5. In summary, the following affidavit sets forth facts that MATTHEW KEYS transmitted, via the Internet, communications resulting in an intrusion into a protected computer owned by Tribune Media Company, located in Los Angeles, California, which computer was used to publish news and post advertising in interstate and foreign commerce.

6. Since approximately 2008, a loosely affiliated organization of computer hackers, known as "Anonymous," has claimed responsibility for numerous computer crimes in retaliation for actions with which Anonymous disagrees, including intrusions and DoS attacks targeting foreign government websites in Australia, Egypt, Sweden, Tunisia, as well as the websites and/or computer networks of Amazon, PayPal, MasterCard, Visa, the Church of Scientology and HBGary, a company based in Sacramento, California.

7. On or about December 1, 2010, KTXL Fox 40 (hereafter "Fox 40"), a television station located in Sacramento, California, learned that its e-mail contact list had been compromised. The e-mail list was located on the "P2P Server" of Fox 40's parent company Tribune Media, located in Los Angeles, California. The first person to notice the problem was Fox 40's news producer (the "Producer"), who began receiving unsolicited e-mails from an unknown person who claimed to have the e-mail list.

8. The Producer contacted the FBI in Sacramento about the suspicious e-mails. The Producer identified MATTHEW KEYS, a former employee whose job title was "Web Producer," as a potential suspect. Approximately one month before this incident, in October 2010, the

Producer had terminated KEYS' employment. KEYS had been responsible for maintaining Fox 40's Twitter and Facebook accounts, which he did using his own (non-Fox 40 news) e-mail account. According to the Producer, after departing, KEYS changed the passwords to both the Twitter and Facebook accounts, preventing any other employee of Fox news from accessing or modifying them. During the time that KEYS was in control of the Twitter and Facebook accounts, about 6,000 followers were deleted from the Fox 40 Twitter account. This was a significant event for Fox 40, as the Twitter account was a revenue stream for the company. During that time, the Fox 40 Twitter account was also used to post news headlines from the station's competition. This was an embarrassing situation for Fox 40; four days passed before the Producer was able to regain control of the accounts.

A. The Suspicious December 2010 E-Mails

9. On or about December 1, 2010, the Producer received the first e-mail from the account "foxmulder4099@yahoo.co.uk," which had the subject "Santas Lap." The e-mail message suggested that the writer had obtained the e-mail addresses of all of Fox 40's customers. Several e-mails were provided in the e-mail as proof of this claim. Numerous e-mails were exchanged between the Producer and the person using the e-mail account "foxmulder4099@yahoo.co.uk." These e-mails carried the same theme of disparaging remarks about Fox 40 business practices.

10. On or about December 2, 2010, a separate e-mail address, "cybertroll69x@hotmail.com," was used to forward to the Producer a message purportedly sent from an individual known as "J.H.," a legitimate Fox 40 employee, in which "J.H." claimed

foxmulder4099 was MATTHEW KEYS. J.H, in e-mail conversation with the Producer, denied having sent the above e-mail.

11. "cybertroll69x@hotmail.com" was registered by someone purporting to be MATT KEYS from a zip code of 95824 for Sacramento, California; these values are set by the user upon account creation and are not subject to verification. The account was activated on December 2, 2010 and accessed only once by the user. The IP address used to access this account was 98.208.49.74, and resolved to a location in Sacramento, California. An attempt to identify the user of this IP address was unsuccessful.

12. On or about December 3, 2010, Fox 40 News received an e-mail from a person purporting to be "Cancer Man." The subject line of the e-mail was "Re: Donating" the e-mail contained the phrase "watch yourselves Fox 40" and contained a forwarded e-mail which had been sent from the American Cancer Society to Cancer Man. The forwarded e-mail appeared to be a response from the American Cancer Society to Cancer Man. A review of the response from the American Cancer Society indicated that the person purporting to be Cancer Man had sent an e-mail to the American Cancer Society from the e-mail address "CancerMan4099@yahoo.co.uk" and had provided a contact name of "MATTHEW KEYS."

13. On or about December 3, 2010, a Fox 40 customer complained about receiving unsolicited e-mail from an e-mail address of "fox40truthers@gmail.com."

14. On or about December 6, 2010, the Producer received an e-mail from the person purporting to be "Walter Skinner" with an e-mail address of WalterSkinner5099@yahoo.co.uk. This e-mail appeared to be in the form of a press release. The e-mail referred to the Producer's Facebook page.

15. A complete listing of all e-mail addresses used to send suspicious e-mails to Fox 40 is as follows:

a. "foxmulder4099@yahoo.co.uk"

b. "cybertroll69x@hotmail.com"

c. "walterskinner5099@Yahoo.co.uk"; and

d. cancerman4099@yahoo.co.uk

e. "fox40truthers@gmail.com."

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

B. <u>E-Mails Between MATTHEW KEYS and the Producer Concerning Anonymous</u>

16. On or about December 12, 2010, a person purporting to be MATTHEW KEYS using an e-mail address of "Matthew@sactownmedia.com" sent the Producer an e-mail. In this e-mail, KEYS told the Producer that he had infiltrated the group Anonymous. KEYS further stated he had access to future Anonymous operations including operations against PayPal, Amazon, the Los Angeles Times, Fox News and others.

17. On or about December 12, 2010, the Producer spoke with MATTHEW KEYS in a telephone conversation. During the conversation they discussed a computer intrusion by Anonymous into a website called Gawker. KEYS told the Producer he had entered an IRC chat room with over 2,000 members. KEYS further stated that while in this chat room he met

someone who invited him into a private chat room populated by 15 highly skilled hackers. KEYS told the Producer that he had computer records of his interaction with the Anonymous group members. KEYS said he told the hackers about his past journalism experience. In this call, KEYS also denied having been in any way involved with the suspicious e-mails the Producer had been receiving (referred to above).

C. The Defacement of the LA Times Website

18. On or about December 14, 2010, two days after KEYS predicted that the LA Times might be a target of Anonymous, the FBI in Sacramento learned that a server belonging to Tribune Media (parent company of both the LA Times and Fox 40) was compromised and at least one headline was altered. According to an internal investigation conducted by employees of Tribune Media, the person or persons who committed the computer intrusion had utilized the Tribune Media accounts "Anon1234" and "Arseface," each of which were identified as unauthorized users on the Tribune Media server. Further, it was reported to the FBI in Sacramento that an employee of the Tribune observed in Anonymous IRC channels a user by the name of "sharpie" claiming involvement in the LA Times defacement.

D. KEY's Acknowledgment of his Participation in Internet Chats with Anonymous

19. On or about March 18, 2011, MATTHEW KEYS wrote on the website, producermatthew.com, for which a Whois query returns registrant "Matthew Keys, 4655 Fruitridge Road, Sacramento, California 95820, United States":

> Earlier today, the website Gawker published a story outing several high-level members of the hacktivist group Anonymous. The Gawker story sourced me in several paragraphs as a journalist who had gained access to secret chat rooms in which high-ranking

> members of the group would plan various attacks on websites, to be executed by common members of Anonymous in public chat rooms. I provided Gawker with just one of dozens of logs that were taken during my two-month access to top level hackers within Anonymous. In addition to providing Gawker with one log, I provided the PBS NewsHour with a record back in December.
>
> I identified myself as a journalist during my interaction with the top-level Anonymous hackers and at no time did I offer said individuals any agreement of confidentiality. In fact, I asked several of them for their feelings should they be exposed. They seemed, by and large, indifferent.

20. On or about June 26, 2011, KEYS further wrote on his website, producermatthew.com:

> I have been made aware that a computer hacker who goes by the name of Sabu has been allegedly exposed by a white hat hacker named The Jester.
>
> Hacker Sabu was one of several I observed in a secret, top-level chat room run on the same server that Anonymous widely used to carry out and coordinate its denial of service attacks against merchants and government websites between December 2010 and January 2011. The chat room was internetfeds and possessed highly intelligent black hat hackers who seemed to carry out attacks that were not in the name, or aligning with the agenda, of the hacktivist group collective Anonymous.

E. <u>KEY's Use of the Username "AESCracked" During Internet Chats</u>

21. On March 6, 2012, KEYS further posted on his website, producermatthew.com an image (provided below as Exhibit A, a contextual screenshot, and Exhibit B, a close-up) of an IRC chat on the Mac operating system under which he wrote: "During my observance of Anonymous/LulzSec hackers in a chat room called 'InternetFeds,' ... Log recorded December 22, 2010." I know from my experience that the program shown appears to be "Colloquy," a chat program available for the Mac, which I have used and found to be identical to that shown in the image. I know from my experience that when a person uses the Colloquy program, Colloquy will

show that person's username in red (as opposed to all other usernames, which appear in orange). In the aforementioned image posted by KEYS, the username in red was intentionally blurred, but is approximately ten characters in length, and ends in "d." Further, the username in red is referred to by another user as "AES."

22. In December 2011, the FBI in Sacramento was reviewing evidence pertaining to a computer intrusion by Anonymous into a local company called HBGary. While reviewing digital evidence which had been seized pursuant to a federal search warrant, FBI investigators noted a chat in which "Kayla" discussed KEYS:

a. In a chat believed to have taken place in March 2011 between Kayla and others, Kayla wrote, "this 'keys' faggot we think is AESCracked who was an ex journalist..."

b. Kayla also wrote, "but in that gawker article it says his name is 'Matt Keys' lol he's not so innocent and we have logs of him too, he was the one who gave us passwords for LA times, fox40 and some others, he had superuser on alot of media"

Further, Kayla posted a link to the www.producermatthew.com blog discussed above wherein MATTHEW KEYS admitted providing logs from Anonymous IRC channels to Gawker.

23. In December 2011, I reviewed chat logs seized during a search warrant in Toledo, Ohio for digital media belonging to a suspected member of Anonymous going by the usernames "Owen" and "Iowa." These logs included excerpts from the above-mentioned #internetfeds chat room during the December 2010 to January 2011 timeframe. I have prepared a list of what I believe to be relevant findings from these chat logs as Exhibit C. Some of the more pertinent quotes from the #internetfeds chat room, referred to above, are as follows:

Dec 08 20:55:12 Sabu that would be nice to get access to fox. let me know if I can get access. I want to see if I can get further in
...
Dec 08 20:59:20 **AESCracked** **i'm not a hacker.**
Dec 08 20:59:23 **AESCracked** **i'm an ex-employee**
...
Dec 08 21:00:47 **AESCracked** **user: anon1234**
Dec 08 21:00:50 **AESCracked** **pass: common2**
Dec 08 21:01:23 **AESCracked** **go fuck some shit up!**
Dec 08 21:01:29 sharpie thanks very much
Dec 08 21:01:32 Sabu AESCracked: thank you.

(emphasis added).

24. In the above exchange, AESCracked, who I believe to be MATTHEW KEYS, provided the user name and password utilized in the intrusion of the Tribune Media server located in Los Angeles, California, as described in paragraph 18 above. This password granted access to the three Content Management Systems controlling the content contained on the websites of Tribune's subsidiaries Fox 40, based in Sacramento, California, and the Los Angeles Times, based in Los Angeles, California. As further described in Exhibit C:

a. AESCracked specifically asked if anyone was interested in defacing Fox or the LA Times. As described in paragraph 18 above, the same server in Los Angeles served both Fox 40 as well as the LA Times.

b. AESCracked claimed to be an ex-employee. As described in paragraph 8 above, KEYS had recently been terminated by Fox 40 and was unemployed as of December 2010.

c. AESCracked asked if anyone wished to purchase an e-mail list. As described in paragraph 13 above, the Fox 40 e-mail list had been stolen.

d. AESCracked communicated with Sabu, Kayla, Sharpie and others about the username and passwords in the IRC channel #internetfeds. As described in

paragraphs 19 to 20 above, KEYS admitted on his website to communicating with Sabu during the very same December 2010 timeframe, in the very same IRC channel "internetfeds".

25. AESCracked accessed the #OperationPayback[1] IRC chat channel from IP address 78.129.220.46 in about January 2011. After reviewing documents provided by Yahoo! Inc., I have learned that this IP address was the one used by the sender of an e-mail from "foxmulder4099@yahoo.co.uk" to Fox 40 as described in paragraphs 9 and 10 above.

26. On January 5, 2011, AESCracked was banned from the AnonOps chat server[2] after having been accused by members of the #internetfeds channel of leaking information to the media. Shortly thereafter, still on January 5, 2011, users of the #internetfeds channel including Tred and Kayla identified AESCracked logging in under a slightly modified username "A2SCracked" from the IP address 75.53.171.204:

> * ***Notice -- Client connecting at belldandy.anonops.ru:A2SCracked (A2SCracked@75-53-171-204.lightspeed.nscrca.sbcglobal.net).

I have learned from AT&T that the IP address 75.53.171.204 was registered to KEYS, and only KEYS, on January 5, 2011, at 3381 Shadow Tree Drive, Apt 327, Sacramento, California, 95834.

27. On July 6, 2012, I reviewed portions of the book *We Are Anonymous* by Parmy Olson, which was published June 5, 2012. On page 446 of this book, Olson wrote: "Owen's

---

1 Operation Payback, as of December 2010, was an Internet-based DoS attack campaign attributed to Anonymous, and targeting PayPal and other companies. Operation Payback participants claimed the attacks were in retaliation for PayPal's decision to halt the processing of donations to WikiLeaks following WikiLeaks' controversial public release of sensitive US documents. Communication amongst participants occurred largely via IRC, utilizing channels such as the #OperationPayback channel denoted above.

2 The AnonOps chat server is a computer that hosted multiple Internet chat channels including, but not limited to, #internetfeds and #OperationPayback.

quote ... comes from screenshots of the #InternetFeds chat room made by freelance journalist Matthew Keys, which were e-mailed to me by Keys in early 2011. Keys was invited to observe the goings-on in InternetFeds from December of 2010 to January of 2011. He used the nickname AESCracked." Olson also wrote on page 446: "Further description of dialogue and content from discussions in the channel comes from scores of screenshots provided by Matthew Keys."

28. Also on July 6, 2012, I read a Twitter post dated May 25, 2012, in which KEYS, username @ProducerMatthew, wrote "This is the book I'm in. You should think about buying it." In this post, KEYS linked the book *We Are Anonymous*, and addressed his comment to Parmy Olson's Twitter username @parmy.

29. According to the logs excerpted in Exhibit C, AESCracked, as dudenudeguy@gmail.com, sent what he said were nude pictures of himself to an the person utilizing the moniker "Owen." With "Owen," AESCracked claimed to be a white male, with brown hair and brown eyes, from the West Coast. I have seen a picture of KEYS; he appears to be a white male with brown hair and brown eyes.

30. Other individuals with whom AESCracked discussed hacking and Anonymous included:

a. Sharpie

b. Switch

c. Blergh

d. N3ot0xin

e. Chronom AKA Tflow

f. Rand0m

g. Pellsson

h. Tred

i. Garrett

As discussed in paragraph 18 above, the moniker "sharpie" was associated with the defacement of the LA Times website.

F. Approximate Damage to Tribune Media

31. According to the Managing Director, Technology Architect at Tribune Media, approximately 333 man hours were spent by Tribune employees responding to the compromise of Tribune Media's server on December 14, 2010, at an estimated labor cost of $17,650.40. This estimate did not include costs relating to hardware and/or service upgrades implemented by Tribune following the intrusion, costs relating to the stolen e-mail list affecting Fox 40 News in Sacramento, nor ad revenue losses taken as a result of the attack.

G. Summary of KEYS's Involvement in the Tribune Media Compromise

32. Based on the above, there is probable cause to believe the following: after being terminated from his job at Fox 40 in Sacramento, California, KEYS accessed in an unauthorized manner the server in Los Angeles belonging to Tribune Media. From this server, KEYS stole the e-mail list of Fox 40's customers. KEYS offered to sell this list to members of Anonymous. KEYS also used this list to send spurious e-mails to Fox 40's customers and to disrupt the business operations of Fox 40. Furthermore, KEYS then provided the user name and password, as well as instructions and guidance, to members of the group Anonymous with the intent of causing harm and financial damage to the media properties of Tribune Media, including the LA Times, based in Los Angeles.

H. KEYS Currently Resides at the SUBJECT PREMISES, Along With Evidence and Instrumentalities of His Crimes

33. On February 7, 2012, FBI investigators confirmed with United States Postal Inspector Michael Chavez that, on January 18, 2012, MATTHEW KEYS filed a change of address request with the United States Postal Service, giving his new address as 5123 Riverside Station Blvd, Secaucus, NJ 07094.

34. I have also read posts by KEYS on his web page, producermatthew.com, in which he stated he was moving to New York from California in January of 2012.

35. On October 2, 2012, Newark-based FBI agents confirmed that KEYS initially resided at 5123 Riverside Station Blvd, Secaucus, NJ 07094, but recently moved to unit 5201 in the same complex – the SUBJECT PREMISES.

36. Furthermore, I have probable cause to believe that the evidence and instrumentalities of the Specified Federal Offenses can be found on the computer(s) and/or digital media used by MATTHEW KEYS and located at the SUBJECT PREMISES. The bases for my belief are as follows: (1) as described above, there is probable cause to believe that KEYS participated in committing the Specified Federal Offenses; (2) evidence of the Specified Federal Offenses, including the chat logs discussed in paragraph 21 (*see also* Exhibits A and B attached hereto) was retained on KEYS's computer as recently as March 6, 2012, post-dating his move from Sacramento, California to Secaucus, New Jersey; (3) KEYS presently maintains the website www.producermatthew.com, on which he has stated that he actively monitors the Internet and updates his website from his residence; (4) based upon my training and experience, and the investigation to date, I know that KEYS is proficient with computers and related technology, and

that individuals such as KEYS generally retain their computers and attendant digital media when moving from one residence to another; and (5) based on my training and experience, I am aware that data, even if deleted, will remain on a computer until overwritten. Finally, there is probable cause to believe that KEYS maintains data from his interaction with members of Anonymous at the SUBJECT PREMISES because he regards this as an accomplishment that he wants to publish and receive credit for in the future. Tellingly, his web blog, www.producermatthew.com, is still active and contains stories going back to May 2010, including stories about Anonymous from approximately December 2010.