ORIGINAL

United States District Court

NORTHERN DISTRICT OF GEORGIA

UNITED STATES OF AMERICA

v.

Michael C. Ford

CRIMINAL COMPLAINT
Case Number: 1:15-MJ-386

UNDER SEAL

I, the undersigned complainant being duly sworn, state the following is true and correct to the best of my knowledge and belief. On or about January 2015 through on or about May 2015, the defendant, Michael C. Ford did, :
(a) with the intent to harass and to cause substantial emotional distress to at least one person did use an interactive computer service and a facility of interstate commerce, including e-mail, to engage in a course of conduct that caused substantial emotional distress to at least one person in violation of Title 18, United States Code, Section 2261A(2)(A);

(b) knowingly and with intent to extort an item of value did transmit in interstate and foreign commerce communications containing threats to injure the property or reputation of the addressee in violation of Title 18, United States Code, Section 875(d);

(c) intentionally access a computer without authorization and exceed authorized access, and thereby obtain information from any protected computer, namely a server of Google Inc., and the offense was committed in furtherance of criminal and tortious act in violation of the laws of the United States and any State, in violation of Title 18, United States Code, Section 1030(a)(2), (c)(2)(B);

(d) with intent to extort from any person any thing of value, transmit in interstate and foreign commerce communications containing a threat to impair the confidentiality of information obtained form a protected computer without authorization, in violation of Title 18, United States Code, Section 1030(a)(7)(B);

(e) having devised and intending to devise a scheme and artifice to defraud victims and to obtain money and property, including online account passwords other personally identifiable information, by means of materially false and fraudulent pretenses, representations, and promises, and for the purpose of executing the scheme and artifice to defraud, transmit and cause to be transmitted, by means of wire communication in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds, in violation of Title 18, United States Code, Sections 1343 and 2.

I further state that I am a Special Agent with the Diplomatic Security Service and that this complaint is based on the following facts:

PLEASE SEE ATTACHED AFFIDAVIT

Continued on the attached sheet and made a part hereof. Yes

Signature of Complainant
Eric J. Kasik

Based upon this complaint, this Court finds that there is probable cause to believe that an offense has been committed and that the defendant has committed it. Sworn to before me, and subscribed in my presence

May 15, 2015
Date

at Atlanta, Georgia
City and State

E. CLAYTON SCOFIELD, III
UNITED STATES MAGISTRATE JUDGE
Name and Title of Judicial Officer

Signature of Judicial Officer

AUSA Kamal Ghali / 2015R00429

AFFIDAVIT IN SUPPORT OF OF A CRIMINAL COMPLAINT AND ARREST WARRANT

I, Eric J. Kasik, Special Agent of the Department of State Diplomatic Security Service, being first duly sworn under oath, hereby state that the following is true and correct to the best of my knowledge and belief:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the United States Department of State's Diplomatic Security Service ("DSS") and have been so employed since 2011. I received formal training at the Federal Law Enforcement Training Center in Glynco, Georgia, and the Diplomatic Security Service Training Center in Dunn Loring, Virginia. I am currently assigned to the Diplomatic Security Office of Special Investigations. My current assignment includes investigating administrative and criminal misconduct by employees of the Department of State, including investigating violations of 18 U.S.C. 371, 1028, 1028A, 1029, 1030, 1341, 1343, 1542, 1543, 1546, 1946, and 2261A. Based on my training and experience, I am familiar with the means by which individuals use computers and information networks to commit various crimes.

2. In or about April 2015, as set forth herein, DSS began investigating a target, later determined to be a U.S. Embassy London employee, Michael C. Ford ("FORD"), for engaging in a computer hacking, cyber stalking, and extortion

3. I am submitting this affidavit in support of a criminal complaint and arrest warrant, charging FORD with violations of 18 U.S.C. § 875 (Interstate Threats); 18 U.S.C. § 1030 (Fraud in Connection with Computers); 18 U.S.C. § 1343 (Wire Fraud), and 18 U.S.C. § 2261A (Cyberstalking). This affidavit is being filed based on my personal knowledge, my review of documents and computer records, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause to support this complaint. I have not included each and every fact of the investigation known to me.

COURT'S VENUE

4. Venue is proper in the Northern District of Georgia pursuant to 18 U.S.C. § 3238. As set forth below, FORD began to commit the offenses described below while he was in the United Kingdom, which is outside of the jurisdiction of any particular U.S. district. FORD's last known residence, prior to moving to the United Kingdom in 2005, was in the Northern District of Georgia. On or about May 3, 2015, FORD traveled from the United Kingdom to the Northern District of Georgia, where he is believed to be visiting relatives. We anticipate arresting FORD in the Northern District of Georgia, on or about May 17, 2015, before he boards his scheduled flight to the United Kingdom.

PROBABLE CAUSE

Jane Doe One

5. On or about April 16, 2015, DSS agents received a request for assistance from Federal Bureau of Investigation ("FBI") Special Agent David McClelland from the Louisville, Kentucky, FBI Field Office. I have spoken with SA McClelland, who stated that he was assisting local law enforcement agents from the Henderson Police Department in Henderson, Kentucky, in their investigation into an unknown target who he believed might be using a U.S. State Department IP[1] address to hide his identity. According to SA McClelland, in or about January-February 2015, the target apparently hacked into and stole compromising photographs from online accounts belonging to Jane Doe One, an 18-year-old Kentucky resident. He then sent threatening, extortionate e-mails to her. Jane Doe One's identity is known to the affiant but is being withheld from this affidavit to protect her identity.

6. I have reviewed copies of the e-mail messages that Jane Doe One received from the target. In them, the target admitted that he had obtained

[1] An "Internet Protocol address" (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

sexually explicit photographs of Jane Doe One and sent her sample photographs as proof. He then demanded that Jane Doe One take videos of other "girls" and "sexy girls" who were undressing in changing rooms at pools, gyms, and clothing stores, and then give the videos to him. The target threatened Jane Doe One that, if she did not send him the demanded videos, he would post the sexually explicit photographs of Jane Doe One widely online, along with Jane Doe One's actual name and address, which he listed in the e-mail message. He also threatened to e-mail the photographs to several of Jane Doe One's acquaintances, which he listed by first name and last name and, in one case, included a phone number.

7. For example, on or about January 26, 2015, the target, using the Google e-mail account "David Anderson" "XXXXXX[2]@googlemail.com," (hereinafter the "talent scout" e-mail account), sent a series of e-mail messages to Jane Doe One. The first stated: *"finally, I found you! What do you think? Nice ass!"* He attached a photograph of her of a sexual nature. When Jane Doe One asked the target where he got the photo, the target responded, *"I'm a wizard, I have lots. Did you like it? :)."* He then asked *"can I text the picture to [and inserted a phone number of an acquaintance of Jane Doe One] or maybe email it to [list of first names and last names of several of Jane Doe One's friends]."*

[2] I have redacted the actual name of the e-mail account, which had the words "talent" and "scout" in it and will be referred to herein as "the 'talent scout' e-mail account."

8. Then the target threatened to post on the internet Jane Doe One's name and address, along with the photographs, and listed her current address in the e-mail.

9. Jane Doe One did not know who the target was, how he obtained her photographs, or how he knew her name and address, as well as her friends' first names and last names and phone numbers. She believed that he must have obtained the photographs and information by hacking into her online accounts.

10. When Jane Doe One responded that she was going to go to the police and remarked that the target had hacked her accounts, the target responded, *"I've hacked nothing. You threaten me again and I send it out. Would you like that."*

11. When Jane Doe One again refused and begged the target to leave her alone, the target responded, *"I want you to video girls in the changing room [of her gym]. If you don't, I send your details and pictures to everyone. What do you say? Looks like you've made up your mind. Get ready for my email and post to go out tomorrow morning. Enjoy!"*

12. A few days later, on or about January 28, 2015, the target, using the same "talent scout" e-mail account, wrote: *"I want you to record videos of sexy girls changing. In gyms, clothing stores, pools . . . . You do that, and I disappear."*

13. Jane Doe One continued to plead with the target to leave her alone. The target responded, *"OK, time's up. Everything I have will be posted online and sent to your friends. Pictures, name, phone number, home address…I gave you a chance and you blew it!"*

Jane Doe Two

14. On or about May 6, 2015, FBI Special Agent Amanda Becker, from the Chicago, Illinois, FBI Field Office, informed members of the prosecution team that she was investigating an unknown target who, on or about March 20, 2015, apparently hacked into various online accounts belonging to Jane Doe Two, a 22-year-old Illinois resident. Jane Doe Two's identity is known to the affiant but is being withheld from this affidavit to protect her identity.

15. I have reviewed copies of the e-mail messages that Jane Doe Two received from the target and reviewed the written memorandum of Jane Doe Two's interview with SA Becker.

16. The target initially sent Jane Doe Two an e-mail message to her Google e-mail account, posing as a Google representative and claiming that Jane Doe Two's Google e-mail account was going to be deleted unless she provided her password. Jane Doe Two provided her password, as directed. The target then apparently hacked into Jane Doe Two's Google account, presumably using the stolen password. He then obtained, presumably from Jane Doe Two's

hacked accounts, two or more private photographs of Jane Doe Two of a sexual nature. He also obtained other PII about Jane Doe Two, including her first and last name, her address, where she worked and went to school, and her parent's first and last names and e-mail addresses. The target then sent Jane Doe Two several threatening e-mail messages to her Google e-mail account. He admitted that he had obtained sexual photographs of Jane Doe Two and sent her the photographs as proof. He then demanded that she provide her current home address and her parents' contact information and other PII. He warned her that, if she refused, he would e-mail the photographs of her to a list of others, listing the first and last names of several of her acquaintances. The target also threatened to post her photographs online.

17. For example, on or about March 20, 2015, the target, using the Google e-mail account "Accounts Deletion" "YYYYYYY[3]@gmail.com," sent Jane Doe Two an email message to her Google email account, with the subject line in the header reading: *"Goodbye, Your Email Account is Scheduled to Be Deleted."* The body of the e-mail stated that *"We have received your request to delete your Google account. The request details are as follows: March 20, 2015 2:33 AM PDT <> IP address [Listing numbers]. The deletion process may take up to 96 hours to complete. If*

[3]I have redacted the actual name of the e-mail account, which had the words "deletion" and "confirmation" in it and will be referred hereafter as "the 'deletion confirmation' e-mail account".

this request was made in error, you may cancel the process by responding to this email with your current password in the message body. Your account will remain active once your emailed password has been verified through our automated system. We are sorry to see you go, thank you for using Gmail!" It was signed *"Sincerely, Gmail Account Deletion Team."*

18. After Jane Doe Two provided her password to the target, on or about March 24, 2015, he sent her a series of e-mail messages from the same "david anderson" "talent scout" e-mail account described above. In the first, he stated, *"I might just have to send everyone these"* and then listed her first name, last name, and home address, along with the personal e-mail account addresses of her mother and father. He attached two or more sexually explicit photographs of Jane Doe Two. In subsequent e-mails, the target confirmed that he knew other personal details about Jane Doe Two, including where she worked and went to school.

19. The target further stated: *"Email me back or I send everything I have. The choice is yours. . . . I'll give you til tomorrow to think it over. If I don't hear back from you, I email everything to your parents and friends and post the pictures online."*

20. The target then sent e-mail messages to Jane Doe Two's mother and father, asking them questions about their daughter.

21. Jane Doe Two does not know the target's identity or how he identified her. Jane Doe Two's parents do not know the target or anyone by the name of "David Anderson." Jane Doe Two is the daughter of a well-known executive of a large, multinational company headquartered in Chicago. She shares the same last name as her father.

Linking FORD to the Criminal Activity

22. During the course of this investigation, I have linked this criminal activity to FORD in several ways.

The Suspect E-mail Accounts Belong to FORD

23. I have reviewed subscriber records for the "talent scout" e-mail account that were obtained from Google on or about April 2, 2015, by the Henderson Police Department. According to those records, the account subscriber's name was listed as "david anderson." The account was created on September 21, 2009. The Internet Protocol ("IP") address that the accountholder initially used to create the "talent scout" e-mail account in 2009 is 169.252.4.21. Likewise, in January-February 2015, the accountholder repeatedly logged into the "talent scout" e-mail account from several IP addresses, including 169.252.4.21 and 169.253.194.1. Using an open-source tool called "Domain Tools," and performing a "who is" look up, agents determined that these IP addresses resolve to the U.S. Department of State. The other IP addresses that

logged into the account in January-February 2015 resolve to two Internet Service Providers in the United Kingdom.

24. In an attempt to identify which particular computer was assigned to the State Department IP addresses, I have spoken with DSS computer specialists, as well as State Department security personnel and Information Technology personnel. Those individuals have informed me that, by performing keyword searches using the suspect "talent scout" e-mail account, they identified the specific State Department computer that is located at a workstation cubicle located in the U.S. Embassy in London. Personnel from the U.S. Embassy in London told me that the only person who sits at that workstation cubicle and uses that computer is Michael C. Ford. FORD is a U.S. citizen who has worked as an Embassy employee in London since 2009. They confirmed that FORD has sat at that cubicle and used that computer since well before January 2015, when the target sent the e-mails to Jane Doe One.

Incriminating Records Were Found on FORD's Workstation Computer

25. Embassy personnel have provided me with a copy of the warning "banner" that appears on employees' computer screens each time they log into their workplace computer. It provides the user's consent to allow the government to, at any time, and for any lawful government purpose, monitor, intercept, and search and seize any communications or data transiting or stored

on the "information system," which includes the computer, the network, all computers connected to the network, and all devices and storage media attached to the network or computer. It also states that the user agrees that he has no reasonable expectation of privacy in any communications or data transiting or stored on the information system.

26. On several occasions in April and May 2015, DSS computer specialists obtained a forensic copy of FORD's directory on the Embassy's network. A "directory" is essentially a folder on the network that is assigned to a specific computer user. When a user logs into the network using his username and password, by default, documents saved to the user's Desktop, My Documents folder, and Downloads folder will be saved to the user's directory on the network, as well as to the user's local hard drive located inside his workstation computer. The user can also specifically choose to save files to his directory on the network as well as to his local hard drive. Only the user has access to his network directory. Users cannot see or save files to another user's network directory. A network administrator can easily identify which directory belongs to a user because the folder's name is the same as the user's username. In this case, that name is "FordMC."

27. From these forensic copies, DSS computer specialists have obtained, and provided to me, copies of specific documents or files that were stored on FORD's directory.

28. For example, one document is a spreadsheet that appears to summarize some of FORD's more recent criminal activities. Along the far left hand column of the spreadsheet is a list of account names for approximately 250 e-mail addresses. Many are Google e-mail accounts, which is consistent with the target's Google "phishing" ploy described above. Many of the e-mail address account names appear to be females and have domain names that end in .edu, (e.g., JaneDoe3@rmu.edu, JaneDoe4@mail.bradley.edu, JaneDoe5@bsu.edu, JaneDoe 6@umich.edu). DSS agents have determined that several of the accountholders appear to attend the same college in Indiana, where they belong to the same sorority. One is a 17-year-old. This leads me to believe that FORD may be targeting college-aged women throughout the U.S.

29. In the next column to the immediate right is what appears to be a list of passwords. There are other column headers to the right of the password column that read: "work," "cons," "icloud," "pics," "facebook," "picasa," "instagram," and "twitter," and then under each column header, is a "y" or "n," which I believe refers to "yes" or "no." I recognize "icloud" as a popular online (or "cloud") storage service that Apple operates. Users who have Apple devices

can store photographs and contacts and other content in their iCloud account. I recognize Facebook as a popular online social networking service provider, where users can create accounts and often post and store photographs. I recognize "Picasa" and "Instagram" as popular online photograph sharing service providers. Users of these various photo storage and photo sharing services typically set up accounts with these various providers and then password-protect access to their accounts so that others cannot access them without the account holders' permission.

30. I believe that the account holders listed on the spreadsheet are victims of FORD's criminal activity. This is because, under the column header "work," virtually every e-mail account password listed on the left hand column has a corresponding entry under the "work" column that reads "y," presumably shorthand for "yes." I believe this means that FORD has tested the password and determined that it "works" to let him hack into the victim's e-mail account. I also believe that, once the target has successfully hacked into the victim's e-mail account, the target then tries to hack into the victim's other online photo storage and photo sharing accounts, where he searches for sexually explicit photographs and PII belonging to the victim and the victim's friends. I believe that, once he obtains the sexually explicit photographs, he uses them as leverage to try to force the victims to cede to his various demands.

31. Further linking Ford and the spreadsheet found in his directory to the criminal activity described above, I noticed that the same "deletion confirmation" e-mail address was listed at the very top of the spreadsheet. I recognized the "deletion confirmation" account as the sender of the e-mail messages that Jane Doe Two received from the target, as described above. I did not see either Jane Doe One or Jane Doe Two's e-mail accounts listed on the spreadsheet, which leads me to believe that the spreadsheet represents only a fraction of FORD's victims.

32. Other documents obtained from FORD's directory appear to be drafts of letters, saved as word documents, purporting to be sent from a Google representative. The letters warn about account deletion and ask for account passwords. These are strikingly similar to the "phishing" e-mail message that Jane Doe Two received from the target, using the "deletion confirmation" e-mail account as described above. I believe that FORD drafted these letters and used them as templates. He likely cut and pasted the text from these word documents into the "phishing" e-mail messages that he sent to his potential victims to try to trick them into sending him their account passwords.

Other Corroboration that FORD is Engaged in the Criminal Activity

33. Embassy personnel provided me with documents from FORD's employment file. Those records indicate that FORD began working at the

Embassy in 2009. This start date is consistent with the Google records that show that the "talent scout" Google account was created in September 2009 by a computer that can be traced to FORD's State Department-owned computer at the Embassy.

34. I also obtained from these records FORD's social security number and date of birth. A criminal records check reveals that a Michael C. Ford, with the same social security number, has a criminal arrest for "peeping tom"-like offenses.[4] This activity is consistent with the target's demands to Jane Doe One that she take, and give to him, video footage of "sexy girls" taking their clothes off in changing rooms at gyms, pools, and clothing stores.

35. I have also obtained records from UK law enforcement agents regarding an e-mail stalking and harassment complaint they received in 2013. UK law enforcement traced the e-mail messages back to the residence of "Michael Ford," and their records list an address in South Croydon that I have identified from Embassy records as FORD's current address in South Croydon.

FORD's Vacation Travel to the United States

36. On or about May 6, 2015, DSS agents queried a law enforcement database and became aware that FORD and his wife and son traveled from London to Atlanta, Georgia, on or about May 3, 2015. They are apparently here

[4] The record contained a birth date that was off by one digit. I attribute this to a clerical error.

visiting family. They are scheduled to return to London on May 17, 2015, out of Hartfield Jackson International Airport in the Northern District of Georgia.

RELEVANT FEDERAL OFFENSES

37. Based upon the information above, I submit that there is probable cause to believe that FORD has violated 18 U.S.C. § 875(b) (Interstate Threats); 18 U.S.C. § 1030 (Fraud in Connection with Computers); 18 U.S.C. § 1343 (Wire Fraud), and 18 U.S.C. § 2261A (Cyberstalking).

38. The Complaint, Affidavit, and Arrest Warrant in this case are the result of an investigation into the defendant's extensive criminal behavior, and the investigation is ongoing. The defendant is not yet in custody. Disclosure of the Complaint, Affidavit, and Arrest Warrant would enable the defendant to evade arrest and potentially travel back to the UK, where he currently holds indefinite residency status. The confidentiality of the investigation and the viability of the arrest plan could be compromised by the premature release of the information contained in the Complaint, Affidavit, and Arrest Warrant.

39. In order to preserve the secrecy of the case until the defendant is taken into custody, the government respectfully requests that the Court seal the Complaint, Affidavit, and Warrant. The government further requests that the government be permitted to disclose the Complaint and Arrest Warrant to persons necessary to effectuate the arrest of the defendant.

CONCLUSION

40. Based on my training and experience, and the facts as set forth in this affidavit, I submit that there is probable cause to believe that FORD has sent interstate threats in violation of 18 U.S.C. § 875, and has committed computer fraud and abuse in violation of 18 U.S.C. § 1030, wire fraud in violation of 18 U.S.C. § 1343, and cyberstalking in violation of 18 U.S.C. § 2261A. Accordingly, an arrest warrant is requested.