IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	)	
	)	
v.	)	Magistrate No. 12653 M
	)	
ALEXANDER WATERLAND	)	**[UNDER SEAL]**

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, Joseph J. Ondercin, state the following:

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI) and have been so employed since November 2005. I am currently assigned to the Pittsburgh Division of the FBI, Cyber Squad. In this capacity, I am charged with investigating possible violations of federal criminal law. By virtue of my FBI employment, I perform and have performed a variety of investigative tasks, including functioning as a case agent on computer crime cases. I have received extensive training in the conduct of computer crime investigations.

2. I make this Affidavit in support of an application for a criminal complaint. As set forth below there is probable cause to believe that ALEXANDER WATERLAND committed violations of Title 18, United States Code, Sections 875(d) (Internet Threats) and 1030(a)(7)(B) (Computer Fraud and Abuse Act). As detailed below the means used to accomplish this violation involved the use of a computer in transmitting communications in interstate commerce.

3. The facts set forth in this affidavit are based on my personal knowledge, knowledge obtained during my participation in this investigation, knowledge obtained from

other individuals, including other law enforcement personnel, review of documents and computer records related to this investigation, communications with others who have personal knowledge of the events and circumstances described herein, and information gained through my training and experience. Because this affidavit is submitted for the limited purpose of securing a criminal complaint, this affidavit does not set forth each and every fact learned by me during the course of this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that WATERLAND violated Title 18 United States Code, Sections 875(d) and 1030(a)(7)(B).

4. Your affiant is aware that the group known as Anonymous has become a renowned international "hacktivism" organization of loosely connected computer hackers who purportedly commit computer intrusions for the purpose of stealing information or disrupting organizations of activities for which Anonymous does not agree with.

5. On April 26, 2012, a video was posted on YouTube by User ID AnonOperative13. The video, titled "Anonymous Message to The University Of Pittsburgh," and available to anyone on the internet, claimed that Anonymous had hacked into the computer systems of the University of Pittsburgh and had stolen records related to students, faculty, and alumni. In the video, AnonOperative13 demanded that the Chancellor of the University make a public apology for not safeguarding the welfare of the students, under threat that the stolen records would be publicly released. This threat generated substantial media attention.[1]

[1] This YouTube threat was posted by AnonOperative13 just five days after the cessation of a series of over 45 bomb threats to the University of Pittsburgh that caused dozens of mass evacuations and generated significant local and national media attention. Those bomb threats were perpetrated by a group calling themselves the "Threateners," who, like AnonOperative13, attempted to extort the Chancellor of the University to concede to their demands under threats delivered over the internet.

6. These types of record files described by AnonOperative13 would have been stored at the University of Pittsburgh on "protected computers" as defined in Title 18, United States Code, Section 1030(e)(2)(B).

7. In addition, a YouTube search of the User ID AnonOperative13 revealed that AnonOperative13 had posted three other videos of a similar nature to the Anonymous threat he posted against the University of Pittsburgh on April 26. The first was a video titled "Anonymous Message to Alliance Computers," posted on YouTube on February 28, 2012, which claimed that Alliance Computers, a company located in Harrisburg, Pennsylvania, had had its computer systems hacked by Anonymous. The second was a video titled "Anonymous – message to zeptotraining.com," posted on YouTube on April 20, 2012, which claimed that a web site, zeptotraining.com, had been hacked by Anonymous.[2] The third was a video titled "Anonymous Message to Georgia State (college) Senate," posted on April 29, 2012, which claimed that Anonymous had hacked the Georgia College and State University Senate web site.

8. On May 2, 2012, the individual using YouTube user ID AnonOperative13 posted a comment on YouTube about his April 26 video threat to the University of Pittsburgh. In the comment, AnonOperative13 included information about specific University of Pittsburgh employees, including names, email addresses, telephone extensions, and office locations. In the posting, AnonOperative13 stated that "We also would like to state that we are NOT going to release the information unless Pitt admins dot [sic] follow our very simple request! We are giving Pitt until Monday, May 6, 2012 and should remain posted for no less than 15 days." This posting referenced the demand included within the April 26 YouTube video threat to the University of Pittsburgh that the Chancellor of the University make a public apology.

[2] An internet search revealed that Zepto Training is a company which offers Information Technology training and is based in Ghana.

9. On May 14, 2012, an email was sent from the email address AnonOperative@gmail.com to the general email account for the University of Pittsburgh Police. The email stated, "Do what's best, time is of the essence, so you have seven days to have the public apology to the students released... otherwise user names and passwords are next! We are anonymous! We Are Legion! We are your brothers & Sisters! We are the students and faculty of Pitt! We are your worst nightmare! The internet is here! You Will now Expect US!" The email contained additional attachments which were curriculum vitae of specific faculty members at the University of Pittsburgh.

10. Records obtained through the investigation showed that YouTube user ID AnonOperative13, which posted the April 26 and May 2 threats to the University of Pittsburgh, listed a contact email address of AnonOperative@gmail.com.

11. Records obtained through the investigation have shown investigators the Internet Protocol (IP) addresses of the individual who has accessed the email account AnonOperative@gmail.com as well as the related YouTube account of AnonOperative13. Although numerous IP addresses have accessed the related accounts, investigators have determined through records obtained that one of the IP addresses resolved to an address in an apartment complex at 2000 Loveland Madeira Road, Loveland, OH 45140, another has resolved to a MiFi wireless device located in Mason, OH and belonging to a company known as Express Scripts, and a third has resolved to an Amber Luby in Indian Head, Maryland.

12. Further investigation has revealed that ALEXANDER WATERLAND lives in the apartment complex at 2000 Loveland Madeira Road, Loveland, OH 45140, was employed at the Mason, OH facility of Express Scripts as a computer specialist, and is the brother of

Amber Luby who visited Luby in Maryland on the day her IP address accessed the AnonOperative@gmail.com email account.

13. Investigators have determined that the IP address resolving to the apartment complex where WATERLAND resided at 2000 Loveland Madeira Road, Loveland, OH 45140 was associated with an unsecured wireless router.[3] Records obtained from the University of Pittsburgh showed that someone using the IP address associated with the unsecured wireless router located at the apartment complex in Loveland, OH downloaded a significant amount of data from the University of Pittsburgh's Computer Science web pages from April 25, 2012 at 21:54:20 EST until April 26, 2012 at 00:10:39 EST. These pages accessed by the user of the unsecured wireless router contained data about faculty, staff, and courses.

14. On May 23, 2012, the FBI executed a search warrant at the residence of ALEXANDER WATERLAND, 2000 Loveland Madeira Road, Apartment 9, Loveland, OH 45140. The FBI seized computers, smart phones, and electronic storage devices at that location. Additionally, WATERLAND's employer, Express Scripts, provided WATERLAND's work laptop to the FBI on that date.

15. A forensic review of the hard drive of WATERLAND's personal desktop computer revealed that it had been completely wiped of its memory and contained no files or applications on it. On May 23, 2012, WATERLAND indicated to agents of the FBI that this desktop computer was the computer he primarily used for browsing the Internet. WATERLAND indicated on that date that he had been expecting the FBI to come to his workplace at Express Scripts.

[3] An unsecured wireless router is one whose IP address may be utilized without verification, such as a password. Based on my experience, I know that an unsecured router in an apartment building could be accessed by anyone in or around that building within 100 yards or more. I also know that it is a common tactic of those engaged in illegal internet activity to "pirate" others' unsecured wireless connections in order to shield their IP address, and thus their true identity.

16. Forensic reviews of a personal computer that WATERLAND said was his "gaming computer," as well as the work laptop belonging to WATERLAND, as well as his personal smart phone, revealed numerous Internet searches that had been conducted for items and news related to the hacking group Anonymous.

17. The forensic review of WATERLAND's "gaming computer" showed that on March 2, 2012, that computer accessed the web page www.youtube.com/user/AnonOperative13. There were four records within the computer's hard drive which indicated visits to this page. This web page is assigned to the YouTube user AnonOperative13, which contains links to the four YouTube threat videos posted by AnonOperative13 described in preceding paragraphs.

18. The forensic review of WATERLAND's personal smart phone revealed a large number of images of individuals wearing Guy Fawkes masks. Your affiant is aware that these images are known to be frequently used by members of Anonymous in their messages to the public, and several of the images found on WATERLAND's smart phone were the same images used in the YouTube threat videos of AnonOperative13.

19. Also found within WATERLAND's smart phone were Google searches for "Alliance Computers," which had been a YouTube target of AnonOperative13, as well as evidence of visits to the Alliance Computers web site. Additionally, one of the pictures on WATERLAND's personal smart phone was a picture taken of a computer monitor which featured the website address www.zeptotraining.com/adminLogin.php. Investigators went to this web address on the internet and noted that this was the administrator login screen for the site zeptotraining.com, which was also one of the companies noted above as receiving a YouTube threat from AnonOperative13. Also on WATERLAND's personal smart phone was

a web link saved to a web page at oldcapitol.gcsu.edu/senatemembers/indvhistory.aspx?ID=2722. This web page was part of the Georgia College and State University Senate page, specifically containing identifying information for one of its members, Gerald Adkins. The same link was posted by Anonoperative13 on the YouTube page for the video threat against the Georgia College and State University Senate.

20. Forensic analysis also revealed that WATERLAND's smart phone visited multiple voice synthesizing websites. Investigators visited each of these sites and found them to all be websites which allow a user to type text and have the text read in a computerized audio voice. When tested by investigators, one of the voice synthesizing sites accessed by WATERLAND's phone generated a computerized voice which was identical to the one featured in the Anonymous YouTube threat to Alliance Computers.

21. Finally, the SD memory card found within WATERLAND's Express Scripts work smart phone contained a picture which was recovered from deleted files. The picture was of a computer monitor which depicted the desktop area of a computer, displaying several icons. One of the icons displayed a picture of a globe against a black background identical to the opening frame of AnonOperative13's YouTube threat video against the University of Pittsburgh. The icon, which appeared to be a video file, was titled "Anonymous – Message…". Directly next to this icon on the computer screen was an icon for a Word document entitled "pitt." Further analysis revealed that this photograph was taken on April 27, 2012, the day after AnonOperative13's YouTube threat to the University of Pittsburgh, and the type of camera which created the file was a PG06100, the same model as WATERLAND's work smart phone.

22. Based on the above, your affiant believes that probable cause exists to believe that ALEXANDER WATERLAND has committed violations of federal law, specifically Title 18, United States Code, Section 875(d) (Interstate Threats) and Title 18, United States Code, Section 1030(a)(7)(B) (Interstate Extortion Related to a Protected Computer). As such, your affiant requests that an arrest warrant be issued for WATERLAND.

JOSEPH J. ONDERCIN
Special Agent
Federal Bureau of Investigation

Sworn to before me this 19th day of June, 2012.

MAUREEN P. KELLY
United States Magistrate Judge