

**AFFIDAVIT OF SPECIAL AGENT LAURA MACRORIE
IN SUPPORT OF A CRIMINAL COMPLAINT AND ARREST WARRANT**

I, Special Agent Laura Macrorie, being duly sworn, hereby state the following:

1. I am currently employed as a Special Agent with the Federal Bureau of Investigation (“FBI”) and have been so employed since March 2020. I have received twenty-one weeks of formal training in investigative techniques at the FBI Academy in Quantico, Virginia. I also have received training from the FBI Cyber Division in basic networking, mobile communications, analysis of digital records, social media, cloud communications, email tracing, and other cyber investigative skills.

2. As part of my duties, I am authorized to investigate violations of the laws of the United States, including criminal violations relating to computer-system intrusions, internet fraud, and cyberstalking, including but not limited to violations of 18 U.S.C. §§ 2261A(2).

PURPOSE OF AFFIDAVIT

3. I make this affidavit in support of a criminal complaint and arrest warrant charging JAMES FLORENCE JR. (“FLORENCE”) (DOB XX/XX/1987), of Plymouth, Massachusetts, with cyberstalking, in violation of 18 U.S.C. § 2261A(2) (the “Target Offense”).

4. Because this affidavit is being submitted for the limited purpose of securing a criminal complaint, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to secure a criminal complaint. Where statements of others are set forth in this affidavit, they are set forth in substance and in part.

5. The statements contained in this affidavit are based in part on information provided and written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents; information gathered from the service of

subpoenas and other records; independent investigation and analysis by FBI agents/analysts and computer forensic professionals; and my experience, training, and background as a Special Agent with the FBI.

STATEMENT OF PROBABLE CAUSE

A. Harassment of the Victim

6. In late 2017, the Victim, a resident of and university professor in Massachusetts, discovered that a photograph(s) of her and photographs of articles of her underwear had been posted without her knowledge on Craigslist,¹ in a section of the website soliciting casual sexual encounters. The photos of the Victim's underwear appeared to have been taken in the Victim's former residence.²

7. In 2020, the Twitter accounts @multimay1 and @JMultima sent the Victim the same photos of her underwear, claiming to be in possession of them. In addition, a Twitter account with username @[Victim first name]32DD³ was created using a photograph of the Victim and posted photos of the underwear. Those Twitter accounts, @multimay1 and @[Victim first name]32DD, also tagged the Victim's actual Twitter handle in vulgar tweets.

8. At the time, the Victim primarily used Twitter for professional reasons. The Victim did not want her professional connections seeing the obscene tweets in which she was tagged because she felt it would mar her reputation. As a result, she deleted her Twitter account.

¹ Craigslist is a U.S.-based company operating craigslist.org, a classified advertisements website.

² The Victim informed investigators that the photo in question appeared to have been taken in an apartment she and her husband shared between approximately 2015 and 2016.

³ The victim's actual first and last names appear in various email addresses, social media identifiers, as well as communications detailed in this affidavit. The brackets reflect that the victim's name has been redacted in order to protect the privacy of the victim.

9. In February 2023 the Victim discovered images of her had been posted on the website ladies.exposed.⁴ Images included a variety of photo collages that included images that had been edited to make the Victim appear to be nude or semi-nude, a photo of the Victim's driver's license, the Victim's then true phone number, true email addresses, true home address, a photo of the Victim's current residence, and the Victim's professional information. Captions of the uploaded images included "Own & Share [Victim's first, middle, and last name] – Make This Whore Famous", "Humiliate & Share Webslut [Victim first name]", and "Fully Exposed Webslut [Victim first name]. Post & Share Her Everywhere. Make The Whore Famous".

10. As a result of these postings, messages were sent to the Victim via email and text message by unknown individuals. At least two emails included threats to disseminate the Victim's images to coworkers and/or students if she did not comply with the senders' demands, which, for at least one of the senders, included a demand that she produce sexual images.⁵

11. On or around July 20, 2023, the Victim received an email from an email address bearing the Victim's name (a[Victim last name]@proton.me)⁶ with the subject "Read This Professor". The email contained the following message:

⁴ Records from ladies.exposed revealed seven (7) accounts associated with the Victim's harassment uploaded any one of approximately 128 unique images a total of approximately 687 times between February 24, 2023 and May 31, 2024.

⁵ Over the course of the conduct described herein, the Victim has also received harassing and extorting communications that do not appear to originate from FLORENCE (based upon information obtained to date). These communications are believed to be from individuals who have directed communications toward the Victim as a result of FLORENCE's posts encouraging them to do so.

⁶ Proton Mail ("proton.me") is a Swiss-based end-to-end encrypted email service. In my training and experience, this email service is often used by individuals seeking to hide their identity.

If You Ignore This Posting Will Continue

Hello My [University name] Professor. I Am Sure By Now Deleting Your Emails, Changing Your Number, Removing All Your Social Media Accounts And Trying To Take Down Your Information From Websites And Searches Has Been Tiring.

My Point Is If You Would Like To Stop Being Posted I Can Do This For You. You Will Need To Send A Selfie Holding A Paper Sign Including Your Name And Todays Date So I Know This Is The Correct Professor For Us To Speak Further.⁷

12. In May 2023, the Victim's personal information, including personal email addresses, home address, professional contact information, account passwords, and even a list of hair colors the Victim has dyed her hair, was posted anonymously on Doxbin, a text storage site primarily used for the purpose of doxing.⁸

13. Between June 2023 and April 2024, the Victim became aware of five (5) Reddit accounts displaying the Victim's name and images. At least three of the Reddit accounts posted digitally altered images depicting the Victim as nude or semi-nude. Reddit account [Victim last name]-Exposed posted a photo of her driver's license (with information such as her address) and included the message "Accept It Your Exposure Is Permanent Slut" in the biography section of the user profile, which the Victim felt was a message directed at her. This same Reddit account also posted a section titled "Fan Tributes" consisting of eight (8) photos of erect penises in front of a digital image of the Victim. The section ended with the statement "Enjoy Your Exposure You Naughty Bimbo. You Belong To The Internet."

⁷ As more fully outlined below (infra, ¶25), subsequent investigation has revealed probable cause to believe that this particular email was sent to the Victim by FLORENCE.

⁸ Doxing is the act of publicly providing personally identifiable information about an individual or organization, usually via the Internet, without their consent, and with the primary objective to humiliate, bully, harass, extort, or otherwise harm the victim.

14. The Victim's name, image, and personal information was also used to create at least three (3) artificial intelligence-driven chatbots⁹ on two different platforms between approximately September 2023 and July 2024¹⁰. The chatbots were programmed with the Victim's personal and professional information which would then inform the chatbot on how to respond to users during a chat. This information included the Victim's date of birth, home address, employment information, education, hobbies, typical dress, the names and employment of her husband and a close friend, and even the date of her mother's death. For example, based on my review of subscriber information associated with one of the chatbots and my conversation with a chatbot administrator, if another user interacting with the chatbot asked the "Victim" where she lived, the chatbot could provide the Victim's true home address followed by "Why don't you come over?"

15. The Victim's images, including images altered to make the Victim appear nude or semi-nude, were posted to numerous photo-sharing and/or pornography platforms where users could view, download, and/or comment on the images. On one particular website, users posted comments such as "Mmmmm sizzling hot piss and cum target" and "Follow me to the toilets and show me your big tits ! Then get on your knees and suck my cock before I bend you over and fuck you against the toilet door ! As a cheap whore !"

16. The Victim's name, image, and other personal information was posted on at least 13 websites. At least 27 unique accounts were used to harass, impersonate, or otherwise cause the Victim substantial emotional distress. To date, the Victim has received at least 60 distressing

⁹ A chatbot is a software application or web interface that is designed to mimic human - conversation through text or voice interactions.

¹⁰ As detailed below, among the evidence recovered from search warrants in this matter is an invoice from one of these chatbot companies directed to FLORENCE by name.

text messages, emails, or calls from unknown senders addressed to the Victim discussing her image and information posted online through August 2024.¹¹

B. Identification of FLORENCE

17. Records obtained in this investigation revealed that some of the emails used to create the Twitter accounts that were used to harass the Victim in 2020 had overlapping information. In this regard: (1) the @JMultima Twitter account was created on April 22, 2020 using the Google email [Victim first name]s32dd@gmail.com; (2) the @multimay1 Twitter account was created on May 8, 2020 with the Google email [Victim first name]s32ddd@gmail.com; and (3) the @[Victim first name]32DD Twitter account was created on July 7, 2020 with the Google email [Victim first name]sbig32ddtits@gmail.com.

18. Records from Google indicated that the Google emails used to create the @multimay1 and @[Victim first name]32DD Twitter accounts both used the [Victim first name]s32dd@gmail.com account (that had been used to create the @JMultima Twitter account) as a recovery email.¹² Because the same email address was used in connection with each of these three Twitter accounts (either to create, or as a recovery email), I believe that they were created by the same individual who had access to and control over that Google email account.

19. Google records also identified a recovery phone number, XXX-XXX-1059, for the [Victim first name]sbig32ddtits@gmail.com Google account (used to create the @[Victim first name]32DD Twitter account). Records produced by AT&T for phone number XXX-XXX-

¹¹ Even after the Victim changed her phone number, her husband received text messages addressed to or about the Victim.

¹² Google instructs users to “[s]et a recovery email address and phone number so we can reach you in case we detect unusual activity in your Google Account, or you accidentally get locked out.” See <https://myaccount.google.com/intro/recovery/email?hl=en-US> (last visited February 9, 2024).

1059 showed that FLORENCE was the assigned user and the payor for the account from approximately April 28, 2016 until the beginning of 2022.

20. FLORENCE is known to the Victim. FLORENCE met the Victim through a mutual friend, who had gone to high school with FLORENCE and college with the Victim. FLORENCE attended parties at the Victim's residence between approximately 2015 and 2017. The photos purportedly of the Victim's underwear (*see supra*, ¶¶6, 7) appear to have been taken at that same residence, according to the Victim.

21. Investigators have also obtained records of the IP addresses that had been utilized to log into various accounts used to harass the Victim in 2023, such as from the "ladies.exposed" website and from Reddit. *See supra*, ¶¶9, 12. On six occasions (May 23, 2023, June 28, 2023, July 11, 2023, July 12, 2023, July 15, 2023, and July 21, 2023), an Amazon account belonging to FLORENCE had been logged into utilizing an identical IP address that had been used to log onto one of the harassing accounts the very same day.

22. A number of federal search warrants have been obtained for the content of email accounts linked to FLORENCE and/or the harassment of the Victim.

23. One such account was jflorenc05@gmail.com. That account was linked to FLORENCE by, among other things, phone numbers that provider records show were subscribed in FLORENCE's name, FLORENCE's Amazon account, multiple logins using IP addresses assigned to FLORENCE's home by his internet provider, and a software distribution/gaming platform utilized by FLORENCE. The content of the jflorenc05@gmail.com account revealed, as relevant here:

- a. Bookmarked websites ("www.fakenudepictures.com" and "www.nudify-her.com/contact") that advertised photo editing services to create sexually

explicit images. For example, one such site advertised the following, “Want to see your crush completely nude? Our fakers will create your fake nudes request. Send us a photo of the girl you like us to photoshop naked and we will create a high-quality fake nude of her. We can erase clothes from photos or make nude face swaps. Discretion is guaranteed.”

- b. Approximately 30 Google searches between July 2017 and June 2022 associated with the Victim, including the Victim’s name, the Victim’s Twitter account username, the Victim’s MySpace and other online accounts, and various online articles that featured the Victim’s photo.
- c. Google Maps queries for the Victim’s home address on March 4, 2017 and July 16, 2017.¹³

24. Another such email account was oceanica234@gmail.com. This account was tied to FLORENCE through other accounts identified in the investigation. In addition, among other things, the account was logged into using IP addresses assigned to FLORENCE by his internet provider approximately 78 times between January 1, 2023 and July 2, 2024 (and, as detailed below, contained an invoice billing FLORENCE by name). The content of the oceanica234@gmail.com account revealed, as relevant here:

- a. Visits to URLs associated with the Victim’s Facebook, LinkedIn, Instagram, and SlideShare username or accounts, her professional website, the university program at which the Victim worked, the Victim’s biographic page on the university website, and a feature on the Victim in the local business journal.

¹³ The Victim has stated FLORENCE had never been to her home at that address.

- b. Searches related to the Target Offenses, including “alter image with ai”, “fake nude pics”, “fake nudes photoshop”, “deep fake app”, “deepfake software”, “deepswap apps”, “ezgif”, “exposed pic sites”, “exposure sites”, “how to add cleavage in photoshop”, “how to link images in reddit post”, “cumming in stolen panties”, and “cumming in stolen socks.”
- c. The following searches on February 8, 2023: “vpn for ladies.exposed”, “what vpn works for ladies.exposed”, “ladies dot exposed from vpn”, and “ladies exposed from vpn.”¹⁴
- d. An email invoice for the chatbot platform Crushon.ai. This invoice was for a one-year Premium subscription, from December 30, 2023 to December 30, 2024, and was billed to James Florence Jr., at a specific Apartment address in Plainville, MA.¹⁵
- e. An image depicting the Victim with an unknown white male. The image appeared to have been digitally altered to make the Victim appear nude. The Exif data associated with the photo indicated it was associated with Adobe Photoshop software for Windows and created on May 22, 2018, which was the same date the oceanica234@gmail.com account engaged in various searches about creating explicit images, including “fake nudes photoshop”, “fake nudes artist”, “fake the bitch”, and a visit to “fakenudepictures.com.”

¹⁴ This is the same timeframe in which the victim discovered that images of the Victim had been posted to “ladies.exposed.”

¹⁵ The specific address was included in the invoice.

f. Several email exchanges regarding advertisements posted by the Craigslist account associated with oceanica234@gmail.com. Records from Craigslist revealed this account posted approximately 39 advertisements for “panties, bras, and socks” either to purchase or to share in person for the purpose of masturbating together. In an email to an interested party, FLORENCE stated “hello! I have panties, socks, and bras from several girls, as well as plenty of pics of them. they’re all people I know, friends of mine, etc. Looking for someone who would like to get off together using their stolen things.”

25. Records associated with the oceanica234@gmail.com also account showed the account was accessed using an IP address that was also used on the same day to access one of the chatbots created in the Victim’s name and image. The chatbot was associated with the a[Victim last name]@proton.me email address. Specifically, the account that created the chatbot was registered using [Victim last name][Victim first name]@gmail.com. Google records indicated this account listed a[Victim last name]@proton.me as its recovery email. I believe FLORENCE controls the chatbot account and the Proton email account in her name that was responsible for sending the extortionate email to the Victim referenced in paragraph 11.

CONCLUSION

26. Based on all of the foregoing, I submit that there is probable cause to believe that JAMES FLORENCE JR., has engaged in cyberstalking, in violation of Title 18, United States Code, Section 2261A(2).

Sworn to under the pains and penalties of perjury.

/s/ Laura Macrorie

LAURA MACRORIE
Special Agent, Federal Bureau of Investigation

Sworn to via electronic means in accordance with Fed. R. Crim. P. 4.1 on September 9,
2024.



Page Kelley

HON. M. PAGE KELLEY
UNITED STATES MAGISTRATE JUDGE
DISTRICT OF MASSACHUSETTS