it, FBI agent John Cauthen expressed doubts about Mr. Keys' involvement in the alleged breach of the P2P server. In a report dated Feb 14, 2011, Cauthen wrote a note: "Given the effort to hide the identity of the sender via the use of fake e-mails and proxy servers, it seems incongruous for the subject, if it is indeed Matthew Keys, to send out an e-mail identifying himself by name." (*See* Feb. 11 Report of John Cauthen, attached hereto as Def.'s Ex. B.) The same report mentions that Mr. Keys was himself a victim of a compromised Twitter account. (*Id.*) Based in part on these facts, Cauthen wrote, "it appears Matthew Keys may not have been the subject behind the compromise at FOX40." (*Id.*) Another report dated June 6, 2011 authored by Cauthen expressed similar sentiments. (*See* June 6 Report of John Cauthen, attached hereto as Def.'s Ex. C.) He thought it "illogical that the real hacker would identify himself so obviously while going to such lengths to avoid detection through the use of proxy servers." (*Id.*) He thought Mr. Keys was "genuinely baffled" by allegations he compromised the e-mail server. (*Id.*) Rather, Cauthen viewed Mr. Keys' involvement as "likely only a journalistic interest. (*Id.*)

B. COMMUNICATION BETWEEN MERCER AND MR. KEYS REGARDING ANONYMOUS.

On December 12, 2010, using Matthew@sactownmedia.com, Mr. Keys sent Mercer an e-mail. (Andrews Aff. at \P 16.) In the e-mail, Mr. Keys stated he "had infiltrated the group Anonymous,"² and

² Andrews' affidavit does not elaborate on who or what the group Anonymous is. A proper treatment would require volumes, but for the purposes of this Motion it suffices to describe Anonymous as an informal international collective of digital activists. They are known for the high-profile "hacktivist" (a portmanteau of hacker and activist) actions of some of the members.

told Mercer he "had access to future Anonymous operations, including against the Los Angeles Times. (*Id.*)

Around the same time, Mercer and Mr. Keys spoke by phone. (Andrews Aff. at ¶ 17.) According to Mercer, Mr. Keys claimed he had access to a private chat room with "15 highly skilled hackers" affiliated with Anonymous. (*Id.*) Mercer confronted Mr. Keys about the suspicious e-mails discussed above, and Mr. Keys denied any involvement. (*Id.*)

C. INTERNAL INVESTIGATION OF THE DECEMBER 14, 2010 EDITS TO THE LOS ANGELES TIMES WEBSITE.

Andrews' affidavit states that based on an internal investigation, the person who altered the Los Angeles Times headline used Tribune CMS accounts "Anon1234" and "Arseface." (Andrews Aff. at ¶ 18.) And a Tribune employee observed a user named "sharpie" taking credit for the edits in some "Anonymous IRC channels." (*Id.*)

D. MR. KEYS PUBLISHED ARTICLES ACKNOWLEDGING ACCESS TO "TOP LEVEL HACKERS" USING THE NAME "AESCracked."

In March and June 2011, Mr. Keys published articles on his website, producermatthew.com, acknowledging that he had access to the private "internetfeds" chatroom, that he had provided the Gawker website (gawker.com) with "one of dozens of logs" taken during that access, that he had identified himself as a journalist, and that he had observed the notorious "Sabu" in the chatroom. (Andrews Aff. at ¶¶ 19-20.) Mr. Keys also acknowledged providing screenshots to Parmy Olson, author of *We Are Anonymous* [Little, Brown and Co, 2012]. (*Id.* at ¶¶ 27-28.)

On March 6, 2011, Mr. Keys published a screenshot of his participation in the chatroom. (Andrews Aff. at ¶ 21.) Two images of this screenshot are attached as exhibits to Andrews' affidavit. (*See id.*) The screenshot shows Colloquy, a chat program, in a chatroom. (*Id.*) Although Mr. Keys' username was mostly blurred, the screenshot appears to show that it ended with a "d" and that another user referred to the username as "AES." (*Id.*)

Е.

CHAT LOGS SEIZED DURING OTHER INVESTIGATIONS.

In December 2011, investigators discovered a chat log seized pursuant to a search warrant in which the username "Kayla" expresses a belief that Mr. Keys was AESCracked. (Andrews Aff. at ¶ 22.)

LAW OFFICES OF JAY LEIDERMAN 5740 Ralston Street, Suite 300 Ventura, California 93003 Tel: 805-654-0200 Fax: 805-654-0280

Kayla also wrote, "lol he's not so innocent and we have logs of him too, he was the one who gave us passwords for the LA times, fox40 and some others, he had superuser on a lot of media."

Around the same time, Andrews discovered logs obtained during a different search of "digital media" belonging to a person alleged to have used the name "Owen" and "Iowa." (Andrews Aff. at ¶ 23.) In these logs, AESCracked says, "i'm not a hacker. [¶] i'm an ex-employee . . . user: anon1234 [¶] pass: common2 [¶] go fuck some shit up!" (*Id.*) This username/password combination allegedly granted access to the Tribune Company CMS. (Id. at ¶ 24.) Other logs from this seizure, attached to the affidavit as Exhibit C, suggest that (a) AESCracked asked if anyone was interested in defacing the LA Times; (b) AESCracked claimed to be an ex-employee; (c) AESCracked asked if anyone wanted to purchase an e-mail list; and (4) AESCracked did all this in the "internetfeds" and "Operation Payback" chatrooms. (*Id.*)

F.

OTHER IP ADDRESS INFORMATION.

Andrews' affidavit states that at an unspecified date and time in January 2011 AESCracked used IP address 78.129.220.46 to connect to a channel on the AnonOps chat server. (Andrews Aff. at ¶ 25.) This address "was the one used by the sender of an e-mail from 'foxmulder4099@yahoo.co.uk' to Fox 40 as described ... above." (Id.) On January 5, 2011, shortly after AESCracked was banned from the same server, "A2SCracked" connected using IP address 75.53.171.204, which was allegedly registered to Mr. Keys at the time. (*Id.* at \P 25.)

G. JUSTIFICATION FOR THE BREADTH OF THE SEARCH.

Attachment B to the warrant application provides a boilerplate list of the items Andrews sought to "search, copy, image and seize":

- a. Any computer equipment or digital devices belonging to MATTHEW KEYS that are capable of being used to commit the Specified Federal Offenses, or to create, access, or store evidence, or instrumentalities of such crimes, as set forth in Attachment B;
- b. Any computer equipment or digital devices belonging to MATTHEW KEYS used to facilitate the transmission, creation, display, encoding, or storage of data, including word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices, and optical scanners that belong to KEYS and are capable of

being used to commit or further the crimes outlined above, or to create, access, process, or store evidence and instrumentalities of such crimes, as set forth in Attachment B;

- c. Any magnetic, electronic, or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, personal digital assistants, and cell phones belonging to MATTHEW KEYS that are capable of being used to commit or further the crimes outlined above, or to create, access, or store evidence and instrumentalities of such crimes, as set forth in Attachment B;
- d. Any documentation, operating logs, and reference manuals regarding the operation of the computer equipment, storage devices, or software belonging to MATTHEW KEYS;
- e. Any applications, utility programs, compilers, interpreters, and other software belonging to MATTHEW KEYS used to facilitate direct or indirect communication with the computer hardware, storage devices, or data belonging to KEYS to be searched;
- f. Any physical keys, encryption devices, dongles, or similar physical items belonging to MATTHEW KEYS which are necessary to gain access to KEYS's computer equipment, storage devices, or data;
- g. Any passwords, password files, test keys, encryption codes, or other information belonging to MATTHEW KEYS necessary to access the computer equipment, storage devices, or data; and
- h. All records, documents, programs, applications, or materials created, modified, or stored in any form, including digital form, on any computer or digital devices belonging to MATTHEW KEYS, that show the actual user(s) of the computers or digital devices during any time period in which the device was used to commit the crimes referenced above, including the web browser's history; temporary Internet

Case 2:13-cr-00082-KJM Document 23 Filed 12/13/13 Page 14 of 31

files; cookies, bookmarked, or favorite web pages; email addresses used from the computer; MAC IDs and/or Internet Protocol addresses used by the computer; email, instant messages, and other electronic communications; address books; contact lists; records of social networking and online service usage; and software that would allow others to control the digital device such as viruses, Trojan horses, and other forms of malicious software (or alternatively, the lack of software that would allow others to control the device).

- All records, documents, programs, applications, or materials created, modified, or stored in any form, including digital form, on any computer or digital device belonging to MATTHEW KEYS, that show evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the computer or digital device.
 - j. All records, documents, programs, applications, or materials created, modified, or stored in any form, including in digital form, on any computer or digital device belonging to MATTHEW KEYS, that show contextual information necessary to understand the evidence, contraband, fruits, or instrumentalities described in Attachment B.

(See Def.'s Ex. A, Attachment B.) Andrews offered the following boilerplate justification for this broad seizure:

a. Searching computer systems is a highly technical process which requires specific expertise <u>and</u> specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application or operating system that is being searched.

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased,

LAW OFFICES OF JAY LEIDERMAN 5740 Ralston Street, Suite 300 Ventura, California 93003 Tel: 805-654-0200 Fax: 805-654-0280

compressed, encrypted or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted.

- c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 gigabytes (GB) of data are now commonplace in desktop computers. Consequently, each non-networked, desktop computer found during a search can easily contain the equivalent of 250 million pages of data, which, if printed out, would result in a stack of paper over ten miles high. Further, a 500 GB drive could contain as many as approximately 250 full run movies or 450,000 songs.
- d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt." to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "stenography." For example, by using stenography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract

and sort through the data that is concealed or encrypted to determine whether it is evidence, contraband, or instrumentalities of a crime.

(Andrews Aff. at ¶ 37.) "In light of these concerns," Andrews requested permission to "search, copy, image and seize the computer hardware (and associated peripherals) that are believed to contain some or all of the evidence described in this warrant, and to conduct an off-site search of the image" (Id. at ¶ 38, 38d.)

II.

EXECUTION OF THE WARRANT.

On October 4, 2012, agents conducted the seizure authorized by the warrant at Mr. Keys' residence. The agents seized one laptop computer and two external hard drives. They also took a number of photographs and conducted a recorded interview of Mr. Keys.

At about 1:30 am the night before the execution of the search warrant, Mr. Keys ate a snack and took two 50 mg doses of Trazodone, also known as Desyrel, an anti-depressant often prescribed to induce sleep. (Decl. of Matthew Keys ("Keys Decl.") at ¶¶ 3, 4; see also Decl. of Dr. Barry Cogen ("Cogen Decl.") at \P 4.) The common side effects of Trazodone include confusion, fatigue, and nervousness. (Cogen Decl. at ¶ 7.) Mr. Keys fell asleep between 2:00 and 2:30 am. (Keys. Decl. at ¶ 5.) Awoken before 6:00 from a "deep sleep" by federal agents, he was "drowsy, confused and forgetful." (Id. at ¶¶ 7, 9.) Agents encouraged and obtained written and oral statements from Mr. Keys, despite the fact that Mr. Keys had expressed concerns about his state of mind. (Id. at ¶ 8.)

28

I.

THE SEARCH WARRANT AUTHORIZED AN OVERBROAD GENERAL SEARCH OF ALL OF MR. KEYS' ELECTRONIC MEDIA.

ARGUMENT

By permitting the seizure of every conceivable type of electronic media, the October 3, 2012 search warrant was unconstitutionally overbroad and the modern equivalent of a general warrant. "It is familiar history that indiscriminate searches and seizures conducted under the authority of 'general warrants' were the immediate evils that motivated the framing and adoption of the Fourth Amendment." Payton v. New York, 445 U.S. 573, 583 (1980); see also Coolidge v. New Hampshire, 402 U.S. 443, 467 (1971) (the "specific evil . . . abhorred by the colonists . . . is not that of intrusion per se, but of a general, exploratory rummaging in a person's belongings"). To prevent the abuse of such indiscriminate

> LAW OFFICES OF JAY LEIDERMAN 5740 Ralston Street, Suite 300 Ventura, California 93003 Tel: 805-654-0200 Fax: 805-654-0280

Case 2:13-cr-00082-KJM Document 23 Filed 12/13/13 Page 17 of 31

rummaging, the Fourth Amendment requires each warrant to "particularly describ[e] the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. That is, search warrants must be specific. *United States v. Towne*, 997 F.2d 537, 544 (9th Cir. 1993). "Specificity has two aspects: particularity and breadth." *Id.* (quoting *In re Grand Jury Subpoenas Dated December 10, 1987*, 926 F.2d 847, 856-57 (9th Cir. 1991)). Not only must a warrant "clearly state what is sought," but its scope must also be "limited by the probable cause on which the warrant is based." *Id.* (same).

The Fourth Amendment's specificity requirements make computer searches especially difficult. On one hand, computers are particularly vulnerable to general rummaging. A single computer, hard disk, or USB drive may contain information about every aspect of a person's life. Even cheap storage media can store millions of pages of information, personal pictures, and intimate details of one's life. Moreover, the content of a computer file may not be obvious without opening the file itself. The government's inability to determine whether a file is concealed, compressed, erased, or booby-trapped without examining it creates a "powerful incentive to seize more rather than less: . . . Let's take everything back to the lab, have a good look around and see what we might stumble on." *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1170-71 (9th Cir. 2010) (en banc) (per curiam) ("*CDT III*"). The very nature of computer searches raises the ominous specter of general warrants.

On the other hand, it may be difficult for an officer applying for a search warrant to be very specific. How many computers or storage devices does the suspect possess? And which ones are likely to contain evidence? Did the suspect use a laptop computer, a tablet, or a smartphone? Further, the technical aspects of computer searches can be complicated. Sorting through gigabytes of information takes time. Information may be encrypted or otherwise unreadable. In rare instances, some hardware or software "may contain 'booby traps' that destroy or alter data if certain procedures are not scrupulously followed." As such, courts have recognized a "legitimate need to scoop up large quantities of data, and sift through it carefully for concealed or disguised pieces of evidence" *CDT III*, 621 F.3d at 1176. This need, however, does not yield to the Fourth Amendment.

MOTION TO SUPPRESS Page 11

A. IN ORDER TO CONDUCT WHOLESALE SEIZURES OF ELECTRONIC MEDIA, THE GOVERNMENT MUST PRESENT A FACTUAL BASIS FOR DOING SO, IT MUST FOLLOW A SEGREGATION PROTOCOL FOR IDENTIFYING RELEVANT INFORMATION, AND IT MUST RETURN IRRELEVANT INFORMATION.

To prevent every warrant authorizing a computer search from functioning as a general warrant, the Ninth Circuit requires such warrants follow a number of rules: (1) the government must provide a factual justification for a broad search and seizure of the computer; (2) the search must be monitored by a neutral, detached magistrate; (3) the government must seal and hold documents pending judicial approval of a further search; (4) large-scale removal is only appropriate where on-site sorting is infeasible and no there is no practical alternative; (5) the government must promptly return documents outside the scope of the search.

These rules have their roots in a case decided before computers were commonplace. In *United States v. Tamura*, 694 F.2d 591 (9th Cir. 1982), the FBI served a warrant on a business' accounting department for specific records. When the business' employees refused to help the agents locate the specific records the warrant authorized them to seize, the agents seized all of the records for the years in question. *Id.* at 594-95. Despite taking "large quantities" of documents not described in the warrant, the government argued the search was nevertheless reasonable because "the documents were intermingled and it was difficult to separate the described documents from the irrelevant ones." *Id.* at 595. The court rejected this argument:

It is true that all items in a set of files may be inspected during a search, provided that sufficiently specific guidelines for identifying the documents sought are provided in the search warrant and are followed by the officers conducting the search. However, the wholesale *seizure* for later detailed examination of records not described in a warrant is significantly more intrusive, and has been characterized as 'the kind of investigatory dragnet that the fourth amendment was designed to prevent.' We cannot sanction the procedure followed by the Government in this case.

Id. (emphasis in original) (internal footnote and citations omitted).

The *Tamura* court provided guidance for the "comparatively rare" times when information "cannot feasibly be sorted on site." *Tamura*, 694 F.2d at 595-96. The government should seal and hold the documents pending judicial approval for a further search. *Id.* A magistrate should grant prior

> LAW OFFICES OF JAY LEIDERMAN 5740 Ralston Street, Suite 300 Ventura, California 93003 Tel: 805-654-0200 Fax: 805-654-0280

approval for "large-scale removal of material . . . *only where on-site sorting is infeasible and no other practical alternative exists.*" *Id.* at 969 (emphasis added). "The essential safeguard required is that
wholesale removal must be monitored by the judgment of a neutral, detached magistrate." *Id.* (footnote
omitted). Although such wholesale seizures may be more convenient without judicial participation, they
are not reasonable. *Id.* Moreover, the government must return out-of-scope documents after
segregation: any "unnecessary delay" may result in an "unreasonable and therefore unconstitutional
manner of executing the warrant." *Id.* at 597.

Nearly twenty-five years later, in *United States v. Hill*, 459 F.3d 966, 973 (9th Cir. 2006), the Ninth Circuit revisited *Tamura* in the context of a broad seizure of "all computer media."

Acknowledging "significant problems" inherent in computer searches, the court nevertheless refused to give the government an "automatic blank check" for broad computer searches and seizures. *Id.* at 974-75. Rather, to justify a wholesale seizure of electronic media, "the government must still demonstrate to the magistrate *factually* why such a broad search and seizure authority is reasonable in the case at hand." *Id.* at 975 (emphasis in original). The court recognized that in some cases, the government will have "no basis" for believing they will actually encounter "the kind of technological problems that would make an immediate onsite search and selective removal of relevant evidence impracticable." *Id.* To give teeth to this preference for onsite searches over wholesale seizure, *Hill* requires "some threshold showing before the government may 'seize the haystack to look for the needle." *Id.*

Most recently, in *CDT III*, 621 F.3d 1162, an en banc panel of the Ninth Circuit again applied *Tamura*'s logic to computer searches. "The point of *Tamura* procedures is to maintain the privacy of materials that are intermingled with seizable materials, and to avoid turning a limited search for particular information into a general search" *Id.* at 1170. While the government has a "legitimate need" for broad computer searches, that need "creates a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant." *Id.* at 1176. To balance the needs of law enforcement with the privacy "at the heart of the Fourth Amendment," the en banc panel's per curiam opinion endorsed *Tamura* as a "workable framework." *Id.* at 1177.

LAW OFFICES OF JAY LEIDERMAN 5740 Ralston Street, Suite 300 Ventura, California 93003 Tel: 805-654-0200 Fax: 805-654-0280 Here, the government failed to follow the Ninth Circuit's precedents in *Tamura*, *Hill*, and *CDT III*. The wholesale seizure of Mr. Keys' electronic media was not monitored by a neutral, detached magistrate. Nor did the government take any precautionary measures to prevent a general search.
Rather the government seized everything so they could rummage in Mr. Keys' personal and professional life at their leisure. The agents did not return any irrelevant documents or data to Mr. Keys until counsel received discovery. These failures violated the protective measures required by *Tamura* and *CDT III*.

Furthermore, Andrews' boilerplate affidavit describes the difficulty of computer searches in general terms, rather than in specific factual terms that apply to Mr. Keys case. It provides no basis to anticipate the need for any exotic forensic equipment or specialized personnel. Worse, Andrews can point to no reason to believe Mr. Keys' data would be hidden or protected by sophisticated booby traps. Rather, the evidence in the affidavit suggests Mr. Keys was a run-of-the-mill Mac user without any special "hacking" skills. And while the data in modern storage media is often voluminous, and the content of a file may not be apparent until it is opened, neither of these facts explain why the FBI chose to seize everything, rather than simply copying the files. In short, the affidavit fails to provide a factual basis for wholesale seizure in this case, as *Hill* requires.

В.

THE WARRANT COMPLETELY IGNORES CHIEF JUDGE KOZINSKI'S GUIDELINES IN *COMPREHENSIVE DRUG TESTING III*.

Moreover, to assist government agents performing computer searches and seizures, Chief Judge Alex Kozinski's five-judge concurrence in *Comprehensive Drug Testing III* provides five concrete guidelines, none of which were followed here. Chief Judge Kozinski's guidelines are based largely on the reasoning in the court's per curiam opinion. While not law,³ they are intended to provide the government "a safe harbor," while at the same time protecting the values of the Fourth Amendment. *CDT III*, 621 F.3d at 1178 (Kozinski, C.J., concurring). In short form, these guidelines are:

 ³ Chief Judge Kozinski's guidelines were originally included in the panel's majority opinion. See United States v.
 Comprehensive Drug Testing, Inc., 579 F.3d 989, 1004-07 (9th Cir. 2009) ("*CDT II*"). However, the opinion was subsequently revised, and the guidelines were moved to the plurality's concurrence. See CDT III, 621 F.3d at 1183 (Callahan, J., concurring in part and dissenting in part) ("The concurrence is not joined by a majority of the en banc panel and accordingly the suggested guidelines are not Ninth Circuit law.").

- Magistrate judges should insist that the government waive reliance upon the plain view doctrine in digital evidence cases.
- 2. Segregation and redaction of electronic data must be done either by specialized personnel or an independent third party. If the segregation is to be done by government computer personnel, the government must agree in the warrant application that the computer personnel will not disclose to the investigators any information other than that which is the target of the warrant.
- 3. Warrants and subpoenas must disclose the actual risks of destruction of information as well as prior efforts to seize that information in other judicial fora.
- 4. The government's search protocol must be designed to uncover only the information for which it has probable cause, and only that information may be examined by the case agents.
- 5. The government must destroy or, if the recipient may lawfully possess it, return nonresponsive data, keeping the issuing magistrate informed about when it has done so and what it has kept.

Id. at 1180 (same) (internal citations omitted).

The government ignored these guidelines. First, neither the government nor the authorizing magistrate made any mention of the plain view doctrine. Although Defendant does not expect the government to rely on the plain view doctrine in this case, the failure to acknowledge the slippery slope of electronic plain view demonstrates a disregard for the guidelines. Second, the government did not use "specialized personnel" or an "independent third party" to segregate relevant from irrelevant data. Instead, the government seized all of Mr. Keys' media and removed it for leisurely rummaging. Third, the warrant provides no particular basis for the conjecture that there might be hidden, encrypted, or booby-trapped data. Andrews' affidavit identified no "actual risks" of information destruction, and no *facts* supporting the proposition that Mr. Keys' equipment or data may have been booby-trapped. Indeed, it fails to justify anything more intrusive than plugging in an external USB drive and copy/pasting data. Fourth, the warrant contains no particular search protocol. As a result, the government's general search and seizure swept up large volumes of information without probable cause.

LAW OFFICES OF JAY LEIDERMAN 5740 Ralston Street, Suite 300 Ventura, California 93003 Tel: 805-654-0200 Fax: 805-654-0280

And fifth, the government has kept all information it seized. Although Mr. Keys has received a copy of
 his own data, he was required to provide his own media. Nothing has been returned; indeed, the
 indictment seeks forfeiture of all electronic media seized pursuant to the warrant, without regard for its
 relevance.

In sum, the October 3, 2012 warrant in this case authorized seizure of every conceivable kind of electronic media, with no particularized search protocols or other safeguards to segregate relevant from irrelevant information. It authorized the modern equivalent of a general search. The warrant was unconstitutionally overbroad, and its fruits must be suppressed.

II. <u>AT THE TIME ANDREWS APPLIED FOR THE WARRANT, THE FACTS</u> <u>SUPPORTING PROBABLE CAUSE TO BELIEVE MR. KEYS POSSESSED ANY</u> EVIDENCE WERE STALE.

Aside from the overbreadth problem, the facts in Special Agent Andrews' supporting affidavit were simply too stale to support the proposition that the October 4, 2012 search would turn up any evidence of wrongdoing. Under the staleness doctrine, an affidavit supporting a search warrant "must be based on facts so closely related to the time of the issue of the warrant as to justify a finding of probable cause at that time." United States v. Lacy, 119 F.3d 742, 745 (9th Cir. 1997) (quoting Durham v. United States, 403 F.2d 190, 193 (9th Cir. 1968); Sgro v. United States, 287 U.S. 206, 210, 53 S.Ct. 138, 140 (1932)) (emphasis added) (internal quotation marks omitted). Staleness is evaluated "in light of the particular facts of the case and the nature of the criminal activity and property sought." United States v. Greany, 929 F.2d 523, 525 (9th Cir. 1991). Thus, while a "significant gap in time can diminish the probability that the evidence will be uncovered in the search," see United States v. Grant, 682 F.3d 827, 835 (9th Cir. 2012), the "mere lapse of substantial amounts of time is not controlling in a question of staleness." United States v. Dozier, 844 F.2d 701, 707 (9th Cir. 1988). Instead, the warrant should be upheld if there is a "sufficient basis to believe, based on a continuing pattern or other good reasons, that the items to be seized are still on the premises." United States v. Gann, 732 F.2d 714, 722 (9th Cir. 1984). Where "the evidence sought is of an ongoing criminal business of a necessarily long-term nature, ... rather than that of a completed act, greater lapses of time are permitted " Greany, 929 F.2d at 525.

Case 2:13-cr-00082-KJM Document 23 Filed 12/13/13 Page 23 of 31

Andrews' affidavit provides no reason to suspect any "ongoing criminal business" justifying the lapse of time between the date of the crime, December 14, 2010, and the date of the warrant, October 3, 2012. The nearly 22-month delay is too long to support the search. *See United States v. Greathouse*, 297 F.Supp.2d 1264, 1272 (D. Or. 2003) (finding a thirteen month delay in Internet child pornography cases "simply too long . . . absent evidence of ongoing or continuous criminal activity"). Although at least one court has upheld a search for child pornography after a ten-month delay, that search was upheld because the affidavit in support of the warrants "provided 'good reason' to believe" the evidence would still be present. *See Lacy*, 119 F.3d 742, 746.

Here, Andrews' speculative justifications for the delay fall short of establishing probable cause that Mr. Keys retained evidence. He stated his belief that Mr. Keys would retain such evidence for so long because:

- (1) . . . there is probable cause to believe that KEYS participated in committing the Specified Federal Offenses;
- (2) evidence of Specified Federal Offenses, including the chat logs discussed in paragraph 21
 (*see also* Exhibits A and B attached hereto) was retained on KEYS's computer as recently as
 March 6, 2012, post-dating his move from Sacramento, California to Seacaucus, New Jersey;
 - (3) KEYS presently maintains the website www.producermatthew.com, on which he has stated that he actively monitors the Internet and updates his website from his residence;
- (4) based on my training and experience, and the investigation to date, I know that KEYS is proficient with computers and related technology, and that individuals such as KEYS generally retain their computers and attendant digital media when moving from one residence to another; and
- (5) based on my training and experience, I am aware that data, even if deleted, will remain on a computer until overwritten.

Andrews further stated his belief that Mr. Keys would retain data from his interaction with Anonymous at home because "he regards this as an accomplishment that he wants to publish and receive credit for in the future."

LAW OFFICES OF JAY LEIDERMAN 5740 Ralston Street, Suite 300 Ventura, California 93003 Tel: 805-654-0200 Fax: 805-654-0280

Case 2:13-cr-00082-KJM Document 23 Filed 12/13/13 Page 24 of 31

These justifications fail for at least three reasons. First, and most obviously, there is "simply no evidence presented here of any ongoing criminal activity." *Greathouse*, 297 F.Supp.2d at 1272. Probable cause that Mr. Keys participated in the LA Times edit is not itself probable cause that Mr. Keys would have evidence of it 22 months later, after a cross-country move. Second, the screenshot Mr. Keys posted to his website on March 6, 2012 was a screenshot, not "chat logs." There is no evidence Mr. Keys ever recorded or kept any such chat logs. And just because a single file is published on a website does not mean that similar files reside on personal computing equipment, even where the administrator updates the site remotely from home. Third, and most troubling, Andrews' affidavit relies on crude stereotypes of computer users and journalists. According to Andrews, "individuals such as KEYS"—those allegedly "proficient with computers and related technology"—are more likely to retain storage media for long periods of time. Similarly, because Mr. Keys was acting as a journalist during his interactions with Anonymous, Andrews' hypothesized that he held on to his data to "receive credit for it in the future." These generalizations lack foundation. The government cannot neuter the staleness doctrine for all journalists and other computer-proficient people on such a flimsy basis, without regard for the facts of the case.

In short, by October 3, 2012, government agents no longer had probable cause to suspect that Mr. Keys possessed any evidence of the crime. Andrews failed to demonstrate any evidence of ongoing criminal activity, and his assertions that agents would find evidence of prior criminal activity were based on sleight-of-hand and crude generalizations. Under these circumstances, the warrant should be quashed and all evidence obtained therefrom suppressed.

 III.
 <u>THE AFFIDAVIT CONTAINS DELIBERATE OR RECKLESS</u>

 MISREPRESENTATIONS AND OMISSIONS REQUIRING A FRANKS HEARING.

It is well-settled that a defendant may challenge a warrant by challenging the truthfulness of statements therein. Where a defendant (1) "makes a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard of the truth, was included by the affiant in the warrant affidavit," and (2) demonstrates that "the allegedly false statement is necessary to the finding of probable cause, the Fourth Amendment requires that a hearing be held at the defendant's request." *Franks v. Delaware*, 438 U.S. 154, 155-56 (1978) ("*Franks*"). To obtain a *Franks* hearing,

MOTION TO SUPPRESS Page 18 LAW OFFICES OF JAY LEIDERMAN 5740 Ralston Street, Suite 300 Ventura, California 93003 Tel: 805-654-0200 Fax: 805-654-0280

the defendant need not demonstrate "clear proof" of deception; the question of proof is "reserved for the evidentiary hearing." United States v. Stanert, 762 F.2d 775, 781 (9th Cir. 1985) (citing United States v. Chesher, 678 F.2d 1353, 1362 (9th Cir. 1982)). Franks hearings are not limited to showings of false 3 4 affirmative statements, but are also appropriate where a warrant affidavit contains "deliberate or reckless" omissions of facts that tend to mislead." Stanert, 762 F.2d at 780-81; see also United States v. Jawara, 474 F.3d 565, 582 (9th Cir. 2007) (affirming *Stanert*). Where a warrant is challenged for omissions 6 tending to mislead, probable cause must be reconsidered with the omitted information included. United 8 States v. DeLeon, 979 F.2d 761, 764 (9th Cir. 1992).

> ANDREWS' AFFIDAVIT CONTAINS DELIBERATE OR RECKLESSLY-MADE A. STATEMENTS AND OMISSIONS.

The search warrant affidavit contains two misleading material omissions. First, Andrews omitted any reference to FBI agent John Cauthen's documented belief that Mr. Keys was not responsible for the "suspicious e-mails" sent to Fox 40 in early December, 2010. Cauthen's reports provide compelling reasons to believe Mr. Keys was not responsible. It would have been "incongruous" and "illogical" for Mr. Keys to disclose his identity in the suspicious e-mails. Indeed, Mr. Keys was "genuinely baffled" by the idea. Cauthen's opinion was that Mr. Keys' interest in the hacking community was "journalistic," not criminal. Yet none of this information was disclosed in Andrews' affidavit.

Second, Andrews' selective use of IP address information overstates the precision of that evidence. First, in discussing the "suspicious e-mails," despite investigating each of them, Andrews identified only a single IP address which he claims "resolved to a location in Sacramento, California."⁴ Mr. Keys lived in Sacramento at the time and used AT&T as an Internet Service Provider. Yet documents received in discovery indicate that this IP address was administered by Comcast. (See Comcast Response to Government Subpoena, Def.'s Ex. D.) Andrews' inclusion of this IP address and its alleged location were calculated to implicate Mr. Keys, despite other evidence that did not point to

27 28

1

2

5

7

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

⁴ Andrews explained that "[s]ubpoenas for these [other] accounts determined either that the information was unavailable or that the account used was by a proxy server." (Andrews Aff. at ¶ 15.) He offered no further details.

him at all. Second, the only IP address Andrews tied to the "AESCracked" nickname was 78.129.220.46, which fortuitously was allegedly also used by foxmulder4099@yahoo.co.uk. Presumably, this is the IP address of a proxy server, which "acts as an intermediary for requests from clients seeking resources from other servers." (Andrews Aff. at ¶ 4f.) But neither Andrews' description of a proxy server nor his discussion of this IP address includes the fact that proxy servers often serve as proxies for many people at a time. Nor does Andrews make any effort to explain the month-long gap in time between foxmulder4099's use of the IP address and AESCracked's use of the IP address, or how that time lapse affects the analysis. In short, Andrews' use of IP address information was calculated to highlight information pointing to Mr. Keys while minimizing information suggesting someone else was responsible.

These omissions were not merely negligent. Andrews knew or should have known of Cauthen's opinions of the case. And his use of IP address information supports a finding of reckless or intentional omission "because the false statements and omissions contained in the affidavit all *bolster* the case for probable cause, which suggests the mistakes were not the product of mere negligence." *Chism v. Washington State*, 661 F.3d 380, 388 (9th Cir. 2011). As one district court recently acknowledged, "[m]uch, if not all, of the cyber-evidence (the E-mail addresses and IP addresses used) will lead you to an innocent person." *Id.* at 391 (quoting Washington State Police training materials with approval). Andrews singled out such "cyber-evidence" when it implicated Mr. Keys, but ignored it when it did not. *Cf. id.* at 388 (finding it "conspicuous that . . . the omissions purged the affidavit of any reference to the possibility that someone other than [the defendant] was responsible for the offending [computer-related crimes]"). These omissions satisfy *Franks*' first prong.

B.

WITH THE FALSE STATEMENTS AND OMISSIONS CORRECTED, THE AFFIDAVIT DOES NOT SUPPORT A FINDING OF PROBABLE CAUSE.

With Cauthen's opinions and a complete picture of IP addresses included, a reasonable magistrate would be unlikely to find probable cause. A straightforward affidavit would included Cauthen's prior belief that Mr. Keys neither compromised the P2P server nor sent any of the "suspicious e-mails." This fatally undermines the probative value of those e-mails.

LAW OFFICES OF JAY LEIDERMAN 5740 Ralston Street, Suite 300 Ventura, California 93003 Tel: 805-654-0200 Fax: 805-654-0280

MOTION TO SUPPRESS Page 20

What is left of the affidavit? (1) Mr. Keys' acknowledgements that, working as a journalist, he had "infiltrated" a private Anonymous chatroom; and (2) excerpts of chat logs allegedly seized from other systems which allegedly belonged to some other people who were also allegedly in the same chatroom during the some of the same times as "AESCracked." Obviously, Mr. Keys' acknowledgement that he had infiltrated Anonymous as a journalist does not itself implicate him in any criminal activity; it is merely an admission of journalism. Journalism is not a crime. The chat logs, seized pursuant to other investigations with no clear connection to this case or to Mr. Keys, are unaccompanied by any facts supporting their authenticity or reliability. Even combined with Mr. Keys' admissions that he had participated in some chats, the logs do not support probable cause to believe that Mr. Keys was indeed responsible for any crimes.

In sum, Mr. Keys has made a "substantial preliminary showing" that Andrews' affidavit contains deliberate or recklessly-made material omissions. With the omissions corrected, the affidavit does not provide probable cause to suspect Mr. Keys of any criminal activity. Therefore, he is entitled to a *Franks* hearing.

IV. <u>THE FRUIT OF THE POISONOUS TREE DOCTRINE REQUIRES SUPPRESSION OF</u> <u>WRITTEN AND RECORDED STATEMENTS OF MR. KEYS.</u>

It is well-established that statements obtained as a result of an unlawful search or seizure must be suppressed. Such statements have been dubbed "fruit of the poisonous tree." *Nardone v. United States*, 308 U.S. 338, 341 (1939); *Wong Sun v. United States*, 371 U.S. 471 (1963). Unless the government can "purge the primary taint" by showing it would have inevitably obtained the statements from an independent source, the statements are inadmissible. *Brown v. Illinois*, 422 U.S. 590, 600 (1975); *see also Nix v. Williams*, 467 U.S. 431, 443 (1984) ("The independent source doctrine allows admission of evidence that has been discovered by means wholly independent of any constitutional violation.").

In this case, the police interview was a direct result of the search and seizure. There is no reason to believe the government could have obtained statements from Mr. Keys without first obtaining and executing its unlawfully overbroad general warrant. Mr. Keys' statements are fruit of the poisonous tree and must be suppressed.

> LAW OFFICES OF JAY LEIDERMAN 5740 Ralston Street, Suite 300 Ventura, California 93003 Tel: 805-654-0200 Fax: 805-654-0280

MOTION TO SUPPRESS Page 21

1 ||

2

3

V.

MR. KEYS' MIRANDA WAIVER WAS INVALID BECAUSE IT WAS NOT VOLUNTARY, KNOWING AND INTELLIGENT.

Independently, the written and recorded statements obtained during the execution of the October 3, 2012 search warrant must be suppressed because they were taken in violation of *Miranda v. Arizona*, 384 U.S. 436, 86 S.Ct. 1602 (1966). A defendant in a criminal case is deprived of due process of law if his conviction is founded, in whole or in part, upon an involuntary confession. *See Jackson v. Denno*, 378 U.S. 368, 376 (1964). A defendant who objects to the admission of a confession on the ground that it was involuntary has a constitutional right to an evidentiary hearing to determine the voluntariness of the confession before it is heard by a jury. *Id.* at 376-77.

Before the government may introduce a defendant's custodial, incriminating statements, it must prove that the defendant voluntarily, knowingly, and intelligently waived his rights. *See Miranda*, 384 U.S. at 475; *Colorado v. Spring*, 479 U.S. 564, 573, 107 S.Ct. 851 (1987); *Derrick v. Peterson*, 924 F.2d 813, 820 (9th Cir. 1990) (noting that a court must also find that the defendant understood his rights). When a defendant challenges a *Miranda* waiver, the government must prove such waiver by a preponderance of the evidence. *Colorado v. Connelly*, 479 U.S. 157, 168, 107 S.Ct. 515 (1986).

A. MR. KEYS INVOLUNTARILY WAIVED HIS *MIRANDA* RIGHTS.

A statement is involuntary if it is "extracted by any sort of threats or violence [or] obtained by any direct or implied promises, however slight, [or] by the exertion of any improper influence." *United States v. Guerrero*, 847 F.2d 1363, 1366 (9th Cir. 1988) (citation and internal quotation omitted). "A confession is not voluntary if it is made by a person whose mental condition at the time was such that the confession most probably was not the product of any meaningful act of volition." *United States v. Smith*, 638 F.2d 131, 133 (9th Cir. 1981) (citation and internal quotation omitted). Courts have held that incriminating statements made by an intoxicated defendant were involuntary and inadmissible. *See Gladden v. Unsworth*, 396 F.2d 373, 380 (9th Cir. 1968).

In order to determine whether a statement is voluntary, the court must weigh "whether, considering the totality of the circumstances, the government obtained the statement by physical or psychological coercion or by improper inducement so that the suspect's will was overborne." *Derrick v. Peterson*, 924 F.2d at 817 (citation and internal quotation omitted). Courts will also consider factors

> LAW OFFICES OF JAY LEIDERMAN 5740 Ralston Street, Suite 300 Ventura, California 93003 Tel: 805-654-0200 Fax: 805-654-0280

Case 2:13-cr-00082-KJM Document 23 Filed 12/13/13 Page 29 of 31

such as the defendant's age and education; the length of the detention; whether the defendant was offered food; the accused's physical and mental characteristics; the accused's experience with the criminal justice system; the location of the interrogation; the conduct of the police officers; and the type and length of questioning. *See, e.g., Taylor v. Maddox*, 366 F.3d 992, 1013-14 (9th Cir. 2004); *Lucero v. Kerby*, 133 F.3d 1299, 1311 (10th Cir. 1998); *see also* 18 U.S.C. § 3501 ("The presence or absence of any of the above-mentioned factors to be taken into consideration by the judge need not be conclusive on the issue of voluntariness").

Here, Mr. Keys' interrogation started shortly before 6:00 a.m., October 4, 2012. Earlier that morning, Mr. Keys took 100 mg of Trazodone—double his prescribed dosage—in order to induce sleep. Within a few hours of taking the Trazodone and falling asleep, he was suddenly awoken when government agents entered his bedroom in his New Jersey apartment stating that they needed to ask him some questions. The agents started to question Mr. Keys almost immediately upon waking him up from his sleep. Two agents separated him while the rest searched the house and spoke to Mr. Keys' roommates. During this time, Mr. Keys was still under the influence of a full dose of Trazodone. (Cogen Decl. at ¶ 8.) As a result, Mr. Keys' mental state was clouded.

Because of this compromised mental state, Mr. Keys' *Miranda* waiver was involuntary and his statements are otherwise inherently unreliable. (*See* Cogen Decl. at ¶¶ 9-10.) Therefore, this Court should suppress his written confession and any inculpatory statements he made during the interrogation.

B. MR. KEYS DID NOT KNOWINGLY AND INTELLIGENTLY WAIVE HIS *MIRANDA* RIGHTS.

In addition to voluntariness, a defendant's *Miranda* waiver must also be knowing and intelligent. *See Derrick v. Peterson*, 924 F.3d at 820; *see also Gladden*, 396 F.2d at 376. The waiver must be made "with a full awareness both of the nature of the right to be abandoned and consequences of the decision to abandon it." *Moran v. Burbine*, 475 U.S. 412, 421 (1986). Reviewing courts must look to the "totality of the circumstances surrounding the interrogation" to answer these inquiries. *Id.*; *see also Tague v. Louisiana*, 444 U.S. 469, 471 (1980) (per curiam) (government failed to show that petitioner had waived his *Miranda* rights because the arresting officer could not remember the statements that he read to the petitioner from a notice of *Miranda* rights, whether he asked the petitioner if he understood

> LAW OFFICES OF JAY LEIDERMAN 5740 Ralston Street, Suite 300 Ventura, California 93003 Tel: 805-654-0200 Fax: 805-654-0280

MOTION TO SUPPRESS Page 23

the rights, or whether he conducted any tests to determine if the petitioner was literate or otherwise capable of understanding his rights).

Factors commonly considered by courts in determining whether a valid *Miranda* waiver occurred includes a suspect's intelligence, age, and physical and mental condition, and the explicitness of the suspect's *Miranda* waiver. *See United States v. Montoya-Arrubla*, 749 F.2d 700 (11th Cir. 1985) (intoxication considered as possible evidence of an invalid waiver); *Sample v. Eyman*, 469 F.2d 819, 821 (9th Cir. 1972) (man's severe emotional distress following his wife's death precluded a finding of a knowing and intelligent waiver of *Miranda* rights). An otherwise voluntary confession may be inadmissible if the accused lacks the mental capacity to make a knowing and intelligent waiver. *See United States v. Frank*, 956 F.2d 872, 876 (9th Cir. 1991) (citing *Moran*, 475 U.S. at 421); *see also United States v. Garibay*, 143 F.3d 534, 537-38 (9th Cir. 1998) (defendant with limited English skills and low mental capacity did not validly waive his *Miranda* rights). Like voluntariness, whether a suspect knowingly and intelligently waives his *Miranda* rights is viewed in light of the totality of the circumstances surrounding the interrogation. *See Colorado v. Spring*, 479 U.S. at 573 (internal citations and quotations omitted).

Here, Mr. Keys was suddenly woken from a deep sleep by government agents after he consumed Trazodone, a powerful sleep-inducing drug. The agents told Mr. Keys they had a search warrant, and he was questioned by FBI agents Cauthen and Andrews. (*See* Transcript of FBI Interview, attached hereto as Def.'s Ex. E.) According to the transcript, Cauthen hastily read Mr. Keys his *Miranda* rights and began questioning him. (*Id.* at 1-2.) While the three were getting situated, Cauthen informed Mr. Keys he was not going to be arrested today, but Cauthen was going to read him his rights. (*Id.*) After Cauthen finished, Mr. Keys interrupted the interrogation by saying, "Before we all start" (*Id.* at 2.) Cauthen acknowledged to Mr. Keys that he appeared uneasy, and that he would answer all of his questions. (*Id.*) But Mr. Keys was never allowed to finish his thought. Neither Cauthen nor Andrews asked Mr. Keys if he understood his rights. Instead, Cauthen interrupted Mr. Keys while he attempted to speak immediately after he was mirandized.

Mr. Keys was woken up out of a bed early in the morning, by multiple FBI agents mere hours after taking a powerful sleeping pill. The FBI agents simultaneously read Mr. Keys his *Miranda* rights

> LAW OFFICES OF JAY LEIDERMAN 5740 Ralston Street, Suite 300 Ventura, California 93003 Tel: 805-654-0200 Fax: 805-654-0280

MOTION TO SUPPRESS Page 24

while showing him a voluminous search warrant issued for his home. (*See* Def.'s Ex. E.) When he interrupted the interrogation, he was cut off by Cauthen; the conversation continued on to introductions and questioning. *Id.* In light of the totality of the circumstances surrounding Mr. Keys' interrogation, it is clear that he did not understand the nature of the rights abandoned or the consequences of abandoning them. Thus, Mr. Keys did not knowingly and intelligently waive his *Miranda* rights.

For the reasons argued above, any *Miranda* waiver by Mr. Keys during the October 4, 2012 interrogation was not voluntary, knowing, and intelligent. Therefore, this court should suppress the written and oral statements subsequently obtained.

CONCLUSION

For the reasons argued above, this court should suppress all electronic evidence seized and statements obtained as a result of the October 3, 2012 search warrant and execution thereof. Dated: December 13, 2013

By: <u>/s/ Jay Leiderman</u> Jason S. Leiderman Eric J. Lindgren LAW OFFICES OF JAY LEIDERMAN By: <u>/s/ Tor Ekeland</u> Tor Ekeland TOR EKELAND, P.C. Attorneys for Defendant MATTHEW KEYS LAW OFFICES OF JAY LEIDERMAN S740 Ralston Street, Suite 300 Ventura, California 93003 Tel: 805-654-0200

Fax: 805-654-0280