

1  
2  
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

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT COURT OF CALIFORNIA

UNITED STATES OF AMERICA,

Plaintiff,

Cr. No. S-13-0082 KJM

vs.

MATTHEW KEYS,

Defendant.

ORDER

---

On January 29, 2014, the court heard argument on defendant's motion to suppress his statements to the authorities and evidence seized under the authority of a search warrant. Jason Leiderman and Tor Ekeland appeared for defendant Keys; Assistant United States Attorneys James Silver and Matthew Segal appeared for the United States. As explained below, the motion is DENIED.

I. PROCEDURAL BACKGROUND

Defendant is charged with conspiring to cause damage to a protected computer in violation of 18 U.S.C. § 371; transmission of malicious codes, 18 U.S.C. § 1030(a)(5)(A); attempted transmission of malicious code, 18 U.S.C. §§ 1030(a)(5)(A) and 1030(b); and forfeiture, 18 U.S.C. § 982(a)(2)(A). ECF No. 1.

1 On December 13, 2013, defendant filed a motion to suppress all property and  
2 information seized during the October 4, 2012 execution of a search warrant at his New Jersey  
3 residence and any fruits of the search; his oral written statement dated October 4, 2012; the  
4 audio recording and any transcript of his statement to investigators on October 4, 2012; and the  
5 perceptions, recollections and observations of the officers related to the taped statement. ECF  
6 No. 23 at 2.

7 II. THE WARRANT AND ITS EXECUTION

8 On October 3, 2012, Michael A. Hammer, United States Magistrate Judge for  
9 the District of New Jersey, issued a warrant for the search and seizure of “[e]vidence  
10 contraband, fruits, and instrumentalities of criminal violations of federal law, including Title  
11 18, United States Code, Sections 371 (conspiracy), 1030(a)(5) (transmitting malicious code)  
12 and 1030(a)(6) (trafficking in passwords).” ECF No. 23-1 at 5. The warrant listed the  
13 following items to be seized:

- 14 a. Records relating to unauthorized computer access and/or  
15 computer intrusions including attacks on the Tribune Media Co.  
16 server located in Los Angeles California [sic] for the period  
December 1, 2012 to the present;
- 17 b. Records relating to the trafficking in usernames and  
passwords;
- 18 c. Records relating to:
- 19 i. [foxmulder4099@yahoo.co.uk](mailto:foxmulder4099@yahoo.co.uk)  
20 ii. [cybertroll69x@hotmail.com](mailto:cybertroll69x@hotmail.com)  
21 iii. [walterskinner5099@Yahoo.co.uk](mailto:walterskinner5099@Yahoo.co.uk)  
22 iv. [cancerman4099@yahoo.co.uk](mailto:cancerman4099@yahoo.co.uk)  
23 v. [fox40truthers@gmail.com](mailto:fox40truthers@gmail.com)  
24 vi. [dudenudeguy@gmail.com](mailto:dudenudeguy@gmail.com)  
25 vii. The X-Files  
26 viii. AESCracked  
27 ix. Sabu  
28 x. Kayla

- 1 xi. Sharpie
- 2 xii. Switch
- 3 xiii. Blergh
- 4 xiv. N3ot0xin
- 5 xv. Chronom
- 6 xvi. Rand0m
- 7 xvii. Pellsson
- 8 xviii. Tred
- 9 xix. Garrett
- 10 xx. Tflow
- 11 xxi. Arseface

12 ECF No. 23-1 at 5-6. The warrant continued:

13 In order to search for the items described above that may be  
14 maintained in electronic media, law enforcement personnel are  
15 authorized to search, copy, image and seize the following items  
for offsite review:

16 a. Any computer equipment or digital devices belonging  
17 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 . . . ;

18 b. Any computer equipment or digital devices belonging  
19 to MATTHEW KEYS used to facilitate the transmission,  
20 creation, display, encoding, or storage of data, including word  
21 processing equipment, modems, docking stations, monitors,  
22 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 . . . ;

23 c. Any magnetic, electronic, or optical storage device  
24 capable of storing data, such as floppy disks, hard disks, tapes,  
25 CD-ROMs, CD-Rs, CD-RWs, DVDs, optical disks, printer or  
26 memory buffers, smart cards, PC cards, memory calculators,  
27 electronic dialers, electronic notebooks, personal digital  
assistants, and cell phones belonging to KEYS that are capable of  
being used to commit or further the crimes outlined above, or to  
create, access, or store evidence or instrumentalities of such  
crimes . . . ;

1 d. Any documentation, operating logs, and reference  
2 manuals regarding the operation of the computer equipment,  
storage devices or software belonging to MATTHEW KEYS;

3 e. Any applications, utility programs, compilers,  
4 interpreters, and other software belonging to MATTHEW KEYS  
5 used to facilitate direct or indirect communication with the  
computer hardware, storage devices, or data belonging to KEYS  
to be searched;

6 f. Any physical keys, encryption devices, dongles, or  
7 similar physical items belonging to MATTHEW KEYS which  
are necessary to gain access to KEYS's computer equipment,  
storage devices, or data;

8 g. Any passwords, password files, test keys, encryption  
9 codes, or other information belonging to MATTHEW KEYS  
10 necessary to access the computer equipment, storage devices, or  
data; and

11 h. All records, documents, programs, applications, or  
12 materials created, modified, or stored in any form, including in  
13 digital form, on any computer, or digital device belonging to  
MATTHEW KEYS, that show the actual user(s) of the computers  
14 or digital devices during any time period in which the device was  
used to commit the crimes referenced above, including the web  
15 browser's history, temporary Internet files, cookies, bookmarked,  
or favorite web pages; email addresses used from the computer;  
16 MAC IDs and/or Internet Protocol addresses used by the  
computer; email, instant messages, and other electronic  
17 communications; address books, contact lists; records of social  
networking and online service usage; and software that would  
18 allow others to control the digital devices such as viruses, Trojan  
horses, and other forms of malicious software (or alternately, the  
lack of software that would allow others to control the digital  
device).

19 i. All records, documents, programs, applications, or  
20 materials created, modified, or stored in any form, including in  
digital form, on any computer or digital device belonging to  
21 MATTHEW KEYS, that show evidence of counter-forensic  
programs (and associated data) that are designed to eliminate data  
22 from the computer or digital device.

23 k. All records, documents, programs, applications or  
24 materials created, modified, or stored in any form, including in  
digital form, on any computer or digital device belonging to  
25 MATTHEW KEYS, that show contextual information necessary  
to understand the evidence, contraband, fruits, or  
instrumentalities . . . .

26 ECF No. 23-1 at 7-8.

27 Agent Gabriel Andrews executed the affidavit in support of the warrant,  
28 describing a series of events beginning in 2010. Keys had been "Web Producer" for

1 Sacramento television station KTXL Fox 40, responsible for maintaining the station's Twitter  
2 and Facebook accounts. *Id.* at 15-16. After Keys lost that job in October 2010, the passwords  
3 for those accounts were changed by someone other than an authorized Fox 40 employee.  
4 Before Fox 40 regained control of the accounts, 6,000 followers were deleted from the Twitter  
5 account and the account was used to post news headlines from the station's competitors. *Id.* at  
6 16.

7 In December 2010, the station's producer began to receive emails from a person  
8 who claimed to have the station's email list. *Id.* at 15, 16. The emails, which generally  
9 disparaged Fox 40, began to arrive from [foxmulder4099@yahoo.co.uk](mailto:foxmulder4099@yahoo.co.uk) and included some  
10 information supporting the writer's claim to have obtained email addresses of Fox 40  
11 customers. *Id.* at 16. Other odd messages arrived from [cybertroll69x@hotmail.com](mailto:cybertroll69x@hotmail.com),  
12 [CancerMan4099@yahoo.co.uk](mailto:CancerMan4099@yahoo.co.uk), and from [WalterSkinner5099@yahoo.co.uk](mailto:WalterSkinner5099@yahoo.co.uk), with some  
13 suggestion the sender was Keys. *Id.* at 16-17. "Fox Mulder," "Walter Skinner," and "Cancer  
14 Man" are characters from the Fox television show the X-Files. *Id.* Through subpoenas for  
15 these accounts, the FBI learned that they were used by proxy servers or that information about  
16 them was unavailable. *Id.* at 18.

17 Around this time, a Fox 40 customer complained about receiving an unsolicited  
18 email from the email address of [fox40truthers@gmail.com](mailto:fox40truthers@gmail.com). *Id.* at 17.

19 On December 12, 2010, the producer received an email from  
20 [Matthew@sactownmedia.com](mailto:Matthew@sactownmedia.com) in which the writer, allegedly Keys, told the producer he had  
21 infiltrated Anonymous, an online collective of computer hackers, *see United States v. Collins*,  
22 No. 11-CR-00471-DLJ (PSG), 2013 WL 1089908, at \*1 (N.D. Cal. Mar. 15, 2013), and had  
23 access to future Anonymous operations against PayPal, Amazon, the Los Angeles Times, Fox  
24 News and others. *Id.* at 18. During a telephone conversation, Keys told the producer he had  
25 been invited into a private chat room populated with skilled hackers and told the hackers about  
26 his journalism experience. *Id.* at 19. Keys said he had computer records of his interactions  
27 with the Anonymous group members. *Id.* He denied involvement with the earlier suspicious  
28 emails.

1           On December 14, 2010, a server belonging to Tribune Media, the parent  
2 company of *The Los Angeles Times*, was compromised and at least one headline was altered.  
3 *Id.* at 19. The person who committed the computer intrusion used Tribune Media accounts  
4 identified by the names Anon1234 and Arseface. *Id.*

5           On March 18, 2011, Keys wrote on the website [producermatthew.com](http://producermatthew.com) about a  
6 Gawker story outing several members of Anonymous and crediting Keys with providing “just  
7 one of dozens of logs” that he had taken during his two-month access to the Anonymous chat  
8 room. *Id.* at 20. In June 2011, Keys wrote about a hacker who used the name Sabu, whom he  
9 had encountered during his involvement with the hacker chat room known as “internetfed,” run  
10 on the server Anonymous had used to carry out its denial of service attacks in December 2010  
11 and January 2011. *Id.*

12           In December 2011, the FBI in Sacramento obtained chat room information in  
13 which someone called “Kayla” said Keys was “AESCracked” who gave them passwords for  
14 *The Los Angeles Times*, Fox 40 and other entities as well. *Id.* at 21. Also in December, search  
15 warrant affiant Andrews reviewed chat logs from “internetfed” from December 2010 to January  
16 2011; among the exchanges was AESCracked identifying himself as a former Fox employee,  
17 providing the user name “anon1234,” which had been used to gain access to the Tribune Media  
18 server, and exhorting readers to “go fuck some shit up!” *Id.* at 21-22. AESCracked also asked  
19 if anyone wanted to buy an e-mail list. *Id.* at 22. In these logs, AESCracked communicated  
20 with Sabu, Kayla, Sharpie, Switch, Blergh, N3ot0xin, Chronom, Rand0m, Pellsson, Tred,  
21 Garrett and others. *Id.* at 22, 24-25. He accessed the chat channel from IP address  
22 78.129.220.46, which was also used by the sender of an email from  
23 [foxmulder4099@yahoo.co.uk](mailto:foxmulder4099@yahoo.co.uk).

24           These logs also showed AESCracked was barred from the AnonOps chat server  
25 after users accused him of leaking information to the media and that Kayla and another user  
26 claimed AESCracked was logging in under A2sCracked from IP address 75.53.171.204;  
27 Andrews learned this IP address was registered to Keys. *Id.* at 23.  
28

1           In March 6, 2012 Keys posted a screenshot of an IRC chat and identified it as  
2 part of a log recorded on December 22, 2010. Agent Andrews identified the program as  
3 Colloquy, a chat program available for Macintosh computers, explained that Colloquy shows  
4 the person's username in red, and that in the image Keys posted the username in red is  
5 intentionally blurred, but appears to be ten characters long with "d" as the last letter. Another  
6 participant in the chat room refers to the user as "AES." *Id.* at 20-21.

7           In May 2012, Keys' Twitter post linked to the book *We Are Anonymous* with a  
8 message "This is the book I'm in." *Id.* at 24. In the book, author Parmy Olson relied on Keys'  
9 screenshots of the #Internet Feds chat room and said Keys has used the name AESCracked  
10 while observing the exchanges in the chat room during December 2010 and January 2011. *Id.*  
11 at 24.

12           Agent Andrews avers there is probable cause to believe Keys still had the  
13 information relating to the intrusion into the Tribune Media server at the time of the search  
14 warrant request, even though Keys had moved from Sacramento to Secaucus, New Jersey. The  
15 agent explained it appeared Keys still had the chat logs in March 2012, post-dating his move,  
16 and he maintains the website producermatthew.com from his home. Andrews also attests that,  
17 based on his experience, he knows people proficient with computers generally retain them and  
18 attendant digital media when moving from one place to another and that data will remain on a  
19 computer, even if deleted, until overwritten. *Id.* at 26-27. Andrews further opined that Keys  
20 retained evidence of his interactions with Anonymous because he regards them as an  
21 accomplishment, as suggested by the fact that he maintains stories about Anonymous from  
22 December 2010 on his website. *Id.*

23           In his affidavit, Andrews described what he perceived to be the difficulties of  
24 searching computer systems: because of the multiplicity of hardware and software, it is  
25 impossible to bring to the site all the specialized equipment necessary for a thorough search;  
26 because of the danger that data might be modified or deleted unintentionally, it is better to  
27 conduct the search in a controlled environment; because of the potential for a large volume of  
28 data to be stored in computer systems, it is impracticable to complete the search during the

1 execution of the warrant; because users can disguise files in a variety of ways, it is a time-  
2 consuming process to extract and sort through hidden or encrypted data. *Id.* at 27-28.

3 III. THE MOTION TO SUPPRESS THE PHYSICAL EVIDENCE

4 A. Background

5 Defendant argues that by permitting the seizure of every type of electronic  
6 media, the warrant was overbroad, the modern equivalent of a general warrant. Specifically he  
7 argues Ninth Circuit authority imposes several rules on such a search: (1) the warrant for a  
8 computer search must contain a factual justification for a broad search and seizure of the  
9 computer; (2) the search must be monitored by a neutral, detached magistrate judge; (3) the  
10 government must seal and hold the documents pending judicial approval of a further search; (4)  
11 large scale removal is appropriate only when on-site searching is not feasible; and (5) the  
12 government must return documents outside the scope of the search. ECF No. 23 at 18 (citing  
13 *United States v. Tamura*, 694 F.2d 591 (9th Cir. 1982)). Defendant also suggests the  
14 government should have followed the guidelines for computer searches outlined in Chief Judge  
15 Kozinski's concurrence in *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162  
16 (9th Cir. 2010) (*CDT III*) (per curiam) (en banc). *Id.* at 20-21.

17 Defendant also contends the information on which Agent Andrews relied was  
18 stale because nothing in the supporting affidavit shows there was on-going criminal activity  
19 between the alleged crime, in December 2010, and the search in October 2012. *Id.* at 22-24.

20 Finally, defendant argues the affidavit contains deliberate or reckless  
21 misrepresentations, requiring an evidentiary hearing. *Id.* at 24-27.

22 The government contends the warrant was sufficiently particular and no Ninth  
23 Circuit authority requires the government to follow certain rules in every case. ECF No. 24 at  
24 16-19 (citing, *e.g.*, *United States v. Schesso*, 730 F.3d 1040 (9th Cir. 2013)). It also counters  
25 the information was not stale, as the affidavit showed Keys was proud of his interaction with  
26 Anonymous and thus was likely to have kept records of it. *Id.* at 19-21. The government relies  
27 on the good faith exception to the exclusionary rule to argue the evidence seized should not be  
28



1 suppressed. *Id.* at 21-22. Finally, it argues that no hearing is required because there were no  
2 material omissions in the affidavit.

3 In reply defendant takes issue with the government's attack on his citation to  
4 Judge Kozinski's *CDT III* concurrence, arguing that he referenced these guidelines only in  
5 anticipation of the government's good faith argument, not as a primary basis for suppression.  
6 Under binding Ninth Circuit authority, he argues, the search was overbroad. He then turns to  
7 his staleness attack, noting the warrant contained no information that he was still involved in  
8 criminal activity, as even the freshest evidence the government describes was not indicative of  
9 criminal activity at all. He revisits Judge Kozinski's concurrence to argue the warrant cannot  
10 be saved by the good faith exception. ECF No. 26.

#### 11 B. Fourth Amendment

12 The warrant clause of the Fourth Amendment requires "probable cause,  
13 supported by Oath or affirmation" to justify the issuance of a search warrant. U.S. CONST.  
14 AMEND. IV. In addition, the warrant must "particularly describ[e] the place to be searched, and  
15 the persons or things to be seized." U.S. CONST. AMEND. IV. By limiting the authorization to  
16 search to the specific areas and things for which there is probable cause to search, the  
17 requirement ensures that the search will be carefully tailored to its justifications, and will not  
18 take on the character of the wide-ranging exploratory searches . . . ." *Maryland v. Garrison*,  
19 480 U.S. 79, 84 (1987); *see also Andresen v. Maryland*, 427 U.S. 463, 479 (1976) ("This  
20 requirement makes general searches . . . impossible and prevents the seizure of one thing under  
21 a warrant describing another. As to what is to be taken, nothing is left to the discretion of the  
22 officer executing the warrant." (internal citation and quotation marks omitted)).

23 When the results of a warrant-based search are challenged in a motion to  
24 suppress, the defendant bears the burden of demonstrating that the search is unreasonable under  
25 the Fourth Amendment. *See United States v. Ankeny*, 502 F.3d 829, 836 (9th Cir. 2007).

#### 26 C. Computer Searches, General Searches

27 "General warrants . . . are prohibited by the Fourth Amendment. '(T)he  
28 problem (posed by the general warrant) is not that of the intrusion Per [sic] se, but of a general,

1 exploratory rummaging in a person's belongings . . . . (The Fourth Amendment addresses the  
2 problem) by requiring a 'particular description' of the things to be seized.'" *Andresen*, 427  
3 U.S. at 480 (quoting *Coolidge v. New Hampshire*, 403 US. 443, 467 (1971)).

4 The Fourth Amendment's specificity requirement "has two aspects:  
5 particularity and breadth. Particularity is the requirement that the warrant must clearly state  
6 what is sought. Breadth deals with the requirement that the scope of the warrant be limited by  
7 the probable cause on which the warrant is based." *United States v. Towne*, 997 F.2d 537, 544  
8 (9th Cir. 1993) (internal quotation and citation omitted); *see also United States v. SDI Future*  
9 *Health, Inc.*, 568 F.3d 684, 702-03 (9th Cir. 2009) (distinguishing between the "two distinct  
10 parts" of the evaluation of a warrant: particularity and overbreadth).<sup>1</sup>

11 Despite the particularity requirement, "[w]arrants which describe generic  
12 categories of items are not necessarily invalid if a more precise description of the items subject  
13 to seizure is not possible." *United States v. Shi*, 525 F.3d 709, 731 (9th Cir. 2008) (quoting  
14 *United States v. Adjani*, 452 F.3d 1140, 1147-48 (9th Cir. 2006)). Several factors guide the  
15 determination whether the warrant is sufficiently particular: "(1) whether probable cause exists  
16 to seize all items of a particular type described in the warrant; (2) whether the warrant sets out  
17 objective standards by which executing officers can differentiate items subject to seizure from  
18 those which are not; and (3) whether the government was able to describe the items more  
19 particularly in light of the information available to it at the time the warrant was issued."  
20 *United States v. Spilotro*, 800 F.2d 959, 963 (9th Cir. 1986).

---

21  
22  
23 <sup>1</sup> Although defendant characterizes the search as overbroad, ECF No. 26 at 3, he relies on  
24 cases discussing the specificity requirement. For example, the case law characterizes *United*  
25 *States v. Tamura* as a particularity, rather than an overbreadth, case, though it does also suggest  
26 the agents' refusal to return the documents not named in the warrant was "an unreasonable and  
27 therefore unconstitutional manner of executing the warrant." 694 F.2d 591, 597 (9th Cir.  
28 1982); *see United States v. Nazemzadeh*, No. 11-cr-5726-L, 2013 WL 544054, at \*3-4 (S.D.  
Cal. Feb. 12, 2013) (characterizing *Tamura* as a particularity case and upholding a warrant  
authorizing seizure and removal of all computer storage media as part of the seizure of  
defendant's email account to search for evidence of the conspiracy to export embargoed  
goods).

1           “Searches of electronic records pose unique challenges for ‘striking the right  
2 balance between the government’s interest in law enforcement and the right of individuals to be  
3 free from unreasonable searches and seizures.’” *United States v. Schesso*, 730 F.3d 1040, 1042  
4 (9th Cir. 2013) (quoting *CDT III*, 621 F.3d at 1177). Defendant contends the instant warrant  
5 did not strike the right balance, as illustrated by several cases.

6           As defendant notes, the en banc decision of *CDT III* relied heavily on a case  
7 decided before the advent of electronic media, a case from which he himself derives the rules  
8 he claims must be followed. At issue in *United States v. Tamura* was the government’s seizure  
9 of “large quantities of documents that were not described in the search warrant” during their  
10 search for three categories of documents. 694 F.2d at 594-95. In *Tamura*, when agents  
11 realized that finding the three categories of documents they were permitted to seize would take  
12 too long, they seized all the company’s accounting records for the relevant years and removed  
13 them to another location where they extracted the documents they sought. *Id.* at 595. The  
14 Ninth Circuit acknowledged “all items in a set of files may be inspected during a search,  
15 provided that sufficiently specific guidelines for identifying the documents sought are provided  
16 in the search warrant . . .” but condemned the “wholesale *seizure* for later detailed examination  
17 of records not described in the warrant . . .” *Id.* (emphasis in original). It continued that in the  
18 rare case when documents are so intermingled they cannot be sorted on site, the agents could  
19 seal them pending a magistrate judge’s approval of a further search. *Id.* at 596. Because the  
20 magistrate judge had not authorized the wholesale removal before it occurred, the search was  
21 unreasonable. *Id.* The court recognized, however, that when officers knew beforehand they  
22 would have to transport documents, they could seek authorization from the magistrate judge by  
23 showing “on-site sorting is infeasible and no other practical alternative exists.” *Id.* Ultimately,  
24 the court found that “[r]egardless of the illegality of the Government’s seizure and retention of  
25 documents not covered in the warrant, . . . reversal is not compelled . . . . All of the documents  
26 introduced at trial were seized and retained lawfully because described in and therefore taken  
27 pursuant to the valid search warrant.” *Id.* at 597.

1 Defendant also cites to *United States v. Hill*, to argue that even with the  
2 problems inherent in computer searches, the government cannot expect an “automatic blank  
3 check” for such seizures, but rather must “demonstrate to the magistrate *factually* why such a  
4 broad search and seizure authority is reasonable in the case at hand.” 459 F.3d 966, 975 (9th  
5 Cir. 2006) (emphasis in original). *Hill*, defendant argues, means the government must make  
6 “some threshold showing” before it can “seize the haystack to look for the needle.” *Id.*  
7 However, as in *Tamura*, the Ninth Circuit upheld the search, which authorized the seizure and  
8 removal of all computer and storage media.

9 Finally, defendant turns to *CDT III* and its caution that “[t]he point of the  
10 *Tamura* procedures is to maintain the privacy of materials that are intermingled with seizable  
11 materials, and to avoid turning a limited search for particular information into a general search  
12 of office file systems and computer databases.” 621 F.3d at 1170. In *CDT III*, the government  
13 sought information about ten baseball players it suspected had used steroids, from third parties  
14 not suspected of any involvement in the alleged crimes. As the result of executing warrants in  
15 the Central District of California and the District of Nevada and issuing a grand jury subpoena  
16 in the Northern District, the government seized a computer database containing drug testing  
17 information about hundreds of athletes despite CDT’s offer to provide all the information in its  
18 possession about the ten named baseball players. *Id.* at 1166-67. Three district courts ordered  
19 the return of the property seized and quashed subpoenas, troubled by the breadth of the  
20 information seized. The government timely appealed in two of the actions and the Ninth  
21 Circuit affirmed. It noted the government had failed to follow the *Tamura* procedures the  
22 Central District’s magistrate judge had built into the warrant to protect intermingled data, and  
23 as information obtained during the execution of the Central District warrants made execution of  
24 the Nevada warrant feasible, it upheld the Nevada district court’s condemnation of the agents’  
25 refusal to segregate and return the data on the players not suspected of steroid use. *Id.* at 1170.

26 The government, in contrast, relies on a number of cases that have upheld broad  
27 seizures of computers and electronic media. For example in *United States v. Giberson*, agents  
28 executing a warrant for evidence relating to the defendant’s manufacture of false identification

1 found materials for making IDs near a personal computer. They obtained a second warrant to  
2 search a mirror image of the computer's hard drive and ultimately found child pornography.  
3 The Ninth Circuit rejected the defendant's challenge to the warrant, finding it described the  
4 items to be seized as particularly as it could, given the evidence the government possessed, and  
5 observing that it had "long held that a search warrant authorizing the seizure of materials also  
6 authorizes the search of objects that could contain those materials." 527 F.3d 882, 886 (9th Cir.  
7 2008); *see also United States v. Gomez-Soto*, 723 F.2d 649, 655 (9th Cir. 1984) (upholding  
8 agents' seizure of a microcassette tape when warrant authorized search for documents: "[t]he  
9 failure of the warrant to anticipate the precise container in which the material sought might be  
10 found is not fatal").

11           In *United States v. Hay*, the Ninth Circuit upheld a warrant authorizing the  
12 seizure of the defendant's "computer hardware, software, records, instructions or  
13 documentations" and the agents' subsequent seizure of a computer, seven zip drives labeled  
14 "Linux Backup," software, computer disks, and videotapes. 231 F.3d 630, 633 (9th Cir. 2000).  
15 The court rejected the defendant's challenge to the lack of particularity of the warrant because  
16 "no more specific description of the computer equipment sought was possible," in light of the  
17 fact that the government knew nineteen images of child pornography had been sent to  
18 defendant's computer, but "had no way of knowing where the images were stored." *Id.* at 637  
19 (internal citation and quotation marks omitted). The court also rejected defendant's argument  
20 that suppression was required by *Tamura* because the warrant had specifically authorized the  
21 wholesale seizure, justified by the description in the affidavit of the difficulties in undertaking  
22 an on-site analysis. *Id.*; *see also United States v. Needham*, 718 F.3d 1190, 1193, 1196 (9th Cir.  
23 2013) (rejecting claim that warrant authorizing search of all paper documents and electronic  
24 and digital storage devices for child pornography was a general search because it specified  
25 what officers sought and where they believed they would find it); *United States v. Lacy*, 119  
26 F.3d 742, 746-47 (9th Cir. 1997) (upholding a warrant authorizing search of defendant's entire  
27 computer system based on information defendant had downloaded six images of child  
28 pornography).

1 In *Adjani, supra*, the magistrate judge issued a warrant for the seizure of  
2 Adjani's computer equipment based on allegations he had used email to communicate about  
3 extortionate demands. While executing the warrant, the agents found and seized a second  
4 computer belonging to a person named Reinhold, who had not been identified as a suspect;  
5 agents later located communications on that computer showing Reinhold's involvement in the  
6 plot. The Ninth Circuit upheld the district court's denial of Adjani's and Reinhold's motion to  
7 suppress, saying that the warrant authorizing the seizure of the computer, hard drives, computer  
8 disks and other storage media to permit a search for communications to the victims of the  
9 extortion and evidence of travel was sufficiently particular. 452 F.3d at 1148. The court  
10 recognized the warrant might have provided for a more restrictive search of the email inbox  
11 and outbox for the addresses connected to the plot, but said "[t]o require such a pinpointed  
12 computer search, to an email program or to specific search terms, would likely have failed to  
13 cast a sufficiently wide net to capture the evidence sought." *Id.* at 1149-50.

14 Finally, in *United States v. Schesso, supra*, the court "consider[ed] the  
15 implications of *CDT III*' for the defendant, who was found in possession of numerous images  
16 of child pornography. The district court suppressed the evidence seized under the authority of a  
17 warrant that permitted agents to remove "multiple pieces of electronic media and data storage  
18 devices," but the Ninth Circuit reversed, noting "[t]he government was faced with the challenge  
19 of searching for digital data that was not limited to a specific, known file or set of files. The  
20 government had no way of knowing which or how many illicit files there might be or where  
21 they might be stored, or of describing the items to be seized in a more precise manner." 730  
22 F.3d at 1046. This consideration, coupled with the explanation of the need for off-site analysis  
23 was sufficient to allow the search to stand.

24 Defendant argues that *Schesso*, a panel decision, cannot override the en banc  
25 *CDT III* decision; *Schesso*'s suggestion that *CDT III* and its reliance on *Tamura* was animated  
26 by the particular privacy concerns of that case has little bearing on this court's decision. ECF  
27 No. 26 at 3. This court does, however, consider the context from which *CDT III* arose in  
28 determining its application to this case. While *CDT III* did endorse a variation of the *Tamura*

1 procedures, it did so in the context of motions to quash and for the return of property in a case  
2 brought not by a criminal defendant but by third parties. The court noted the differences  
3 between motions to suppress evidence and motions for the return of property: “Rule 41(g)  
4 [governing the return of property] is concerned with those whose property or privacy interests  
5 are impaired by the seizure,” and that “by forcing the government to return property that it had  
6 not properly seized, CDT was preserving the integrity of its business and the Players  
7 Association is protecting the privacy and economic well-being of its members . . . .” *Id.* at  
8 1172-73. The court did not speculate what uses, if any, the government “may make of the . . .  
9 evidence during a criminal proceeding” because this “must be decided in the context of such a  
10 proceeding, when and if criminal charges are brought against any of the players.” *Id.* at 1173.  
11 In addition to upholding the district court’s order granting the motion for return of property, the  
12 Ninth Circuit determined the court’s reliance on equitable considerations to find the  
13 sequestration and return of property was appropriate. *Id.* at 1174. Here, defendant has not  
14 cited cases suggesting equitable considerations apply to an evaluation of his motion to suppress  
15 the evidence seized. Moreover, although the court in *CDT III* recognized the dangers of over-  
16 seizing computer evidence, it did not discuss, much less overrule, its cases authorizing broad  
17 seizures of electronic media.

18 *CDT III* does not dictate suppression in this case. Here, unlike in *Tamura*, the  
19 warrant authorized the seizure of the electronic media for off-site examination based on the  
20 agent’s description of the difficulties of conducting an on-site review. Defendant complains  
21 that nothing in the affidavit suggests he was a sophisticated user, likely to have encrypted or  
22 booby-trapped any of the files agents sought. ECF No. 23 at 20.<sup>2</sup> However, the affidavit did  
23 describe the ways in which even a “run-of-the mill Mac user” could disguise files through the  
24 use of innocuous filenames or extensions.

25 Moreover, as there is no evidence the government could have known what  
26 computer equipment Keys possessed apart from his Mac or where he might store the

---

27 <sup>2</sup> Defendant also argues the removal of the equipment was not monitored by a neutral,  
28 detached magistrate judge, but a magistrate judge did sign the warrant authorizing the removal.

1 information about his exchanges with Anonymous, the government’s description of the things  
2 to be seized was sufficiently particular. Keys does not complain that the description of the files  
3 sought was too generic.

4 Finally, the affidavit described Keys’ computer as the means of committing the  
5 alleged crime: he joined the internetted chat room by using his computer and he kept logs of  
6 this interactions with Anonymous. Thus, authorizing the seizure of this equipment was  
7 justified.

#### 8 D. Staleness

9 As noted, the warrant clause of the Fourth Amendment requires “probable  
10 cause, supported by Oath or affirmation” to justify the issuance of a search warrant. U.S.  
11 CONST. AMEND. IV. Probable cause means that, based on all the circumstances in the affidavit,  
12 “there is a fair probability that contraband or evidence of a crime will be found in a particular  
13 place.” *Illinois v. Gates*, 462 U.S. 213, 238 (1983); *United States v. Tan Duc Nguyen*, 673 F.  
14 3d 1259, 1264 (9th Cir. 2012). The concept is a fluid one, the product of “a practical common-  
15 sense” inquiry rather than a set of mechanical rules. *Gates*, 462 U.S. at 238-39. “This court  
16 must give “great deference” to the magistrate judge’s determination of probable cause. *United*  
17 *States v. Krupa*, 658 F.3d 1174, 1177 (9th Cir. 2011).

18 Generally, “[a]n affidavit must be based on facts so closely related to the time of  
19 the issuance of the warrant as to justify a finding of probable cause at that time.” *Lacy*, 119  
20 F.3d at 745. However, “[i]nformation underlying a warrant is not stale ‘if there is a sufficient  
21 basis to believe, based on a continuing pattern or other good reasons, that the items to be seized  
22 are still on the premises.’” *Schesso*, 730 F.3d at 1047 (quoting *Lacy*, 119 F.3d at 756-46). In  
23 evaluating staleness, the court considers “the particular facts of the case and the nature of the  
24 criminal activity and property sought.” *Lacy*, 119 F.3d at 745; *see also United States v.*  
25 *Farmer*, 370 F.3d 435, 439 (4th Cir. 2004) (“[T]he vitality of probable cause cannot be  
26 quantified by simply counting the number of days between the occurrence of the facts supplied  
27 and the issuance of the affidavit.”) (internal citation & quotation marks omitted).



1 As defendant says, nothing in the affidavit suggests any ongoing criminal  
2 activity; he contends probable cause to believe he was involved in the intrusion into the *Times*'  
3 server does not equate to probable cause he still possessed any information about it. That there  
4 is no ongoing criminal activity does not mean the information supporting a warrant was stale,  
5 however, as long as "other good reasons" support the magistrate judge's conclusion Keys  
6 would still possess the evidence.

7 Defendant also argues the affidavit relies on the generalization that a person  
8 proficient with computers will retain storage media for a long time. But the magistrate judge  
9 could rely on his own common-sense determination that people hold onto the tools by which  
10 they make their living or pursue their passion or vocation. As the affidavit showed defendant  
11 used his computer to update his website and as part of his profession, it was logical to assume  
12 he would still possess a computer and the means of storing information relating to his  
13 profession. *See, e.g., United States v. Abboud*, 438 F.3d 554, 574 (6th Cir. 2006) (noting that  
14 "business records are a type of evidence that defy staleness"); *see also United States v. Seiver*,  
15 692 F.3d 774, 778 (7th Cir. 2012), *cert. denied*, \_\_\_ U.S. \_\_\_, 133 S.Ct. 915 (2013) ("Computers  
16 and computer equipment are 'not the type of evidence that rapidly dissipates or degrades.'")  
17 (quoting *United States v. Vosburgh*, 602 F.3d 512, 529 (3d Cir. 2010), *cert. denied* 131 S.Ct.  
18 1783 (2011)).

19 Defendant further argues the affidavit makes crude generalizations about  
20 journalists. However, the affidavit details defendant's periodic reference to his interactions  
21 with Anonymous, including his May 2012 reference to the book *We Are Anonymous*, which  
22 relied upon him as a source. From this information the magistrate judge could reasonably  
23 conclude defendant was indeed proud of his work and so would retain his source material.

24 Finally, defendant says there is no evidence he possessed any chat logs, despite  
25 the March 2012 posting of a screenshot of a chat. He is wrong: the affidavit recounted a  
26 conversation defendant had with the producer of Fox 40 in which defendant said "he had  
27 computer records of his interaction with the Anonymous group members." ECF No. 23-1 at  
28 18-19. The affidavit also said defendant referred to a Gawker story about Anonymous, and

1 said he “provided Gawker with just one of dozens of logs that were taken during my two-month  
2 access . . . .” *Id.* at 19-20. The fact that in March 2012 defendant posted a screen shot of a chat  
3 from December 2010, coupled with his admission he had recorded logs, was sufficient to  
4 establish the probability agents would find evidence relating to that series of chats on  
5 defendant’s electronic media in October 2012.

6 E. *Franks*

7 In *Franks v. Delaware*, the United States Supreme Court held:

8 where the defendant makes a substantial preliminary showing  
9 that a false statement knowingly and intentionally, or with  
10 reckless disregard for the truth, was included by the affiant in the  
11 warrant affidavit, and if 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.

12 438 U.S. 154, 155-56 (1978). The Court continued that “to mandate an evidentiary hearing, the  
13 challenger’s attack must be more than conclusory. . . . There must be allegations of deliberate  
14 falsehood or reckless disregard for the truth, and those allegations must be accompanied by an  
15 offer of proof.” *Id.* at 171. It cautioned that “allegations of negligence or innocent mistake are  
16 insufficient.” *Id.* “Deliberate or reckless omissions of facts that tend to mislead” may also  
17 trigger a *Franks* hearing. *United States v. Stanert*, 762 F.2d 775, 781 *as amended by* 769 F.2d  
18 1410 (9th Cir. 1985).

19 In the Ninth Circuit, a defendant is entitled to a *Franks* hearing if he makes  
20 specific allegations that identified portions of the affidavit necessary to a finding of probable  
21 cause are false or misleading, and a sufficient showing that the statements or omissions were  
22 deliberately false or made with a reckless disregard for the truth; the latter showing in turn  
23 requires an offer of proof challenging the veracity of the affiant, not that of his informant.  
24 *United States v. Kiser*, 716 F.2d 1268, 1271 (9th Cir. 1983). At the pleading stage, a defendant  
25 need not present clear proof of deliberate or reckless misrepresentations or omissions; it is  
26 sufficient if he makes a substantial showing that supports a finding of recklessness or intent.  
27 *United States v. Gonzalez, Inc.*, 412 F.3d 1102, 1111 (9th Cir. 2005), *amended on denial of*  
28 *reh’g by* 437 F.3d 854 (9th Cir. 2006).

1 Defendant argues the affidavit is marred by two material omissions. ECF No.  
2 25. First, Agent Andrews did not include information that Agent Cauthen, also involved with  
3 the case, did not believe defendant was involved with the suspicious emails Fox 40 received in  
4 December 2010, because it was illogical for defendant to have disclosed his identity. Second,  
5 Andrews selectively used the IP address information and so overstated its precision.  
6 Specifically, defendant says the IP address Andrews claims “resolved to a location in  
7 Sacramento” was administered by Comcast, although Keys used AT&T as an Internet Service  
8 Provider. In addition, defendant argues the IP address linking [foxmulder4099@yahoo.co.uk](mailto:foxmulder4099@yahoo.co.uk)  
9 and AESCracked is “presumably the IP address of a proxy server,” which serves as proxies for  
10 many people at a time. *Id.* at 25-26.

11 Even if Agent Cauthen’s opinion about defendant’s involvement in the  
12 suspicious emails and more complete information about the IP addresses had been included in  
13 the affidavit, the affidavit still would establish probable cause. The affidavit established that  
14 when defendant’s employment with Fox 40 ended, he reacted by changing passwords to the  
15 station’s Twitter and Facebook accounts; Keys told the producer he had become involved in an  
16 Anonymous chat room and recorded the interactions, a claim he also made on his website, and  
17 identified the chat room as internetfed; logs of the internetfed chat room seized by the FBI  
18 show a participant, identified as AESCracked, claiming to be a former Fox employee, asking if  
19 anyone wanted to go after Fox or *The Los Angeles Times*, providing passwords, and exhorting  
20 others to “go fuck some shit up!”; and a screenshot defendant posted of an exchange in the  
21 internetfed chat room suggested the person using the chat program was AESCracked. Even if  
22 information casting doubt about defendant’s involvement in the emails to Fox 40, the rest of the  
23 affidavit was sufficient to support the warrant’s issuance. Defendant’s request for a *Franks*  
24 hearing is denied.

#### 25 IV. THE MOTION TO SUPPRESS THE STATEMENTS

26 As the search did not violate the Fourth Amendment, defendant’s statements  
27 were not the fruit of any illegality in undertaking the search. The court turns to defendant’s  
28

1 claim that he did not voluntarily, knowingly and intelligently waive his rights under *Miranda v.*  
2 *Arizona*, 384 U.S. 436 (1966).

3 A. Waiver of *Miranda* Rights

4 Defendant argues his statements made to police during the execution of the  
5 search warrant should be suppressed because his *Miranda* waiver was not voluntary, knowing,  
6 and intelligent. He says at the time he waived his *Miranda* rights he was under the influence of  
7 a powerful sleep-inducing drug. ECF No. 23 at 22, 24.

8 Defendant states in his sworn declaration that at 1:30 a.m. on October 4, 2012,  
9 approximately six hours before he was interrogated by FBI agents, he took 100 milligrams of  
10 Trazodone, an antidepressant with sleep-inducing effects, in two 50 milligram doses. Keys  
11 Decl. ¶¶ 3, 4, 6, ECF No. 23-6. He attests he fell asleep around 2:30 a.m. and was in a deep  
12 sleep when the FBI executed the search warrant at his home at approximately 6 a.m. later that  
13 morning. *Id.* ¶ 7. After agents encouraged defendant to read the search warrant, they  
14 questioned defendant for two hours. *Id.* ¶ 8. Agents also encouraged defendant to make a  
15 written statement, a suggestion defendant resisted “citing concern over [his] state of mind.” *Id.*  
16 Throughout the questioning, defendant attests the Trazodone caused him to feel drowsy,  
17 confused, and forgetful. *Id.* ¶ 9. Because of the drug’s effects, defendant asserts his statements  
18 provided that day are “unreliable and not accurate about the events discussed therein.” *Id.*

19 To corroborate his statement on Trazodone and the validity of his *Miranda*  
20 waiver, defendant provides the declaration of Dr. Barry M. Cogen, a doctor of Osteopathy  
21 licensed to practice in California. Cogen Decl. ¶ 1, ECF No. 23-7. Cogen has practiced  
22 general medicine for 24 years, *id.*, and he regularly prescribes Trazodone in his practice and is  
23 “extremely familiar with its effects,” *id.* ¶ 4. Cogen attests that Trazodone “is a very sedating  
24 medication that “does not wear off quickly and will still cause drowsiness, sedation and other  
25 side effects after the person taking [it] is awoken.” *Id.* ¶ 6. Common side effects include  
26 “dizziness, drowsiness, fatigue, and nervousness” and may cause patients to become “drowsy  
27 or less alert and may affect judgment.” *Id.* ¶ 7. Trazodone has a half-life of six hours, meaning  
28 that after six hours, half of the drug remains active in the body. *Id.* ¶ 8. A full 50 milligram

1 dose—and defendant attests he took twice this dose—would still have been active in  
2 defendant’s body at the time he was interrogated. *See id.* Dr. Cogen’s opinion, based upon his  
3 knowledge of Trazodone and defendant’s physical characteristics, as well as upon his review of  
4 a tape of the interrogation, is that defendant’s statements are unreliable because he was  
5 “awoken during his [Trazodone] induced sleep.” *Id.* ¶ 9. Finally, Cogen notes if he were  
6 treating a patient under the influence of Trazodone in a hospital setting, he would not rely  
7 “solely” upon statements made by that patient but would also “seek verifiable, reliable data,  
8 like independent tests.” *Id.* ¶ 11.

9 In sum, defendant argues his waiver was involuntary because of his drug-  
10 influenced mental state. ECF No. 23 at 22. Nor was his waiver knowing and intelligent when  
11 his mental state did not permit him to “understand the nature of the rights abandoned or the  
12 consequences of abandoning them.” *Id.* at 25.

13 The government counters that simply being under the influence of medication  
14 does not equate to coercion. ECF No. 24 at 27. Numerous decisions in the Ninth Circuit and in  
15 this district have so held. *Id.* (citing, among other things, *United States v. Martin*, 781 F.2d  
16 671, 672–74 (9th Cir. 1993)). Moreover, Trazodone may have actually improved defendant’s  
17 mental function and rational faculties by helping maintain his “mental balance.” *Id.* (citing  
18 National Institute of Health (NIH) Report on Trazodone). Finally, the government asserts the  
19 transcript of the FBI’s conversation with defendant demonstrates defendant was “entirely  
20 capable of rational action throughout the interview.” *Id.* at 28.

21 In reply, defendant takes issue with the government’s assertion that Trazodone  
22 could have improved defendant’s brain functioning. ECF No. 26 at 9–10. The NIH report lists  
23 several side effects of the drug, such as weakness, tiredness, nervousness, and decreased ability  
24 to concentrate or remember things. *Id.* at 9. Keys also attempts to distinguish three cases upon  
25 which the government relies: *United States v. Martin*, 781 F.2d 671 (9th Cir. 1993), *United*  
26 *States v. Kelley*, 953 F.2d 562, 565–66 (9th Cir. 1992), and *United States v. Lewis*, 833 F.2d  
27 1380, 1384–86 (9th Cir. 1987).

28 ////

1           The parties do not dispute whether defendant’s statements were elicited through  
2 custodial interrogation. Nor is there a dispute that defendant was properly *Mirandized* before  
3 making the incriminating statements defendant seeks to suppress. Accordingly, the only  
4 question before the court is whether defendant’s decision to respond to the FBI’s questions  
5 after being informed of his *Miranda* rights was voluntary, knowing, and intelligent. *See United*  
6 *States v. Binder*, 769 F.2d 595, 599 (9th Cir. 1985), *overruled on other grounds by United*  
7 *States v. Morales*, 108 F.3d 1031, 1035 n.1 (9th Cir. 1997) (“For a confession obtained during  
8 custodial interrogation to be admissible, any waiver of *Miranda* rights must be voluntary,  
9 knowing, and intelligent.”). The government bears the burden of showing a valid waiver, *id.*,  
10 which must be established by a preponderance of the evidence, *Kelley*, 953 F.2d at 564,  
11 *disapproved of on other grounds by United States v. Kim*, 105 F.3d 1579, 1581 (9th Cir. 1997).  
12 There is a presumption against waiver. *Binder*, 769 F.2d at 599.

13           1. Voluntariness

14           “The sole concern of the Fifth Amendment, upon which *Miranda* was based, is  
15 governmental coercion.” *Colorado v. Connelly*, 479 U.S. 157, 170 (1986). The voluntariness  
16 of a *Miranda* waiver depends on the absence of police overreaching, not on “free choice in any  
17 broader sense of the word.” *Id.* Thus, if a defendant feels compelled to waive his rights by  
18 reason of any compulsion not flowing from law enforcement, the Fifth Amendment is not  
19 implicated. *Id.*

20           To determine whether a confession is voluntary, a court considers “whether,  
21 under the totality of the circumstances, the challenged confession was obtained in a manner  
22 compatible with the requirements of the Constitution . . . .” *United States v. Bautista-Avila*, 6  
23 F.3d 1360, 1364 (9th Cir. 1993) (quotation marks and citation omitted). “A statement is  
24 involuntary if it is extracted by any sort of threats or violence, [or] obtained by any direct or  
25 implied promises, however slight, [or] by the exertion of any improper influence.” *Id.*  
26 (quotation marks and citations omitted) (alteration in original).

27           Here, the government has met its burden to show by a preponderance of the  
28 evidence defendant’s waiver was voluntary. The transcript of the interrogation shows

1 defendant was rational, articulate, cooperative, and polite. Tr. at 6, ECF No. 23-5 (“Define  
2 extreme candor.”); *id.* at 8 (“And, I can show you on the computer how to get access to  
3 those.”); *id.* at 33 (“I had never been subjected to an environment as a journalist or just even as  
4 a human being. I, I just never seen what I saw in that room before. It took me aback. I wasn’t  
5 expecting it.”). No part of the transcript suggests defendant was so affected by Trazodone or  
6 his abrupt awakening that he was incapable of waiving his rights. Defendant also was given  
7 the choice to conduct the interview elsewhere, but he chose to stay in his home. Tr. at 3.

8           Furthermore, there is no evidence to suggest the interrogating agents even knew  
9 defendant was under the influence of Trazodone or any other medication. The transcript shows  
10 the interrogation was amiable, and defendant does not point to instances of improper agent  
11 conduct. Therefore, even if defendant felt compelled to confess because of Trazodone’s  
12 effects, the absence of evidence of police overreaching dooms his attempt to suppress his  
13 statements. *See Connelly*, 479 U.S. at 170. In short, the totality of the circumstances reveals  
14 the agents did not exert any improper influence on defendant to obtain his confession. *See*  
15 *Bautista-Avila*, 6 F.3d at 1364. This conclusion accords with the relevant case law in this  
16 Circuit. *See Martin*, 781 F.2d at 674 (fact that hospitalized defendant may have been in pain  
17 and under influence of pain medication that made him drowsy during questioning by police at  
18 hospital did not render his statements to police involuntary; defendant was awake and relatively  
19 coherent during questioning, had not received excessive quantities or unusual combinations of  
20 drugs, and had shown willingness to speak to police); *Kelley*, 953 F.2d at 565–66 (“The  
21 preponderance of the evidence shows that Kelley’s ability to think rationally was unimpaired  
22 by his being on the verge of heroin withdrawal during part of the interrogation.”); *Lewis*, 833  
23 F.2d at 1384–85 (statements taken in a hospital several hours after defendant was administered  
24 general anesthetic held to be voluntary).

25           Defendant’s attempt to distinguish *Martin*, *Kelley*, and *Lewis* falls flat. Those  
26 cases involved even closer calls than the instant case, because law enforcement in those cases  
27 knew the defendants they interrogated were under the influence of drugs, both because they  
28 were explicitly so told and because the defendants acted in an impaired manner; they continued

1 to question them anyway. *Martin*, 781 F.2d at 672; *Kelley*, 953 F.2d at 564; *Lewis*, 833 F.2d at  
2 1382–83. In contrast here, there is no indication the interrogating agents knew or even  
3 suspected defendant was under the influence of any medication. Accordingly, the agents could  
4 not have exploited defendant’s mental state to compel a confession. Voluntariness is concerned  
5 about police compulsion. No evidence of that exists here.

## 6 2. Knowing and Intelligent

7 Distinct from the voluntariness of a waiver of *Miranda* rights is whether that  
8 waiver was knowing and intelligent: in other words, the waiver ““must have been made with a  
9 full awareness both of the nature of the right being abandoned and the consequences of the  
10 decision to abandon it.”” *Derrick v. Peterson*, 924 F.2d 813, 820 (9th Cir. 1990) (quoting  
11 *Connelly*, 479 U.S. at 573); *see also Cox v. Del Papa*, 542 F.3d 669, 675 (9th Cir. 2008)  
12 (“[T]he voluntariness component turns upon external factors, whereas the cognitive component  
13 depends upon mental capacity. Although courts often merge the two-pronged analysis, the  
14 components should not be conflated.”).

15 A court deciding this issue must consider the totality of the circumstances. *Id.*  
16 Factors courts consider include the defendant’s mental capacity and language skills, whether  
17 the defendant signed a written waiver, whether he appeared to understand his rights, whether  
18 his rights were individually and repeatedly explained to him, and whether he had prior  
19 experience with the criminal justice system. *United States v. Garibay*, 143 F.3d 534, 538 (9th  
20 Cir. 1998). “The government’s burden to make such a showing is great, and the court will  
21 indulge every reasonable presumption against waiver of fundamental constitutional rights.”  
22 *United States v. Garibay*, 143 F.3d 534, 537 (9th Cir. 1998) (quotation marks and citation  
23 omitted).

24 The government has borne its burden to show by a preponderance of the  
25 evidence defendant’s waiver was knowing and voluntary, by providing the transcript of the  
26 interrogation. The portions of the transcript already cited reveal a sophisticated journalist  
27 fluent in English. While the agents did not explicitly ask defendant whether he understood his  
28 rights, they did say “ok?” after informing him of his rights, to which defendant replied “yea.”




1 Tr. at 2. Moreover, defendant explained why he decided to talk to the agents: “This is one of  
2 the reasons why I’m talking to you as opposed to saying, you know, I want a lawyer, or I want  
3 to talk to, you know, counsel at Tribune, or, again I’m sorry, Reuters or anything like that is  
4 because, you know, I did it.” Tr. at 53. Defendant also stated he would be willing to be a  
5 cooperating witness if that would help him avoid publicity. Tr. at 65. Defendant also provided  
6 agents a written statement, although the record does not reveal whether that statement contains  
7 a written waiver of his *Miranda* rights.

8 The record also is silent as to whether defendant has had prior experience with  
9 the criminal justice system. But the record as a whole, including the transcript of the  
10 interrogation, point to one inescapable conclusion: defendant is a worldly, educated, intelligent  
11 person. The totality of the circumstances show by a preponderance of the evidence that  
12 defendant waived his *Miranda* rights “with a full awareness both of the nature of the right  
13 being abandoned and the consequences of the decision to abandon it.” *Derrick*, 924 F.2d at  
14 820.

15 IT IS THEREFORE ORDERED that defendant’s motion to suppress evidence,  
16 ECF No. 23, is DENIED.

17 DATED: March 23, 2014.

18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

  
UNITED STATES DISTRICT JUDGE