

UNITED STATES DISTRICT COURTfor the
District of Minnesota

UNITED STATES OF AMERICA

v.

Case No.

15-MJ-382 (JSM)

ZACHARY LEE MORGENSTERN

CRIMINAL COMPLAINT

I, the undersigned complainant, being duly sworn, state the following is true and correct to the best of my knowledge and belief.

COUNT ONE

(Threats To Use Explosives)

On or about January 6, 2015, in Lyon County, in the State and District of Minnesota, the defendant, ZACHARY LEE MORGENSTERN, through the use of telephone or other instrument of interstate or foreign commerce willfully made a threat to kill, by means of an explosive, in and affecting interstate or foreign commerce, in violation of Title 18, United States Code, Section 844(e).

COUNT TWO

(Threats To Use Explosives)

On or about January 11, 2015, in Lyon County, in the State and District of Minnesota, the defendant, ZACHARY LEE MORGENSTERN, through the use of an instrument of interstate or foreign commerce, namely email, willfully made a threat to kill, by means of an explosive, in and affecting interstate or foreign commerce, in violation of Title 18, United States Code, Section 844(e).

COUNT THREE

(Making Threatening Communications)

On or about January 9, 2015, in Lyon County, in the State and District of Minnesota, the defendant, ZACHARY LEE MORGENSTERN, knowingly and willfully transmitted in interstate commerce a communication containing a threat to injure the person of another – specifically, he placed a hoax telephone call to the Marshall, Minnesota, Police Dispatch, falsely claiming that he was going to “shoot up” the Marshall High School and kill everybody, in violation of Title 18, United States Code, Section 875(c).



COUNT FOUR

(False Information and Hoaxes – Threats To Use Firearms)

On or about January 8, 2015, in Lyon County, in the State and District of Minnesota, the defendant, ZACHARY LEE MORGENSTERN, engaged in conduct with intent to convey false and misleading information under circumstances where such information may reasonably have been believed and where such information indicated that an activity had taken, was taking, and would take place that would constitute a violation of chapter 44 of Title 18, United States Code (namely, 18 U.S.C. § 924(c)(1)(A) prohibiting use of a firearm in relation to a crime of violence for which he may be prosecuted in a court of the United States) – specifically, he placed a hoax telephone call to the Marshall, Minnesota, Police Dispatch, falsely claiming that he had he had taken a father and son hostage at gunpoint at their residence in Marshall, Minnesota, and he claimed he had already shot the father in the leg and would soon shoot both hostages in the head, all in violation of Title 18, United States Code, Sections 1038(a)(1) and 2.

I further state that I am a(n) Special Agent and that this complaint is based on the following facts:

SEE ATTACHED AFFIDAVIT

Continued on the attached sheet and made a part hereof: Yes No



Complainant's signature

Glenn Moule, FBI Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date:

5/11/15

City and State: Minneapolis, MN



Judge's Signature

Honorable Janie S. Mayeron, U.S. Magistrate Judge

Printed Name and Title

STATE OF MINNESOTA)
)
COUNTY OF HENNEPIN)

15-MJ-382 (JSM)
ss. AFFIDAVIT OF GLENN MOULE

1. I am a Special Agent (“SA”) with the Federal Bureau of Investigation (“FBI”) and have been so employed for over five years. I am currently assigned to the Mankato Resident Agency with the Minneapolis, Minnesota, Division of the FBI and work on various criminal offenses to include white collar crime and computer related crimes. I have received specialized FBI training and in the investigation of computer and computer related crimes.

2. This affidavit is made in support of a Complaint charging ZACHARY LEE MORGENSTERN (“MORGENSTERN”) with making threatening communications in violation of Title 18, United States Code, Section 844(e) – explosives, threats to use, Section 875(c) – interstate threatening communications, and Section 1038(a) - false information and hoaxes. The statements in this Affidavit are based on my investigation of this matter which includes information provided to me by other law enforcement officers whom I believe to be reliable. This affidavit contains information to support probable cause, but is not intended to convey facts of the entire investigation.

I. The Internet and Definitions of Technical Terms Pertaining to Computers

3. As part of my training, I have become familiar with the Internet (commonly known as the World Wide Web), a global network of computers, as defined at 18 U.S.C. § 1030(e)(1), and other electronic devices that communicate with each other using various means, including standard telephone lines, high-speed telecommunications links (e.g., copper and fiber optic cable), and wireless transmissions including satellite. Due to the structure of the Internet, connections between computers on the Internet routinely cross state and international borders, even when the computers communicating with each other are in the same state. Individuals and entities use the Internet to gain access to a wide variety of information, to send information to, and receive

information from, other individuals, to conduct commercial transactions, and to communicate via electronic mail (“e-mail”). An individual who wants to use Internet e-mail must first obtain an account with a computer that is linked to the Internet – for example, through a university, an employer, or a commercial service – which is called an “Internet Service Provider” or “ISP” (see definition of “Internet Service Provider” below). Once the individual has accessed the Internet, that individual can use Internet mail services, including sending and receiving e-mail. In addition, the individual can visit Web sites and make purchases from them.

4. Set forth below are some definitions of technical terms used throughout this Affidavit.

a. **Internet Service Providers** or “**ISPs**” are commercial organizations that provide individuals and businesses with access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communication equipment. ISPs can offer various means to access the Internet including telephone based dial-up, broadband based via a digital subscriber line (“DSL”) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password. ISPs maintain records pertaining to their subscribers (regardless of whether those subscribers are entities or

individuals). These records may include account application information, subscriber and billing information, account access information (often times in the form of log files), e-mail communications, information concerning content uploaded and/or stored on or via the ISPs servers, and other information, which may be stored both in computer data format and/or in written or printed record format.

b. **Internet Protocol Address** or **IP Address** refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer the same IP address each time the computer accesses the Internet.

c. **Anonymous proxy** or **anonymizer** is a tool that attempts to make activity on the internet untraceable. A proxy server acts as an intermediary and privacy shield between the client computer and the rest of the internet. The proxy hides the client computer's identifying information.

II. Twitter Services

5. Twitter owns and operates a free-access social networking website of the same name that can be accessed at <http://www.twitter.com>. Twitter allows its users to create their own profile pages, which can include a short biography, a photo of themselves, and location information. Twitter also permits users to create and read 140-character messages called "Tweets," and to restrict their "Tweets" to individuals whom they approve. These features are described in more detail below.

6. Upon creating a Twitter account, a Twitter user must create a unique Twitter username and an account password, and the user may also select a different name of 20 characters

or fewer to identify his or her Twitter account. The Twitter user may also change this username, password, and name without having to open a new Twitter account.

7. Twitter asks users to provide basic identity and contact information, either during the registration process or thereafter. This information may include the user's full name, e-mail addresses, physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, and other personal identifiers. For each user, Twitter may retain information about the date and time at which the user's profile was created, the date and time at which the account was created, and the Internet Protocol ("IP") address at the time of sign-up. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access a given Twitter account.

8. A Twitter user can post a personal photograph or image (also known as an "avatar") to his or her profile, and can also change the profile background or theme for his or her account page. In addition, Twitter users can post "bios" of 160 characters or fewer to their profile pages.

9. Twitter also keeps IP logs for each user. These logs contain information about the user's logins to Twitter including, for each access, the IP address assigned to the user and the date stamp at the time the user accessed his or her profile.

10. As discussed above, Twitter users can use their Twitter accounts to post "Tweets" of 140 characters or fewer. Each Tweet includes a timestamp that displays when the Tweet was posted to Twitter. Twitter users can also "favorite," "retweet," or reply to the Tweets of other users. In addition, when a Tweet includes a Twitter username, often preceded by the @ sign, Twitter designates that Tweet a "mention" of the identified user. In the "Connect" tab for each account, Twitter provides the user with a list of other users who have favorited or retweeted the

user's own Tweets, as well as a list of all Tweets that include the user's username (*i.e.*, a list of all "mentions" and "replies" for that username).

III. Details of the Investigation

A. On January 6, 2015, @RIURichHomie called in a fake bomb threat to a high school in Marshall, Minnesota.

11. On January 6, 2015, a bomb threat was called into the Marshall, Minnesota Police Department dispatch center. The caller claimed to be D.R., a 17-year-old male from Marshall, Minnesota. The caller claimed he had placed bombs around Marshall High School that were set to detonate in approximately one hour. School officials and responding officers searched the school and determined the threat was a hoax. No caller ID information was associated with the call when it came into Marshall Police dispatch.

12. Approximately four hours after the bomb threat was received by Marshall Police dispatch, D.R. received a tweet from Twitter user @RIURichHomie which read "OOPS. NICE BOMB THREAT. TEEHEEEEEEEEE :)." D.R. and his friend, S.V., also received a subsequent tweet on January 6, 2015 from @RIURichHomie in which @RIURichHomie claimed responsibility for the bomb threat and threatened to issue a bomb threat for the school attended by D.R. and S.V.

B. On January 7, 2015, @RIURichHomie harassed S.V.'s juvenile girlfriend with 222 text messages in 46 minutes.

13. On January 7, 2015, T.P., the juvenile girlfriend of S.V., had her cellular phone rendered inoperable due to receiving a series of 222 consecutive text messages over a period of 46 minutes from a telephone number that was unknown to her. The area code of the originating telephone number was 210, which is a Texas area code. All 222 text messages consisted of the identical text message "FRM: anonymously.lulzsec@gmail.com MSG: @RIURichHomie."

C. On January 8, 2015, @RIURichHomie called in a fake hostage situation at victim D.R.'s home.

14. On January 8, 2015, a call was received by Marshall Police dispatch from an unknown male who claimed he had taken a father and son hostage at gunpoint at their residence in Marshall. The caller claimed he had already shot the father in the leg and would soon shoot both hostages in the head. The address provided by the caller for the hostage situation was the residence of D.R.

15. Shortly after the call was received by Marshall Police dispatch, D.R. received a tweet from Twitter user @RIURichHomie in which @RIURichHomie stated he was in the process of "swatting" D.R. Based on my training and experience, "swatting" is a term used to describe the act of placing a hoax call to law enforcement in order to cause an emergency law enforcement response, ideally involving a SWAT team, for purposes of harassing the target of the swatting attack.

D. On January 9, 2015, @RIURichHomie called police, posing as D.R., saying he would "shoot up" Marshall High School.

16. On January 9, 2015, a call was received by Marshall Police dispatch from a male caller who claimed to be D.R., in which the caller stated that he was going to "shoot up" Marshall High School in thirty minutes and kill everybody. Shortly after the call was received, Twitter user @RIURichHomie tweeted that D.R. was going to shoot up a school in ten minutes.

E. On January 11, 2015, another bomb – and shooting -- threat was e-mailed to Marshall High School, purportedly sent by D.R.

17. On January 11, 2015, an email message was received by the Superintendent of Marshall, Minnesota Public Schools which had purportedly been sent by D.R. In the message, the sender claimed he/she was D.R. and had planted a bomb at a Marshall school that would

detonate at 10:00 am the following day. The sender also claimed he/she would arrive at a different Marshall school at the same time and shoot students and faculty members.

F. On January 29, 2015, another bomb threat was e-mailed to Marshall high school, purportedly sent by D.R.

18. On January 29, 2015, an email message was received by a Marshall, Minnesota Public Schools employee that purportedly had been sent by D.R. In the message, the sender claimed he/she had placed a bomb in the building and all survivors would be killed by a team who would be coming to the school.

G. The FBI traced usage of anonymously.lulzsec@gmail.com and Twitter account @RIURichHomie to the residence of Zachary Morgenstern.

19. I served a subpoena on Google for subscriber information and IP connection logs associated with e-mail address anonymously.lulzsec@gmail.com – as noted above, this is the e-mail account that sent 222 text messages to the juvenile girlfriend of S.V. Results of this subpoena showed the account was created on September 8, 2011, and IP connection logs were provided for the time period of August 7, 2014 through February 3, 2015. The email account had been accessed multiple times during this time period utilizing IP address 98.194.185.19. In turn, a Whois lookup for IP address 98.194.185.19 showed it resolved to Comcast Communications, Houston, Texas.

20. I served a subpoena on Twitter for subscriber information and IP connection logs associated with Twitter account @RIURichHomie. Review of the provided IP connection logs showed Twitter account @RIURichHomie had been accessed three times utilizing Comcast Communications IP address 98.194.185.19. The logins had occurred during December 2014 and January 2015, the same time period in which IP address 98.194.185.19 had been utilized to access the email account anonymously.lulzsec@gmail.com. All other logins for Twitter account

@RIURichHomie had been conducted utilizing IP addresses that resolved to anonymous proxy servers.

21. To determine who was the user of this IP address (98.194.185.19), I served a subpoena on Comcast Communications for subscriber information associated with this IP address on January 6, 2015 and February 2, 2015, two dates when IP address 98.194.185.19 had been used to access the email account anonymously.lulzsec@gmail.com. According to Comcast Communications, this IP address was accessed on those dates by the account subscribed to P.Z., 9803 Orchid Cove Ct., Cypress, Texas 77433. The Comcast Communications account for P.Z. had been established on June 26, 2013 and was active as of the date the records were provided by Comcast Communications.

22. Pursuant to a search warrant issued in the District of Minnesota, I obtained the email account for anonymously.lulzsec@gmail.com. Among other evidence located in the gmail account, I found records associated with multiple text message “nuke” attacks, or “SMS bombs,” of the type implemented on January 7, 2015, against the cellular telephone of T.P., the juvenile girlfriend of S.V., which, as described above, rendered T.P.’s cellular telephone inoperable due to receiving a series of 222 consecutive text messages over a period of 46 minutes. As noted above, the message in each of those text messages was “@riurichhomie.” In the anonymously.lulzsec@gmail.com account, I found a series of sent SMS messages, dated January 7, 2015, to the telephone number of T.P., with the message “@riurichhomie.”

H. The evidence suggests that Twitter user @RIURichHomie appears to be Zachary Morgernstern, who previously admitted to launching a DDOS attack against his school district.

23. A query utilizing an online commercial public source records database showed 9803 Orchid Cove Ct., Cypress, Texas 77433, is jointly owned by P.Z. and her husband, J.Z. both of whom are in their early sixties.

24. Online commercial public source records database queries for P.Z. and 9803 Orchid Cove Ct., Cypress, Texas 77433, showed a Texas driver's license had been issued on June 14, 2014 to Zachary Lee Morgenstern, 9803 Orchid Cove Ct., Cypress, Texas 77433. Based on my investigation, I have learned that P.Z. and J.Z are Morgenstern's grandparents.

I. Zachary Morgernstern previously admitted to launching a DDoS attack against the website of his school district in Tomball, Texas.

25. Previously, Morgenstern had been interviewed by FBI Houston in February 2012; he admitted to launching an attempted distributed denial of service ("DDoS") attack against the website of his school district in Tomball, Texas. (Based on my training, my experience, and this investigation, I know that a DDoS attack essentially floods a website with faux requests, blocking legitimate requests for information; the effect is analogous to preventing a victim from receiving telephone calls by tying up the phone line with harassing calls.) During the interview, Morgenstern stated he learned about computers and scripting language from a hacker he met while playing the online game World of Warcraft. Notably, Morgenstern stated to the FBI that he had recently been kicked out of his Pinehurst, Texas home by his stepmother, and had moved in with his grandparents in a subdivision of Cypress, Texas.

26. A Google query for Zachary Morgenstern returned a result for a previous Twitter ID of @ZackL337H4X0R. A summary of the account showed it had been established in May 2012. The account profile listed the location as Tomball, Texas, and the profile picture appeared

to be a screenshot of computer code (“script”) related to a DDoS attack on the Tomball School District. A May 25, 2012 tweet from the account was “Well this is gonna be depressing. Without school the FBI can’t come see me. :)” A May 27, 2012 tweet from the account was “As of right now I’m thinking about putting a muratic acid bomb in a school trash can and rolling around in the cafeteria during lunch LOL.”

J. Twitter user @RIURichHomie was identified as “Zack Morge” who lived with his grandparents in Texas.

27. The FBI has attempted to corroborate the identity of Twitter user @RIURichHomie. For example, in January 2015, J.P., a juvenile male from Marshall, Minnesota, was identified by law enforcement as being an online associate of Twitter user @RIURichHomie. J.P. told law enforcement he has communicated online with the person who utilized Twitter account @RIURichHomie for the past several years through Skype and online games such as World of Warcraft. Although he did not know his true identity, J.P. stated he initially knew @RIURichHomie as Zack Morge, who claimed he lived with his grandparents in Texas, but J.P. was later led to believe his name might actually be “Ian.”

28. Similarly, a Google query for Zack Morge returned a result for a historical MySpace account for Zack Morge of Pinehurst, Texas. A review of the MySpace page showed it contained a photo of a young male who was the purported user of the account. A comparison of this photo with the 2014 Texas driver’s license photo of Zachary Morgenstern showed the photos appear to depict the same person.

29. On March 4, 2015, an FBI contractor called the FBI Houston field office and reported his former neighbor, Zach Morgenstern, who resides with his grandparents at 9803 Orchid Cove Ct., Cypress, Texas, had information regarding a recent hack of the Lenovo website.

The contractor reported Morgenstern was willing to provide the information to the FBI, and was available for contact.

30. On March 31, 2015, an FBI Houston SA called Zach Morgenstern to discuss the information related to the Lenovo hack, as well as other information Morgenstern had about people involved in hacking activities. The telephone call was recorded. I reviewed the audio from the telephone call and found that Morgenstern's voice was similar to the voice of a male caller who called Marshall, Minnesota police dispatch on January 26, 2015 and claimed he had called in bomb threats to other states, as well as Marshall High School. The voice of the male caller was also similar to the voice of the caller responsible for "swatting" calls received by law enforcement in Amesbury, Massachusetts on February 10, 2015 and Marshall, Minnesota on February 16, 2015.

K. Morgenstern's gmail account lists a phone number that was used to "swat" a juvenile female in Marshall, Minnesota.

31. Between April 4, 2015 and April 6, 2015, Morgenstern sent three email messages containing information about various people who were involved in hacking, "swatting," and bomb threats to the FBI Houston SA with whom he had spoken with on March 31, 2015. The email messages were sent using email address zach.morgenstern@gmail.com.

32. I served a subpoena on Google for subscriber information and IP connection logs associated with email address zach.morgenstern@gmail.com. According to Google, this email address was created on April 26, 2014 with the subscriber name of Zachary Morgenstern. A review of the provided IP connection logs showed this email account was accessed 19 times between October 15, 2014 and March 22, 2015 from IP address 98.194.185.19 – as discussed

above, this is the same IP address linked to Twitter user @RIURichHomie and anonymously.lulzsec@gmail.com.

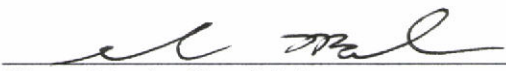
33. Notably, Google records for zach.morgenstern@gmail.com also listed a telephone number that was associated with this account at the time of its creation: (832) 794-0597. On October 7, 2014, a “swatting” call had been received by Marshall, Minnesota police dispatch that was directed at the residence of H.M., a juvenile female from Marshall, Minnesota. After listening to the recorded audio from the “swatting” call, H.M. told law enforcement the voice of the male caller sounded similar to the voice of a person she knew as “Ian” from Texas, who occasionally called her from telephone number (832) 794-0597, the same phone number that was associated with zach.morgenstern@gmail.com.

IV. Conclusion


34. Based on the foregoing facts, I respectfully submit there is probable cause to believe ZACHARY LEE MORGENSTERN transmitted a threatening communication in interstate commerce, in violation of Title 18, United States Code, Sections 844(e), 875(c), and 1038(a). The telephone call placed to Marshall Police dispatch on January 6, 2015 constituted the use of a telephone or other instrument of interstate or foreign commerce in which he willfully made a threat to kill, by means of an explosive, in and affecting interstate or foreign commerce, in violation of Title 18, United States Code, Section 844(e). The email messages sent to Marshall Public Schools employees on January 11, 2015 and January 29, 2015 constituted the use of an instrument of interstate or foreign commerce in which he willfully made a threat to kill, by means of an explosive, in and affecting interstate or foreign commerce, in violation of Title 18, United States Code, Section 844(e). The telephone call placed to Marshall Police dispatch on January 9, 2015 constituted the knowing and willful transmission in interstate commerce of a threatening

communication, in violation of Title 18, United States Code, Section 875(c). The telephone call placed to Marshall Police dispatch on January 8, 2015 constituted conduct engaged in with the intent to convey false and misleading information under circumstances where such information may reasonably have been believed and where such information indicated that an activity had taken, was taking, and would take place that would constitute a violation of chapter 44 of Title 18, United States Code (namely, 18 U.S.C. § 924(c)(1)(A) prohibiting use of a firearm in relation to a crime of violence for which he may be prosecuted in a court of the United States), all in violation of Title 18, United States Code, Sections 1038(a)(1) and 2.

Further your affiant sayeth not.


Glenn Moule, Special Agent
Federal Bureau of Investigation

Sworn and subscribed before me this 11th day of May, 2015.


Honorable Janie S. Mayeron
United States Magistrate Judge