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.

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

II. THE WARRANT AND ITS EXECUTION

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

> a. Records relating to unauthorized computer access and/or computer intrusions including attacks on the Tribune Media Co. server located in Los Angeles California [sic] for the period December 1, 2012 to the present;
>
> b. Records relating to the trafficking in usernames and passwords;
>
> c. Records relating to:
>
> i. foxmulder4099@yahoo.co.uk
>
> ii. cybertroll69x@hotmail.com
>
> iii. walterskinner5099@Yahoo.co.uk
>
> iv. cancerman4099@yahoo.co.uk
>
> v. fox40truthers@gmail.com
>
> vi. dudenudeguy@gmail.com
>
> vii. The X-Files
>
> viii. AESCracked
>
> ix. Sabu
>
> x. Kayla

xi. Sharpie

xii. Switch

xiii. Blergh

xiv. N3ot0xin

xv. Chronom

xvi. Rand0m

xvii. Pellsson

xviii. Tred

xix. Garrett

xx. Tflow

xxi. Arseface

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

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

> 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 in digital form, on any computer, or digital device 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 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 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).
>
> i. 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 evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the computer or digital device.
>
> k. 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 . . . .

ECF No. 23-1 at 7-8.

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

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

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

Around this time, a Fox 40 customer complained about receiving an unsolicited email from the email address of fox40truthers@gmail.com. *Id*. at 17.

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

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

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

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

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

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

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

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

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

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

III. THE MOTION TO SUPPRESS THE PHYSICAL EVIDENCE

A. Background

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

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

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

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

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

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

B. Fourth Amendment

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

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

C. Computer Searches, General Searches

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

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

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

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

---

[1] Although defendant characterizes the search as overbroad, ECF No. 26 at 3, he relies on cases discussing the specificity requirement. For example, the case law characterizes *United States v. Tamura* as a particularity, rather than an overbreadth, case, though it does also suggest the agents' refusal to return the documents not named in the warrant was "an unreasonable and therefore unconstitutional manner of executing the warrant." 694 F.2d 591, 597 (9th Cir. 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).

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

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

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

Finally, defendant turns to *CDT III* and its caution that "[t]he point of the *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 of office file systems and computer databases." 621 F.3d at 1170. In *CDT III*, the government sought information about ten baseball players it suspected had used steroids, from third parties not suspected of any involvement in the alleged crimes. As the result of executing warrants in the Central District of California and the District of Nevada and issuing a grand jury subpoena in the Northern District, the government seized a computer database containing drug testing information about hundreds of athletes despite CDT's offer to provide all the information in its possession about the ten named baseball players. *Id*. at 1166-67. Three district courts ordered the return of the property seized and quashed subpoenas, troubled by the breadth of the information seized. The government timely appealed in two of the actions and the Ninth Circuit affirmed. It noted the government had failed to follow the *Tamura* procedures the Central District's magistrate judge had built into the warrant to protect intermingled data, and as information obtained during the execution of the Central District warrants made execution of the Nevada warrant feasible, it upheld the Nevada district court's condemnation of the agents' refusal to segregate and return the data on the players not suspected of steroid use. *Id*. at 1170.

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

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

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

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

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

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

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

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

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

[2] Defendant also argues the removal of the equipment was not monitored by a neutral, detached magistrate judge, but a magistrate judge did sign the warrant authorizing the removal.

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

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

D. Staleness

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

Generally, "[a]n affidavit must be based on facts so closely related to the time of the issuance of the warrant as to justify a finding of probable cause at that time." *Lacy*, 119 F.3d at 745. However, "[i]nformation underlying a warrant is not stale '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.'" *Schesso*, 730 F.3d at 1047 (quoting *Lacy*, 119 F.3d at 756-46). In evaluating staleness, the court considers "the particular facts of the case and the nature of the criminal activity and property sought." *Lacy*, 119 F.3d at 745; *see also United States v. Farmer*, 370 F.3d 435, 439 (4th Cir. 2004) ("[T]he vitality of probable cause cannot be quantified by simply counting the number of days between the occurrence of the facts supplied and the issuance of the affidavit.") (internal citation & quotation marks omitted).

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

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

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

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

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

E. *Franks*

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

> where the defendant makes a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the 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.

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

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

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

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

IV. THE MOTION TO SUPPRESS THE STATEMENTS

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

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

A. Waiver of *Miranda* Rights

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

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

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

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

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

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

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

/////

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

1. Voluntariness

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

To determine whether a confession is voluntary, a court considers "whether, under the totality of the circumstances, the challenged confession was obtained in a manner compatible with the requirements of the Constitution . . . ." *United States v. Bautista-Avila*, 6 F.3d 1360, 1364 (9th Cir. 1993) (quotation marks and citation omitted). "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." *Id.* (quotation marks and citations omitted) (alteration in original).

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

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

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

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

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

2. Knowing and Intelligent

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

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

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

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

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

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

DATED: March 23, 2014.

UNITED STATES DISTRICT JUDGE