

AFFIDAVIT OF SPECIAL AGENT JEFFREY WILLIAMS
IN SUPPORT OF A CRIMINAL COMPLAINT

I, Jeffrey Williams, state:

INTRODUCTION AND AGENT BACKGROUND

1. I have been a Federal Bureau of Investigation (“FBI”) Special Agent since March 2010. I have received FBI training concerning computer-facilitated crime and other criminal activity. Prior to my employment with the FBI, I worked as a senior business systems analyst at a health insurance company and as a business systems analyst at a consulting company. In these two positions, I have gained experience related to information systems. I hold a Bachelor of Science Degree in Information Systems from Drexel University. Additionally, I have a Master of Science Degree in Computer Information Systems concentrating in Security from Boston University.

2. I am currently investigating Ryan Lin, a 24-year-old Massachusetts resident, and potentially other targets, for engaging in a computer hacking and cyberstalking campaign, in violation of 18 U.S.C. §§ 875 (Interstate Threats), 1028A (Aggravated Identity Theft), 1030 (Computer Fraud and Abuse), 1343 (Wire Fraud), 2261A (Cyberstalking), 2252 (Transportation/Receipt/Distribution/Possession of Visual Depictions of Minors Engaging in Sexually Explicit Conduct); and 2252A (Transportation/Receipt/Distribution/Possession of Child Pornography).

PURPOSES OF AFFIDAVIT

3. This affidavit is being submitted in support of a criminal complaint against Ryan Lin charging that, beginning at least in or about April 2016 and continuing until the present, he committed the crime of Cyberstalking, in that he did:

with the intent to . . . harass, intimidate . . . another person . . . use[] . . . any interactive computer service or electronic communication service . . . to engage in a course of conduct that . . . causes, attempts to cause, or would reasonably be expected to cause substantial emotional distress to a person . . . all in violation of 18 U.S.C. §2261A(2)(B).

4. This affidavit also sets forth probable cause in support of applications for search warrants for the following locations:

- A. [REDACTED], Newton, MA (the “Lin Residence”);
- B. [REDACTED] (“the Lin Motor Vehicle”) parked near Lin Residence or in the detached garage with Massachusetts registration [REDACTED].

These locations are referred to collectively as the “Target Locations.” A separate affidavit will incorporate this affidavit by reference and will set forth additional facts in support of searches of these Target Locations.

5. This affidavit does not set forth all the facts developed during the course of this investigation. Rather, it sets forth only those facts that are necessary and sufficient to establish probable cause to believe that the defendant has committed and will continue to commit the above offense, and that evidence, fruits, contraband, and instrumentalities of this and other offenses will be found in the Target Locations.

6. I have participated in this investigation since August 2017. Prior to the commencement of the federal investigation, this matter was investigated by a number of local police departments, most significantly the Waltham Police Department, working with the Middlesex County District Attorney’s Office. I am familiar with this investigation based not only on my own investigation, but also on information I have received from a variety of sources, including oral and written reports made to me by other law enforcement officers (especially the Waltham police), physical surveillance, public records, business records, and documents

obtained pursuant to search warrants for several online accounts.

BACKGROUND

Overview of Cyberstalking Campaign Aimed at Jennifer Smith

7. Beginning in or about April 2016 and continuing to present, one or more targets have engaged in an extensive, multi-faceted campaign of computer hacking, online harassment, and privacy intrusions targeting a 23-year-old former Massachusetts resident¹ named Jennifer Smith² and her family. This pattern of behavior is referred to as “cyberstalking.” Smith has been the victim of a wide variety of cyberstalking activity, and attacks have also been directed at her friends, family, and institutions and individuals associated with her.

8. In my training and experience, and in working with other agents, I have learned that one of the challenges of cyberstalking investigations is that the original perpetrator often posts personally identifiable information (“PII”) about the victim and those connected with her online. This practice is commonly referred to as “doxing.” In this case, almost a year after the cyberstalking campaign began, in March-May 2017, Smith was doxed on several occasions, meaning that someone posted on at least two well known “doxing” websites detailed personal information about her (her name, address, date of birth, phone numbers, online accounts, passwords to her accounts, etc.) and similar information about those associated with her. As a result, while we believe that we have identified Ryan Lin as the original perpetrator of, and

¹ As a result of this cyberstalking campaign, Smith has recently moved out of state.

² All names in this affidavit, other than Lin, have been changed throughout the affidavit to anonymous pseudonyms, chosen from Census Bureau/Social Security common name data, to protect the privacy of the victims and witnesses. The legal names of the individuals referenced in this affidavit are known to me.

primary operative behind, the computer hacking and cyberstalking campaign against Smith, it is possible that one or more of the actions below, particularly conduct that transpired after Smith was doxed in the spring of 2017, may not actually be Lin's direct work. Rather, they may be actions of those working from the information provided on these forums, possibly at Lin's direction. Nevertheless, there is probable cause to believe that it is Lin who began the campaign against Smith and is responsible, either directly or indirectly, for the repeated acts of harassment aimed at her and her associates.

9. As set forth in more detail below, the hacking/cyberstalking campaign against Smith includes the following activity:

- one or more targets created a collage of photographs that include three pictures of Smith's face with an expression that suggests sexual arousal; one picture of a female's naked breasts; one picture of Smith's buttocks in underwear; and one picture of a vagina, spread by fingers. The appearance and suggestion of the collage is that these are all sexually explicit pictures of Smith. This collage was sent, often accompanied by private diary entries of Smith that discuss, among other sensitive issues, her medical, psychological, and sexual history, via email to hundreds of individuals connected to Smith, including her roommates, her co-workers, her 13-year-old sister, her parents, her parents' work colleagues, and her former teachers, school administrators, and staff of institutions connected to Smith;
- one or more targets accessed, without authorization, Smith's online accounts (including her Apple iCloud account) and electronic devices (including her laptop and iPhone) and obtained Smith's private photographs and videos (incorporated in the above collage) and private journal (which she stored on her Google Drive account and which detail her sensitive medical, psychological, and sexual history) and other personally identifiable information;
- one or more targets created and posted online fraudulent profiles of Smith on websites dedicated to prostitution, sexual fetishes, and other sexual encounters. In these profiles, the target, posing as Smith, claimed that Smith was interested in enacting a rape fantasy, wanted to engage in "BDSM," (an acronym for bondage, discipline/domination, and submission/sadism, masochism), and wanted to participate in a "gang bang" (sexual intercourse, often forcible, between one individual and a group of individuals). These profiles, and subsequent messages, directed interested men to Smith's home address, causing at least three men, who Smith did not know, to show up at Smith's home in

search of sexual activity;

- one or more targets pretending to be Smith's roommate and her mother sent online threats to blow up or shoot up local schools and/or their own residences. These hoax threats triggered law enforcement responses, and caused additional harm to individual(s) and institutions who were targets of the hoax threats;
- one or more targets contacted an individual for whom Smith was pet sitting, claimed to be Smith, and stated that "she" had killed the pet. This message triggered a panicked call from the pet owner to the local police, who came to the home and confronted Smith;
- one or more targets sent threatening and harassing communications to Smith, her family members, friends, and associates, encouraging Smith to commit suicide and threatening to rape and/or kill Smith and her friends; and
- one or more targets sent e-mail and text messages containing images that likely constitute child pornography (including images of pre-pubescent females) to Smith's mother, her former roommate, and to two of Lin's former college classmates.

10. The target(s) used a variety of online accounts and a variety of methods to hide their identity/IP addresses, including by accessing the internet using a service that anonymizes IP addresses ("TOR," an acronym for "The Onion Router"), using Virtual Private Network ("VPN") services, using anonymous overseas texting services; and using overseas encrypted email providers that do not respond to law enforcement and/or do not maintain IP logs or other records.

Meeting and Interactions between Jennifer Smith and Ryan Lin as Roommates

11. Ryan Lin became roommates with Smith in approximately late April/early May 2016, after he answered an advertisement on Craigslist advertising a vacant room at a house in Watertown, Massachusetts. At the time Lin moved in, Smith was living in the house with two other individuals. She had an Apple MacBook laptop, which she kept in her bedroom. Her bedroom door did not have a lock. Her laptop was not password protected. On her laptop, Smith also stored a document that contained passwords to all of her online accounts.

12. Lin is a graduate of Rensselaer Polytechnic Institute (“RPI”), where he majored in computer science. He has an extensive professional background in computers and information technology.

13. Lin exhibited strange behavior toward Smith soon after moving into the apartment. The behavior escalated significantly by the end of May 2016, resulting in Smith leaving the house and moving in with her father on or about May 30, 2016. Smith returned the following month to move the remainder of her belongings out of the apartment.

14. A few weeks after Lin moved in, in approximately mid-May 2016, at Lin’s request, Smith sold marijuana to Lin for approximately \$60. That night, he pounded on her bedroom door at 3:00 a.m., then went into her bedroom, where she was sleeping, screaming at her and accusing her of cheating him of the full amount of marijuana. Although she never sold him marijuana again, from that point forward, Lin repeatedly asked Smith if she would sell him drugs, and referred to her as his “drug dealer.”

15. Soon after he moved in, Lin began texting Smith. In his texts, he referenced the fact that she had recently had an abortion—a fact that she kept private and had not shared with him, or with the other roommates, but that she had written about in her private electronic journal that was accessible from her laptop and that she stored on her Google Drive account.

Specifically, Lin sent Smith a text on May 25, 2016 stating: “I understand abortions can be painful and the one you had in March probably has its lingering effects too. I agree Michael should not have treated you that way.” Michael was a former romantic partner of Smith, and she had not discussed him with Lin, but had written about him in her online journal. Smith rebuffed Lin’s text messages, not responding at all or responding with texts including: “You are

the worst. Do not text me unless an emergency.”

16. In late May 2016, Smith noticed that her prescription medications (used to treat her anxiety and depression) were missing. Within days, at a time when only Lin and Smith were home and right after Lin left the bathroom, the toilet in their shared bathroom began to overflow. Smith called the plumber, who retrieved from the toilet one of her missing plastic bottles that had contained her prescriptions. The flood caused significant damage to the apartment. Lin denied involvement. Within days of this encounter, Smith left the house and moved in with her father.

17. When Smith returned to the house approximately a month later to retrieve the rest of her belongings, she discovered that her online journal—which contained detailed and sensitive information regarding her mental health, her abortion, and her sexual encounters—had been printed and strewn around her bedroom. Smith collected the journal and confronted Lin. He denied that he had printed it. Smith later took a hammer and repeatedly hit Lin’s computer monitor.

18. Lin’s behavior in the apartment also caught the attention of the other two roommates, Amanda Johnson and Christopher Williams. At one point in June of 2016, Lin smeared yogurt around the living room and explained to Johnson that he was “redecorating.” Smith and Johnson confronted Lin about his behavior. Lin called Smith a “whore” during this encounter. Lin also repeatedly tampered with, or disposed of, Johnson’s personal belongings, including her household decorations and kitchen utensils. Lin also had a habit of repeatedly disposing of his food and other garbage in various closets. In June 2016, Lin sent Johnson a text message stating that he would not work for her employer (which he identified by name) for the money she earns (quoting her exact earnings), indicating that he may have also accessed

Johnson's computer. Williams stated that Lin informed him that he had installed hidden cameras on the second floor of the apartment. (Consistent with this, I also observed a "to do" list in one of Lin's email accounts which contained an entry to "Setup hidden camera" in May 2016).

19. Johnson and Williams repeatedly complained to Lin and to the landlord about Lin's disruptive behavior and attempted to have Lin removed from the house. In the spring-summer 2016, all three roommates reached out to the local police about Lin, and the police issued Lin several warnings about his harassing behavior. Eventually, on or about August 1, 2016, Lin was forced out of the apartment. On the same date, Johnson successfully obtained a "harassment prevention order" against Lin from the Waltham District Court.

Online Interactions between Jennifer Smith and Ryan Lin After Smith Moved Out

20. On July 28, 2016, after Smith had moved out and just days before Lin was successfully evicted, all or part of Smith's online journal and a collage of photos (including sexually explicit photos of body parts and photos of Smith's face) were distributed by email to Smith, Lin, Johnson, Williams and two other individuals. The email was sent in a manner that made it appear that Smith herself was sending it, but it was not sent by Smith (this is referred to as email "spoofing."). The text of the email contained excerpts from Smith's journal, with attachments of five PDF documents that contained pages from the journal itself. The next day, Lin sent a reply email to Smith and the other individuals, including their former roommates, and commented extensively on Smith's journal, stating in part:

I have read and heard many stories of friends, relatives, and other people going through horrible times in their lives. Out of them all, your life story takes the cake. What you shared is the most eye-opening, horrifying, yet interesting things I have ever read. It is fascinating how someone can be so incredibly depressed, paranoid, and slutty at the same time. . . I am quite sure I will never read such an intense story again that

involves so much sluttiness and crazy thoughts. So thank you for sharing your thoughts. This is a once in a lifetime experience for me.

21. Despite Smith's attempts to cut off contact with Lin after she moved out, Lin repeatedly attempted to contact her online—thwarting her attempts to block his access to her online profiles. For instance, in October 2016, Smith “de-friended” and then blocked Lin on Facebook. As a result, Lin was no longer able to view her account. Smith then changed her Facebook settings so that only those who were friends with those already connected to her on Facebook (“friends of friends”) could request to be her friend. Lin responded by sending “friend” requests to associates of Smith he had no connection to, such as her uncle. When some of Smith's Facebook friends accepted his request, Lin then had the ability to contact Smith by sending her “friend” requests—which he repeatedly did. These attempts to connect on Facebook continued in November 2016 and multiple times in December 2016—with Lin again contacting Smith—seeking to be her “friend” and sending her messages multiple times. These repeated friend requests were from an account known to be used by Lin—he made no attempt to hide his identity in making these requests.

22. At the same time that Lin was doggedly attempting to reconnect with Smith through Facebook, he was sending her negative antagonistic emails. For instance, in October 2016 he emailed her and referenced episodes of depression and sexual encounters referenced in her journal, stating: “It's not normal for people to sniff sprayed vapors out of socks or sob into pillows every day...I think you need to get some help. I bet [three people listed by name], and that old man you fucked all agree.” In December 2016, he emailed her again, asking to buy drugs and referencing the fact she had posted a warning on Craigslist to others that they should not rent to Ryan Lin. Lin responded:

Please stop with your baseless accusations and insults. I have never harassed you or cyber stalked you. I've been very patient with you, and will continue to be patient because I know crazy girls aren't capable of making good decisions. They just jump from one psychotic episode to another. Remember those times back in Watertown when you told us all about your problems? How you tried to kill yourself in college? How you had a medically induced miscarriage at the 7-week mark? How you were diagnosed with multiple mental disorders as a teenager? You obviously have a lot of problems, which is normal for crazy girls. That being said, you are a liar, slut, and a murderer (abortion). The only 'protection' you need is from yourself and your own mind. You are crazy, but that's alright. You're still my dealer, and we don't have to be friends to make business transactions. I'm still happy to buy weed from you like I did back when we were roommates, and I'm sure you could use the extra money too. That's basically the only thing I've contacted you about over the past few months anyway.

23. Despite being repeatedly rebuffed, and despite having had very limited contact with Smith during the time they lived together, Lin's attempts to stay in Smith's life continued through 2017. Just as Lin made repeated attempts to friend Smith on Facebook in the fall of 2016, in February and March of 2017, Lin created four different Instagram social media profiles, and did not try to hide his identity (using his home IP address and/or email addresses connected to him). He then attempted to connect with Smith as a "friend" through each of these accounts.

24. Overall, the pattern of behavior directly attributable to Lin demonstrates that, despite Smith's clear and repeated attempts to cut off contact with Lin, Lin continued to attempt to engage with her on a variety of platforms and with a variety of techniques. While each of these incidents in isolation may appear relatively harmless, the cumulative effect of this behavior is both harassing and indicative of a significant attachment, disproportionate to the amount of time they spent together.

PROBABLE CAUSE TO BELIEVE A CRIME WAS COMMITTED

25. Beginning shortly after Smith met Lin, a campaign of online harassment against

her, her family members, and associates began. As noted in paragraph 9, above, this campaign was significant in its scope and the damaging nature of the activity, and it is ongoing. While the federal investigation began in approximately August 2017, there was a state/local investigation that began in the spring of 2016. Below are illustrative examples of the types of conduct that have been investigated by the local authorities to date, and are now being investigated federally.

Online Journal and Photograph Distribution

26. Beginning in the summer of 2016, deeply personal excerpts from the journal and/or the collage incorporating Smith's face and naked body parts (some of which were obtained from her online accounts) were emailed to hundreds of Smith's contacts. As noted above, Smith maintained her online journal in her Google Drive (i.e., it was a document associated with her Google account). She did not print the journal or save it on her computer. In order to obtain the journal for distribution, the person would have had to access Smith's Google account. In order to obtain the photos/videos of Smith to include in the collage, the individual would have had to access Smith's Apple iCloud account.

27. The first online distribution of Smith's journal that she was aware of was the email to Smith, Lin, and her Watertown roommates in June or July 2016. Additional distribution of the pictures and/or explicit diary entries have continued intermittently since then, to a number of different groups, in what appears to be a deliberate attempt to torment Smith and her family. For instance, materials were distributed to her co-workers and boss, the car dealership where Smith leases her car, and schools she has attended (e.g., her high school). Smith moved to Waltham, Massachusetts after living with Lin, and the journal was then distributed within Waltham (e.g. to some faculty at Bentley University).

28. The materials have generally been distributed by a “spoofed” email account and accompanied by a message that falsely suggests it is Smith, or someone close to her, that is distributing the materials. For instance, on August 17, 2017, a fraudulent email used the name of Smith’s father and was sent to approximately 50 school email addresses—all employees of a school district in the town in New Hampshire where Smith’s father lives. This email included a picture of Smith and her father with another man, the sexually explicit collage described above, and four of Smith’s diary entries describing personal topics (sexual episodes, suicidal thoughts). The subject line was “My daughter Jennifer loves your school.” The text of the email was: “Let me help educate your kids. Please share this gift with your students. I want your little boys and girls to masturbate furiously to my daughter.”

Harassing Messages via Social Media and Text Messages

29. In addition to receiving multiple friend requests from accounts that appeared to be derivations of Lin’s name, Smith received multiple friend requests and messages on Instagram from unknown accounts. A number of these accounts included harassing messages on similar subjects as the online communications Lin sent to her directly. For instance, in December 2016, Smith received the following messages from an Instagram account “jsnmma”:

- “It would be so nice if you could go back in time further and undo your abortion.”
- “You don’t need to I’m sure your pussy is already super stretched out.”
- “I bet that is how big your fetus was before you terminated it.” [This message accompanied a photo of a gingerbread man.]

While the local investigators attempted to obtain records from jsnmma to attribute the messages, they learned that the account and messages—as with many others sent in the case—were created using services that allow the sender/user to remain anonymous.

30. Those close to Smith have also been subject to a campaign of harassment. After she moved out of the Watertown apartment, Smith moved into a house in Waltham, Massachusetts, with new roommates. Both those roommates and her co-workers at the restaurant where she worked as a pastry chef were then subjected to harassment. Even Smith's friends and family living out of state have been targeted with harassing messages. For example:

- An email was sent, purporting to be from Smith, to her Waltham roommate Matthew Brown, with a sexually explicit excerpt from her journal stating: "Hi Matthew—I wanted to share this with you for being such a good roommate. I hope you read it and enjoy it as much as I did. We should have a foursome with Melissa and Jason [the other roommates] when they get back tonight or I could bring my three coworkers from the restaurant and we can have an orgy at the dollhouse!"
- Smith's roommate in Waltham, Melissa Thomas, received text messages on April 14, 2017, stating: "You do not understand, Melissa. Jennifer is a demon. She appears human on the outside and her flesh is human. But she is a demon on the inside. She needs to be exorcised and her soul purged of the evil inside. I want you to wait for when she comes back home tonight. Tonight when the demon sleeps I want you to take a knife and stab her to death. Melissa do you understand?"
- In August 2017, Smith's best friend who lives in New Jersey, Ashley, received a series of anonymous threatening text messages, including: "HAVE U EVER BEEN RAPED BEFORE? Do you want to be raped???"
- In September 2017, Smith's former boss received an anonymous text with a photograph of her and her 11-month-old nephew (apparently obtained from her social media account) stating: "Look at this cute little boy. Imagine his nice tight baby ass. How would u like it if I raped him while holding a gun to ur head? Hes so adorable just waiting to be fucked. U gonna let that little boy eat you out? May b put some pastries inside yorself to help him. Wow just look at him. He wants u to suck him off. Its ok don't mind the age dif."

Hoax Bomb Threats

31. Further, there have been a series of false police reports that have caused

significant impact to Smith and those close to her. For instance, on July 24, 2017, the Waltham police department received an anonymous tip that there was a bomb at Smith's Waltham residence. This tip invoked a police response, and the officers determined that the call was a hoax. Later that day, the Waltham police department received another anonymous tip about "drug activity" at Smith's residence. Two days later, Waltham Police received another anonymous tip of a bomb in the town—this too was determined to be a hoax. This was the same day—July 26, 2017—as the Rover hoax described below that lead the Weston police to respond to the home where Smith was pet sitting.

32. In addition, some recent threats in the greater Boston area have been attributed—falsely—to those close to Smith. On July 31, 2017, a threat to "shoot up" the Waltham public schools was made to both an anonymous tip line to the police and via an anonymous email sent to school department employees. The threat was made to appear as if it was being made on a Facebook page in the name of "Matthew Brown"—one of Smith's roommates in Waltham. Less than a week later, on August 4, 2017, the Chelmsford Police Department received a similar school shooting threat, which was made to appear as if it was coming from the Facebook page of Smith's former boss. As a result, the Chelmsford Police Department put the school into lockdown, before concluding that the threat was a hoax. The former boss is the same woman who received the graphic text messages described above about her 11-month-old nephew in September 2017.

33. From July-October 2017, hoax bomb threats were repeatedly made against public and private schools, as well as daycare centers, in Waltham, beginning on or about July 13, 2017 (when several separate hoax bomb threats were made involving Waltham High School, for

example). During the same time period, hoax bomb threats have been made to a number of other locations in Waltham, including the private residence where Smith lived until recently.

Unsolicited Distribution of Child Pornography

34. In July-September 2017 the target(s) has repeatedly sent, via e-mail and text messages, unsolicited images of child pornography to Smith's mother and Smith's former roommate. These are discussed in more detail in the affidavit that is being submitted in support of search warrants to search Lin's residence and motor vehicle.

35. The pattern of incidents outlined above, along with the many other incidents of a similar nature under investigation, evidence a campaign of cyberstalking that began in approximately May 2016 and continues to present. While Smith has been the primary victim, the incidents have also targeted those close to her, and even those tangentially related to her. As a result, both she and others have been exposed to a course of conduct that was intended to—and did—cause substantial emotional distress. Furthermore, as described above, this harassment was carried out through the use of a variety of types of interactive computer services. As a result, I have probable cause to believe that Lin engaged in federal cyberstalking as described in paragraph 3 above.

**PROBABLE CAUSE TO BELIVE THAT LIN COMMITTED
THE CHARGED OFFENSES**

Evidence Found on Lin's Former Workplace Computer

36. From January 2017 through on or about July 24, 2017, Lin worked at a software company based in Waltham, Massachusetts. On or about August 29, 2017, FBI agents interviewed company representatives who explained that Lin had been terminated in late July

2017. On the day he was terminated, Lin asked to be given access to his workplace computer, explaining that he needed to log-out of personal accounts from that computer. The company declined Lin's request. After Lin was terminated, the company set the computer aside and re-installed the Windows operating system, with the intention of later re-assigning the computer to another employee. When the FBI arrived, the company voluntarily provided us with the computer.

37. FBI examiners have performed a preliminary examination of the forensic image of Lin's former workplace computer. Although the operating system was reinstalled, which did result in data deletion, we have been able to find various artifacts in the unallocated space on the hard drive. Specifically, in that unallocated space, FBI agents found evidence of the following:

- Dozens of Google Chrome web browsing artifacts referenced bomb threats in and around Waltham. These included artifacts such as "Bomb threat sent to four Waltham schools" and "Waltham, Belmont Schools evacuated after bomb threats." One artifact indicated that the user viewed a Waltham news piece from on or about July 13, 2017, regarding bomb threats in Waltham schools.
- Artifacts that indicated that the user name "RLin" had a Google Chrome browsing artifact showing the web-site "http://textnow.com" as being most visited. TextNow is an anonymous texting service that was used extensively in the cyberstalking campaign against Smith and her associates.
- Artifacts indicated that PureVPN, a VPN service that was used repeatedly in the cyberstalking scheme, was installed on the computer.
- Google Chrome browsing artifacts showing an account in Lin's name with Protonmail, an overseas encrypted email provider that was used repeatedly in the cyberstalking scheme.
- Artifacts indicated that the user visited the Rover.com website and the FetLife.com website, both of which were used in the cyberstalking campaign against Smith.
- Profile information for the music site Spotify, specifically for Spotify profiles for "Jennifer Smith," "Joseph Smith" (Jennifer's brother), and "Ashley Jones" (Smith's best friend who has also been targeted in the cyberstalking campaign).

- Artifacts indicated that the user repeatedly accessed Lin's personal email account, rlincc@gmail.com.

Timing and Knowledge

38. As described above, the online harassment campaign against Smith began shortly after meeting Lin. During Smith and Lin's in-person encounters and in the online communications directly attributable to Lin (i.e. made using accounts that were indisputably his, such as his Google account), the subject matter of the communications was similar to those sent by the anonymous accounts.

39. Further, Lin demonstrated knowledge of matters in his communications with Smith that suggested he was the one to have accessed her online accounts. Most significantly, as described above, in May 2016, Lin sent Smith a text message referencing her recent abortion—a closely guarded secret she had not shared with him or her other roommates but which she had written about in the online journal that was later distributed through anonymous accounts.

Opportunity

40. Smith kept her laptop, with no password protection, in her unlocked bedroom next to Lin's. Her laptop contained her online journal and photographs, as well as her contact list. Lin not only had physical access to Smith's laptop but he had the technical expertise to exploit that access and to hide his tracks while doing so.

Use of Anonymizing Services Generally

41. The cyberstalking campaign against Smith and those connected to her has continued for months, despite significant efforts by local law enforcement, because the perpetrator of the harassment has used technology to conceal his identity. For instance, the emails are being sent using overseas encrypted e-mail providers, services that assign temporary

IP addresses, servers that anonymize the IP addresses, and/or using false identities. The social media accounts are being created in false names, using email accounts set up for that purpose, created using services that mask the true IP address of the user. Anonymous messages are being sent from temporary phone numbers assigned by overseas services. The e-mail, texting and other accounts are being accessed by someone using VPNs, TOR, and proxy computers to hide their true IP address.

42. As discussed below, law enforcement continues to work to investigate and analyze the messages and the services used to send them, and has already identified connections with Lin. But even beyond those specific connections, the use of these services contributes to probable cause in several ways. First, there is direct evidence that Lin used these services. For instance, agents obtained records from Google for Lin's Google account, rlincc@google.com. In that account, on July 23, 2017, Lin sent himself an email with two screenshots of what appears to be his iPhone. The images show what applications ("apps") are installed, and they appear to include several apps that allow for anonymous texting, encrypted e-mail, and provide free "burner" (anonymously assigned temporary) telephone numbers. The screen shot also shows an app for "ProtonMail," a Swiss-based encrypted e-mail provider that the target(s) used extensively in the cyberstalking campaign described above. Second, Lin has openly discussed on his Twitter account the use of such anonymizing services. For example, on June 15, 2017, Lin, using the Twitter handle @ryanlindev, re-tweeted a tweet from "IPVanish," that read: "Your privacy is our priority. That's why we have a strict zero log policy." Lin criticized the tweet, saying, "There is no such thing as VPN that doesn't keep logs. If they can limit your connections or track bandwidth usage, they keep logs." Third, Lin's computer science degree

and work history (e.g. as a writer of code at a local software company) evidence his ability to successfully employ technology to carry on a carefully constructed cyber harassment campaign while avoiding detection for over a year.

43. Further, the advice Lin provides through Twitter is not only advice that he follows online in accounts attributable to him, but it also describes techniques used in making the anonymous threats. For instance, in the Twitter comment quoted above, Lin explains that VPN services track activity by keeping logs—which can be a way to trace online activity back to a user. In a number of the instances of online harassment under investigation, the user both used a VPN and used an anonymizing service to mask his true IP address. Taking this two-step approach provides the user with another layer of anonymity, and demonstrates an awareness of and concern about the exact issue that Lin highlights in his tweet—the fact that VPN’s track activity with logs.

The Rover Hoaxes—Specific Use of Anonymizing Services and a Key Connection

44. Two instances of hoaxes involving Rover, an online app, provide both an example of the type of harassment directed at Smith and a critical evidentiary link to Lin. Rover is an online service that connects pet owners with individuals willing to provide pet care, including dog walking, house sitting, dog boarding, and “drop-in visits.” The company allows potential sitters to sign up (either through their Facebook accounts or with email), and create a profile, providing a name, a description of their experience, and a photograph. Rover reviews the profiles of the applicant and, if approved, includes the profile on its platform. Pet owners can access the platform, search the profiles for a match for the services they need, and contact the sitters through the platform. Once a service is booked, the pet owner and pet sitter can continue

to communicate with each other through the Rover platform, arranging the details of the service, sending photos and messages (e.g. a picture of the dog at park), and showing information about the service (e.g. map of the location/distance walked, number of water breaks, etc.). In addition, Rover users can make and receive payments through the platform, by linking their financial accounts to the system. Rover can be accessed through the internet, at www.rover.com, or via an application (“app”) available at the Apple App Store or on Google Play.

45. In approximately February 2016, Smith registered with Rover to provide pet sitting services (boarding, sitting (in owner’s home), walking, drop-in visits and daycare). Smith provided these services during the brief time that she and Lin were roommates and it was a source of tension between the two—Lin left a door open allowing a dog to escape and Smith confronted him in anger over the incident.

46. After Smith moved out, and changed her phone number, Lin made repeated attempts to establish a connection with her again including, as described above, via Facebook and Instagram. Similarly, Smith received contacts on Rover from users pretending to be dog-owners seeking her services. Smith has reported suspecting that these were fraudulent accounts, and she did not respond.

47. Based on records received from Rover, I have verified that “rlincc@gmail.com”—an email account directly attributable to Lin—sent three messages to Smith on December 17 and 18, 2016, asking Smith to take care of a dog. (Lin does not have a dog.) Based on records received from Google, I have verified that on December 16, 2016, a Rover profile was created using the “rlincc@gmail.com” email address, and that the pet owner profile claimed his/her name was “Ashley.” Smith’s best friend is named Ashley (as noted

above, she has received anonymous rape threats).

48. On April 17, 2017, Smith received an inquiry from a Rover user named “Ashley Plano.” The profile included the photograph of a young woman. This time, Smith did not realize the account was fake. “Ashley” asked Smith if she was able to walk her two Yorkshire Terriers. Smith and “Ashley” exchanged messages using the Rover application on April 17 and 18, and “Ashley” asked Smith to call her at 781-667-3472. Smith called on April 18, 2017, and “Ashley” did not answer. A few hours later, “Ashley” sent a message on the Rover app saying that she no longer needed dog walking services. However, by calling the number provided by “Ashley,” Smith had revealed her new phone number to “Ashley.”

49. Two days later, on April 20, 2017, Smith began receiving harassing text messages on her new phone, the one she had used to call “Ashley,” from a phone number associated with “TextNow,” an anonymous texting service. Smith received 29 texts that day from TextNow numbers. The texts included: “IT WANTED TO LIVE AND YOU KILLED IT,” “THE ONLY QUESTION I HAE IS **** why????,” “OMG THAT POOR FETUS,” “sum 1 needs 2 take duct tape n seal ur cervix,” and “there was blood everywhere yes?”

50. According to records obtained from Rover, on April 20, 2017, “Ashley Plano” contacted Rover stating “I would like to delete my account permanently. If that is not possible, please deactivate it permanently.” Rover Support responded stating that they had deactivated the account. It had been created only three days before—on April 17, 2017. The communications with Smith were the only activity in the account.

51. Law enforcement has been able to connect this “Ashley Plano” Rover account to Ryan Lin in the following manner:

- The Ashley Plano account was created using the email address teleportxf@gmail.com.
- On April 14, 2017, at 14:55:52, the email address “rlincc@gmail.com” was accessed from IP address 199.38.233.169, an IP address owned by WANSecurity, a Kansas VPN service. As discussed above, this Gmail address is directly attributable to Ryan Lin and was used to communicate directly and openly with Smith and her roommates, including when he first responded to the Craigslist advertisement to be their roommate.
- On April 14, 2017, at 15:06:27, the email address teleportxf@gmail.com, provided by “Ashley Plano” to Rover, was accessed from the same exact WANSecurity IP address, 199.38.233.169.
- On April 17, 2017, “Ashley Plano” accessed “her” Rover account at 21:54:25 from IP address 172.111.213.156, an IP address owned by Secure Internet LLC, a VPN. Shortly after, at 23:19:12, the same Secure Internet LLC IP address was used to connect to rlincc@gmail.com.
- Again on April 18, at 23:48:28 and April 19, at 00:30:11, the rlincc@gmail.com account and the Ashley Plano Rover account were accessed in succession from IP address 172.111.213.36, another Secure Internet LLC address.
- Finally, on April 24, 2017, the same Secure Internet LLC IP address was used to connect in succession to the rlincc@gmail.com account and then the teleportfx@gmail.com account.

52. The above sequence demonstrates that the same individual was accessing Ryan Lin’s known Gmail account and the Rover and associated teleportfx Gmail account used to contact Smith as “Ashley Plano.” Further, records from PureVPN show that the same email accounts—Lin’s gmail account and the teleportfx gmail account—were accessed from the same WANSecurity IP address. Significantly, PureVPN was able to determine that their service was accessed by the same customer from two originating IP addresses: the RCN IP address from the home Lin was living in at the time, and the software company where Lin was employed at the time.

53. In addition to the April 2017 activity, which appears designed to obtain a working number for Smith, another significant cyber-harassment incident involving the Rover platform occurred in July 2017.

54. Specifically, on July 26, 2017, while Smith was pet sitting for a dog and a cat in a Boston suburb, her Rover account was accessed without her authorization. The password was changed, the profile photograph was changed to a suggestive photograph from the sexually explicit collage, and a message was sent to the owners of the pets, Wink (a cat) and Luna (a dog), Smith was watching stating: “Hey I’m so sorry to tell you this but Wink is dead. I had a panic attack suddenly and smothered Wink to death. I’ll pack her remains into a ziploc bag and you can come pick her up. Sorry!” The pet owners tried frantically to contact Smith, and when they were unable to do so they called the local police, who came to the home and determined that the incident was a hoax.

55. In addition to the hoax, the person that accessed Smith’s account on July 26, 2017 used it to: 1.) send pornographic images to approximately 10 other pet owners; 2.) send an excerpt of Smith’s journal to another pet owner Smith had worked for multiple times; and 3.) create charges to the Bank of America account Smith had linked to her Rover profile (for \$752.86 and \$35).

Use of Overlapping Service Providers

56. In addition to the direct attribution, the Rover activity demonstrates that Lin uses the same services as the perpetrator of the harassment. As described above, WAN Security was used by Lin to access his Gmail account, and it was used in the Ashley Plano hoax. And in February 2017, Lin used WAN Security to register his Instagram account, rlyn15. On February

8, 2017, he used it to send an email from ryan@ryanlin.com to a local police department to ask for copies of police reports that reference him.

57. Further, the number used by “Ashley Plano” (the false Rover profile created by Lin in April 2017) is a TextNow number, a Canadian anonymous texting service. Similarly TextNow features very predominantly in other aspects of the cyberstalking campaign against Smith. Numbers that track back to TextNow were used, for example, to send harassing text messages to Smith’s co-workers, her family members, her roommates, and friends, including messages threatening to rape and kill Smith and encouraging her to commit suicide. The search of Lin’s workplace computer showed evidence of a TextNow account.

58. PureVPN also features prominently in the cyberstalking campaign, and the search of Lin’s workplace computer showed access of PureVPN.

59. In addition, the search warrant results of Lin’s email show that on December 18, 2016, Ryan Lin received an email from Rover, welcoming him to his new account. Lin used the username name “Ashley” to open that account. The search of Lin’s workplace computer also revealed that he accessed Rover.com from work.

Lin’s History of Similarly Disturbing Conduct with Other Roommates and Classmates

60. The investigation has revealed that Lin had previously engaged in a similar course of conduct with other acquaintances, including high school classmates, college classmates and roommates, and his roommate immediately prior to moving in with Smith.

61. Specifically, in August 2017, Waltham Police Department detectives identified and interviewed several former high school classmates of Lin’s. These individuals recounted that they went to high school with Lin in Connecticut, that he had created fake Facebook profiles

in other students' names, pretended to be other students, and seemed to know private details about classmates that he should not know. A male classmate recalled that Lin sexually harassed some of their female classmates, would describe in detail various sexual acts he wanted to do, and was otherwise inappropriate. The classmate also stated that Lin created a fake Facebook profile in the classmate's name and used it to impersonate him on Facebook and communicate with his friends. When he confronted Lin, Lin admitted to having created the fake profile. Lin also bragged about hacking into the school's computer system. A female classmate stated that Lin wrote, and hand-delivered, harassing poems about her and other classmates. She stated that, even after graduation, Lin repeatedly attempted to "friend" her numerous times on social media, using various fake profiles, and harassed her repeatedly about avoiding his "friend" requests. Another female classmate stated that Lin wrote and gave her harassing poems about herself. She recalled that Lin acquired photographs of her that he would show to others. She stated that Lin created a fake Facebook profile, pretending to be another male classmate, and used that account to try to friend her friends and her. All three described Lin as a computer "genius."

62. In addition, in mid-September 2017, David Miller and Sarah Jones, who have no connection to Smith, met with the FBI in Albany, New York, and independently reported their concerns about their former classmate at RPI, Ryan Lin.

63. Miller and Jones explained that they, along with two other RPI students, had been repeatedly harassed by Lin in college. According to Miller and Jones, in July 2015, they reported Lin's conduct to the RPI dean of students and both ultimately obtained "Cease and Desist" orders against Lin. In describing some of Lin's conduct, Miller stated that Lin repeatedly created phony social media accounts in Miller's name and posed as Miller in

communicating with others.

64. According to Jones, in August-September 2017, she received anonymous and threatening text messages from numbers including 410-100-02 (which I recognize as a similar format to the numbers used to text Smith). During the same time frame, Jones received similar messages from guerillamail e-mail accounts, which was the same email provider used in the cyberstalking campaign involving Smith. The sender repeatedly threatened to rape Jones, stating “I am going to rape u,” “God u are so hot I would definitely love to rape u,” “Wear something nice when u go to sleep tonight plz,.” In the communications, the sender included many details about Jones, including her name, that she went to “Rensselaer,” and was a coder. They included photographs of Jones, apparently taken from her social media profiles. Jones stated that, given her history with Lin from college, she believed that Lin was responsible for sending these more recent communications.

65. According to Miller, in or about September 2016, over the course of a few weeks, Lin (as himself) contacted Miller out of the blue over Facebook Messenger. Lin sent Miller a file that appeared to be an image of an excerpt of an affidavit. Lin then told Miller that he had accidentally sent him the image. Miller saved a copy of that image and provided it to agents. The title is “Affidavit.pdf (page 3 of 5).” I have reviewed the image and confirmed that it is part of the three-page affidavit that Amanda Johnson submitted to the Waltham District Court in August 2016 in support of her protection order against Lin.

66. Lin also sent Miller a video file that depicted Lin, walking around a house, showing a flooded bathroom and impacted kitchen ceiling, as described in the affidavit excerpt. Lin also sent Miller several text files that appeared to be extremely personal diary entries by

“Jennifer.” Miller did not save copies of these communications. Miller stated that, in Lin’s messages to him, Lin appeared to be laughing about the harassment and made comments such as “LOL” (short for “laugh out loud”).

67. Finally, Lin’s roommate immediately prior to his moving in with Smith also had disturbing interactions with Lin. On April 25, 2016, this roommate sent Lin an email titled “Farewell,” stating, “I know you probably hate me for contacting your family . . . The worst choice is to lie and cover up . . . I trusted you, and I’m not violent. Well, until a point I had to protect myself against you . . . don’t push yourself to the point where other people has [sic] to revenge back to you for what you do . . . Why don’t treat people better . . . You are smart indeed when doing lots of tricks . . . like making excuses, harassment, setup misleading information to confuse people . . . You tuned [sic] my place into hell . . . you are living a life afraid of being accused or revenged, and you had to do things so carefully without being caught . . . you start denying everything. You showed me a violent and non-stable side of you . . . I need to protect myself from all of the mess. You left people with no choice: if law does not stop you, what else can? . . .”

68. The course of conduct described by these individuals from Lin’s life—who have no known connection to Smith—contain numerous similarities to the conduct Lin has engaged in towards Smith.

CONCLUSION

69. Based on the information described above, I have probable cause to believe that Ryan Lin has committed the crime of cyberstalking.

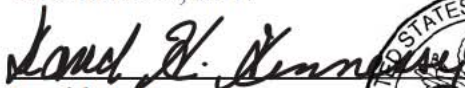
Sworn to under the pains and penalties of perjury.

Respectfully submitted,


JEFFREY WILLIAMS

Special Agent
Federal Bureau of Investigations

Subscribed and sworn to before me
on October 3, 2017


David H. Hennessy
Chief United States Magistrate Judge

