UNITED STATES DISTRICT COURT

for the

Southern District of California

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

One Samsung Hard Drive related to Donald Seoane located at FBI Headquarters, 10385 Vista Sorrento Parkway, San Diego, CA

Case No. '25 MJ142

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Southern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC Secs. 1591, 1594, 1956	Sex Trafficking, Conspiracy and Money Laundering

The application is based on these facts:

See Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Lana Sabata, Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 01/15/2025

Judge's signature

City and state: San Diego, CA

Mitchell D. Dembin, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT

Lana Sabata, being duly sworn, states:

1. I am a special agent with the Federal Bureau of Investigation (FBI) and have been so employed since May 2008. During my career at the FBI, I have focused on investigations involving child exploitation, and human and sex trafficking violations. Prior to my employment with the FBI, I was a local law enforcement officer for approximately seven years. I also served in the United States Armed Forces, Air National Guard, Security Forces. This training and experience, as well as information obtained from other agents and witnesses, forms the basis for opinions I express below.

2. The facts set forth in this affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other FBI special agents and other law enforcement officers with decades of experience; my review of documents and computer records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of this application for search warrants, it does not set forth each and every fact that I or others have learned during the course of this investigation. The dates, times, and amounts discussed herein are approximate.

Purpose of Affidavit

3. This affidavit is made in support of an application for a warrant to search the following items located on one Samsung hard drive containing forensic images[1] of two Devices, which belonged to Donald Seoane, aka "Donny Long":

[1] A forensic image is an exact physical copy of the hard drive, cell phone or other electronic storage media.

A) a forensic image of one ASUS computer tower with connected media devices (hereinafter identified as **DEVICE 1)**; and

B) a forensic image of one white Samsung Galaxy S20 in a Red and Black case, IMEI 354268111077421 (hereinafter identified as **DEVICE 2).**

4. These devices are currently in the possession of the FBI at its headquarters in San Diego, as more particularly described in Attachment A, to seize evidence concerning Michael James PRATT (PRATT) and his co-conspirators for violations of 18 U.S.C. § 1591(d) (Obstruction of Sex Trafficking Enforcement), 18 U.S.C. § 1591(a) and (b)(1) (Sex Trafficking by Force, Fraud and Coercion), 18 U.S.C. § 1594(c) (Conspiracy to Commit Sex Trafficking by Force, Fraud and Coercion), and 18 U.S.C. § 1956 (Money Laundering), more specifically described in Attachment B.

Statement of Probable Cause

Overview of the Conspiracy

5. Michael James PRATT was the mastermind behind the GirlsDoPorn (GDP) and, to a lesser extent, GirlsDoToys (GDT) websites that featured young women appearing in their first pornographic videos. To recruit young women who had never appeared in a pornographic video before, PRATT and others working at his direction used force, fraud, and coercion, to convince/coerce the young women to appear in the videos, including repeated false assurances that the videos would never be posted on the internet. Instead, soon after the videos were filmed, the videos were posted online at PRATT's direction, including on heavily trafficked adult sites, like PornHub. Numerous victims reported that their lives were destroyed as a result. Several of them considered or even tried to commit suicide. Many lost employment, and had to drop out of school; many were disowned by their friends and families; and many suffered extensive harassment from known and unknown individuals who had seen their videos online. Victims pleaded with PRATT and his co-conspirators to

remove the videos from the internet, but the videos often remained online.

6. The websites generated considerable revenue for PRATT. According to financial records, the total revenue generated by the websites is estimated to be at least $17 million U.S. dollars.

7. PRATT was the leader of this criminal scheme, which ran from at least as early as 2012 to October 2019, when law enforcement agents executed a search warrant at PRATT's GDP/GDT business office, which shut the business down.

8. In 2016, multiple women who acted as models for GDP and/or GDT filed a civil lawsuit in San Diego Superior Court against PRATT, Matthew Wolfe, Andre Garcia, and others alleging that they and others tricked them into appearing in pornographic videos posted to GDP and GDT.

9. Trial in the civil case against PRATT and others started in August 2019. Travel records indicate PRATT fled first to Mexico in June 2019 and then continued his flight from there. By September 2019, PRATT had liquidated his assets in the United States and declared bankruptcy. PRATT placed a large amount of money in cryptocurrency.

10. On October 9, 2019, the FBI executed a search warrant at the GDP/GDT business in downtown San Diego, and arrested co-defendants Wolfe, Garcia, Valorie Moser and Theodore Gyi around that same time.

11. On November 7, 2019, the Government filed an indictment against PRATT, Wolfe, Garcia, Gyi, and Moser on charges of sex trafficking five adult women, and PRATT on charges of sex trafficking a minor and production of child pornography. *See* 19CR4488-JLS.

12. On January 2, 2020, San Diego Superior Court Judge Kevin Enright issued a decision, awarding the Plaintiffs over $12 million in damages against Defendants, including PRATT.

13. On February 10, 2022, a federal grand jury returned a 19-

count superseding indictment charging PRATT with one count of conspiracy to commit sex trafficking by force, fraud and coercion, 15 counts of sex trafficking by force, fraud and coercion, one count of production of child pornography, one count of sex trafficking of a minor by force, fraud and coercion, and one count of conspiracy to launder monetary instruments. The grand jury also indicted Wolfe, Garcia, Moser and Gyi on sex trafficking charges. They have since pled guilty; three of the four have been sentenced.

14. On December 21, 2022, the Spanish National Police arrested PRATT at a hotel in Madrid, Spain. PRATT was extradited to the United States in March 2024 and made his initial appearance in the Southern District of California on March 19, 2024.

15. PRATT is set for trial on September 2, 2025.

Link Between PRATT and Donald Seoane, aka "Donny Long"

16. GDP and GDT models operated under stage names when their videos were posted to the websites. The women's names and personally identifiable information (PII) was not posted on the GDT and GDP websites.

17. However, GDP and GDT models' names and PII were repeatedly posted on www.pornwikileaks.com (PWL), disclosing not only their true identities, but also often their home addresses, phone numbers, email addresses and other social media identifiers. Sometimes the posts even included their high schools and colleges, and identifiers for their parents, siblings, husbands and children. Many women reported that they and their families were harassed and stalked after their identifiers were posted on PWL.

18. Visitors to PWL could -and did- leave comments about the women and their videos. Oftentimes, the comments were not just about the women's appearances in their videos, but also comments on their social media, their personal lives and their families.

19. Donald Seoane, aka "Donny Long," was the original owner of PWL. I believe that PRATT bought PWL from Seoane in 2015.

20. Several indicators reflect that PRATT bought PWL from Seoane in 2015. For example, a subpoena response from Domains by Proxy[2] reflects that in November of 2015, Seoane requested a change in PWL's ownership from Seoane to mike@bll-media.com, a known email account for Michael PRATT. Further, much of the information posted to PWL for GDP and GDT models was information almost exclusively available to PRATT and his companies. Third, during the digital evidence review of electronic devices seized from the GDP/GDT business on October 9, 2019, I observed a Skype conversation between PRATT, identified as "mikeyboyboy1" and co-Defendant Wolfe, identified as "wolfsta Wolfsta." In the conversation, PRATT sent Wolfe a photo of a message that PRATT received from GoDaddy. GoDaddy was the hosting service provider for PWL. GoDaddy advised PRATT that PWL was in violation of GoDaddy's terms of service, because PWL was displaying a driver's license:[3]

[2] Wikipedia explains that Domains by Proxy "offers domain privacy services through partner domain registrars, such as GoDaddy and Wild West Domains. Subscribers list Domains by Proxy as their administrative and technical contacts in the Internet's WHOIS database, thereby delegating responsibility for managing unsolicited contacts from third parties and keeping the domains owners' personal information secret."

[3] PRATT and his employees took photos and videos of each female model holding her driver's license and other information before they filmed a video. At times, those images were displayed on PWL. One of those images may have been what GoDaddy identified.

September 14, 2017

mikeyboyboy1 to wolfsta Wolfsta:

mikeyboyboy1 MJP

It has come to our attention that you are displaying personally identifiable information such as driver's license on your website. As this is a security risk and violation of our terms of service, we request that you remove the content listed below. URL: pornwikileaks.com/monica-dumpster-driving-record-three-time-traffic-school-loser/ We request that this content is removed within 24 hours of this notice to prevent further action from our team. Once you have removed the content, please reply back. Regards, Content Abuse Digital Crimes GoDaddy

9/14/2017 7:22:34 PM(UTC+0)

21. Although I do not have a record of Wolfe's reply to this message, I am aware that Wolfe often assisted PRATT with administrative and website maintenance issues, such as the one identified by GoDaddy above. I conclude from this Skype message that PRATT controlled PWL through at least September 2017.

22. In reviewing the digital evidence seized from the GDP/GDT business on October 9, 2019, I also observed conversations between PRATT and Seoane over Skype. For instance, I observed the following conversation between PRATT, again identified as "mikeyboyboy1" and Seoane, identified as "therealdonnylong," in August 2015. The conversation referenced PWL being used to drive traffic, presumably to GDP and/or GDT:

8/27/2015 3:09:03 PM	therealdonnylong	WHATS YOUR EMAIL
8/27/2015 3:09:11 PM	mikeyboyboy1	JORDAN@GIRLSDOPORN.COM
8/27/2015 3:09:34 PM	therealdonnylong	HAVE YOU SEEN YOUTUBE LIVE AND THE CHAT ROOM AND ALL THE USERS
8/27/2015 3:09:35 PM	therealdonnylong	https://www.youtube.com/watch?v=a48o2S1cPoo
8/27/2015 3:09:40 PM	mikeyboyboy1	haha yah one
8/27/2015 3:09:44 PM	therealdonnylong	LOOKS LIKE A GOOD WAY TO GET TRAFFIC
8/27/2015 3:09:50 PM	therealdonnylong	HMMMM
8/27/2015 3:10:03 PM	mikeyboyboy1	yeah get some hoes on there
8/27/2015 3:10:14 PM	therealdonnylong	MAYBE A LIVE PORNWIKILEAKS SHOW WITH A GUY WITH A ANONYMOUS MASK ANSERING QUESTIONS
8/27/2015 3:10:36 PM	mikeyboyboy1	lol prob work
8/27/2015 3:10:36 PM	therealdonnylong	YEA GIRL WITH BIG TITS AND A ANONYMOUS MASK LOL
8/27/2015 3:10:49 PM	therealdonnylong	WAIT WILL SEND U PIX
8/27/2015 3:16:54 PM	therealdonnylong	i DIDNT TAKE THOSE PIX BUT I SENT THEM TO YOU
8/27/2015 3:18:18 PM	mikeyboyboy1	ass is covered in stretchmarks
8/27/2015 3:18:25 PM	mikeyboyboy1	where is she from
8/27/2015 3:18:40 PM	therealdonnylong	DOMINICIAN REPUBLIC
8/27/2015 3:18:49 PM	therealdonnylong	HUGE BUBBLE BUTT
8/27/2015 3:19:22 PM	therealdonnylong	AND PUT A TIGHT BUTT SHORTS OF HER AND RIP A HOLE IN THEM AND FUCK HER THROUGH THEM
8/27/2015 3:19:29 PM	therealdonnylong	ALWAYS A WAY TO COVER UP SHIT LOL
8/27/2015 3:19:40 PM	mikeyboyboy1	haha

23. In November 2023, Seoane was arrested in Florida on state charges of extortion and threats/intimidation of a judge under Florida State Statutes 836.05-01 and 836.12-3. I contacted the Osceola County Sheriff's Department and spoke with Detective J. Akins, who was assigned the Seoane case.

24. Detective Akins explained that Seoane had filed complaints against several agencies, judges, attorneys, law enforcement officers, and members of the Child Protection Team related to his divorce and child custody proceedings. After those complaints were investigated and closed as unfounded, Seoane retaliated by posting videos to multiple websites and social media platforms. Included in those videos were threats to harm an Osceola County Judge, and the Judge's minor daughter if the Judge did not recuse herself from his family court case and return his children to him. For example, on one video, he said that the Judge should be charged for treason, perjury and being an "abusing criminal scumbag, leftist man hating worthless failed mother, failed wife, scumbag gold digging whore." Seoane posted another video, where he stated the Judge should die just as a Maryland judge had died at the hands of a father who had had his custodial rights revoked. Seoane posted another video where he said that someone was willing to pay the daughter one million dollars if she had sex with Seoane. The daughter would have to "yell mommies name to help her the entire time while Donny Long pounds away in every hole. Mommy judge ----it hurts me help me!, mommy judge ----im not going to shi$ right for a month!, mommy judge ---- you caused this and got me thrown out of college so now I have to take it in the poopshoot by Donny Long God for his million dollars!"

25. Upon Seoane's arrest, the Osceola County Sheriff's Office seized a large number of electronic devices from his person and pursuant to a state search warrant executed at Seoane's residence. **Device 1** was seized from Seoane's residence. **Device 2** was seized from Seoane's person when he was arrested in a traffic stop.

26. In the meantime, on Tuesday, April 16, 2024, the United States Attorney's Office received the following anonymous email, outlining the writer's views on Long's (Seoane's) connection to PWL, GDP and PRATT:

> *I'm writing you today about the GirlsDoPorn case, specifically Pratt and his connection to Donny Long.*
>
> *Pratt paid Donny Long (Donald Carlos Seone) $10,000 on one occasion and another $5,000 on another for his part in trashing the girls on the pornwikileaks.com website. This was all documented in Donny Long's Skype, where he talked about it over and over and on at least five occasions on the phone with Dwight Cunningham from The Luxury Companion (the pornstar escorting website).*
>
> *The pornwikileaks.com website is mentioned multiple times on the original GDP inditement. Yet Donny Long, who owned and ran the PornWikiLeaks website, never got arrested for his involvement.*
>
> *Years later, he ended up selling the domain (yet kept the databases) to BangBros.*
>
> *https://mikesouth.com/industry/bonfire-bangbros-claims-all-pornwikileaks-data-destroyed-right-in-the-middle-of-the-girlsdoporn-trial-50023/*
>
> *However, it should be noted Donny Long never stopped using the exact same harassment tactics that they did for the women in the GirlsDoPorn case.*
>
> *In fact, you'll find he's currently in jail in Florida for doing that to a judge! https://apps.osceola.org/Apps/CorrectionsReports/Report/Details/1277492*
>
> *When he was arrested, everything was seized. They now have the database from the Pornwikileaks website in their possession on those hard drives.*
>
> *Michael J Pratt was a horrible person, but he wasn't able to do what he did to those women without the help of Donny Long.*
> *r*
> ***Donny Long should face charges as well.***
>
> *The question is, why hasn't he?*
>
> *Donny Long created, owned, and operated PornWikiLeaks.com for YEARS. In exchange for money, he created a special section of the website dedicated to the young women who worked for GirlsDoPorn so they could (as you know) get extra harassment and exposure.*
>
> *Donny Long is a monster who did a lot of damage to a lot of women for decades.*
>
> *He deserves to face punishment for his involvement in the GirlsDoPornCase.*

27. In September of 2024, I received an update from Detective Akins. He observed that Seoane used his "therealdonnylong" Skype account on **Devices 1** and **2**. He also observed conversations with "therealdonnylong" and "mikeyboyboy1" on **Devices 1 and 2**. However, because these conversations were outside the scope of his warrant, Detective Akins did not read the content of these communications. Detective Akins agreed to provide a copy of the imaged devices to me.

28. On November 19, 2024, FBI San Diego Division, received a copy of **Devices 1** and **2** on a Samsung hard drive. I am asking to search these Devices for Skype conversations between "therealdonnylong" and "mikeyboyboy1" concerning GDP/GDT, PWL and efforts to out the victims. I also seek to find evidence of Seoane's, PRATT's and anyone else's ownership and/or control of PWL, and content posted to PWL concerning GDP and women whose pornographic videos were posted to GDP/GDT.

Procedures For Electronically Stored Information – Cell Phone (Device 1)

29. Following the issuance of this warrant, I will collect the download of Device 1.[4] All forensic analysis of the data contained within the forensic download of Device 1 will employ search protocols directed exclusively to the identification and extraction of data within the scope of this warrant.

30. Based on the foregoing, identifying and extracting data subject to seizure pursuant to this warrant may require a range of data analysis techniques, including manual review, and, consequently, may take weeks or months. The personnel conducting the identification and extraction of data will complete the analysis

[4] Since Device 1 has already been seized and forensically imaged, I have removed the first paragraph of the cell phone search protocol from this affidavit.

within ninety (90) days of the date the warrant is signed, absent further application to this court.

Procedures For Electronically Stored Information – Computer and Electronic Storage Devices (Device 2)

31. With the approval of the Court in signing this warrant, agents executing this search warrant will employ the following procedures regarding computers and other electronic storage devices, including electronic storage media, that may contain data subject to seizure pursuant to this warrant:

Identification and Extraction of Relevant Data[5]

a. After obtaining a forensic image, the imaged copy will be analyzed to identify and extract data subject to seizure pursuant to this warrant. Analysis of the data following the creation of the forensic image can be a highly technical process requiring specific expertise, equipment, and software. There are thousands of different hardware items and software programs, and different versions of the same programs, that can be commercially purchased, installed, and custom-configured on a user's computer system. Computers are easily customized by their users. Even apparently identical computers in an office environment can be different with respect to configuration, including permissions and access rights, passwords, data storage, and security. It is not unusual for a computer forensic examiner to have to obtain specialized hardware or software, and train with it, in order to view and analyze imaged data.

b. Analyzing the contents of a computer or other electronic storage device, even without significant technical challenges, can be very challenging. Searching by keywords, for example, often yields many thousands of hits, each of which must be reviewed in its context by the examiner to determine whether

[5] Since Device 2 has already been seized and forensically imaged, I have removed the "Forensic Imaging" section from this affidavit.

the data is within the scope of the warrant. Merely finding a relevant hit does not end the review process for several reasons. The computer may have stored metadata and other information about a relevant electronic record – e.g., who created it, when and how it was created or downloaded or copied, when it was last accessed, when it was last modified, when it was last printed, and when it was deleted. Keyword searches may also fail to discover relevant electronic records, depending on how the records were created, stored, or used. For example, keywords search text, but many common electronic mail, database, and spreadsheet applications do not store data as searchable text. Instead, the data is saved in a proprietary non-text format. Documents printed by the computer, even if the document was never saved to the hard drive, are recoverable by forensic programs because the printed document is stored as a graphic image. Graphic images, unlike text, are not subject to keyword searches. Similarly, faxes sent to the computer are stored as graphic images and not as text. In addition, a particular relevant piece of data does not exist in a vacuum. To determine who created, modified, copied, downloaded, transferred, communicated about, deleted, or printed the data requires a search of other events that occurred on the computer in the time periods surrounding activity regarding the relevant data. Information about which user had logged in, whether users share passwords, whether the computer was connected to other computers or networks, and whether the user accessed or used other programs or services in the time period surrounding events with the relevant data can help determine who was sitting at the keyboard.

c. It is often difficult or impossible to determine the identity of the person using the computer when incriminating data has been created, modified, accessed, deleted, printed,

copied, uploaded, or downloaded solely by reviewing the incriminating data. Computers generate substantial information about data and about users that generally is not visible to users. Computer-generated data, including registry information, computer logs, user profiles and passwords, web-browsing history, cookies and application and operating system metadata, often provides evidence of who was using the computer at a relevant time. In addition, evidence such as electronic mail, chat sessions, photographs and videos, calendars and address books stored on the computer may identify the user at a particular, relevant time. The manner in which the user has structured and named files, run or accessed particular applications, and created or accessed other, non-incriminating files or documents, may serve to identify a particular user. For example, if an incriminating document is found on the computer but attribution is an issue, other documents or files created around that same time may provide circumstantial evidence of the identity of the user that created the incriminating document.

d. Analyzing data has become increasingly time-consuming as the volume of data stored on a typical computer system and available storage devices has become mind-boggling. For example, a single megabyte of storage space is roughly equivalent to 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is roughly equivalent to 500,000 double-spaced pages of text. Computer hard drives are now being sold for personal computers capable of storing up to 2 terabytes (2,000 gigabytes) of data. And, this data may be stored in a variety of formats or encrypted (several new commercially available operating systems provide for automatic encryption of data upon shutdown of the computer). The sheer volume of data also has extended the time that it takes to analyze data.

Running keyword searches takes longer and results in more hits that must be individually examined for relevance. And, once reviewed, relevant data leads to new keywords and new avenues for identifying data subject to seizure pursuant to the warrant.

e. Based on the foregoing, identifying and extracting data subject to seizure pursuant to this warrant may require a range of data analysis techniques, including the use of hashing tools to identify evidence subject to seizure pursuant to this warrant, and to exclude certain data from analysis, such as known operating system and application files. The identification and extraction process may take weeks or months. The personnel conducting the identification and extraction of data will complete the analysis within one-hundred twenty (120) days from the date this warrant, absent further application to this court.

f. All forensic analysis of the imaged data will employ search protocols directed exclusively to the identification and extraction of data within the scope of this warrant.

Genuine Risks of Destruction of Data

32. Given that the Samsung Hard drive is an image of Devices 1 and 2, and these Devices are currently in the custody of the Osceola County Sheriff's Office, I do not see a significant risk that the data will be destroyed.

//

//

//

Prior Attempts to Obtain Data

33. The Osceola County Sheriff's Department has reviewed the Devices pursuant to a separate warrant. However, the FBI has not attempted to obtain data from **Devices 1 and 2.**

Request For Sealing

34. This search warrant need not be sealed and will be disclosed to defense counsel for PRATT.

Conclusion

35. Based on the foregoing, I respectfully submit that there is probable cause to believe that evidence of and property designed for use, intended for use, or that PRATT and his co-conspirators have used in the commission of violations of 18 U.S.C. Sec. 1591(d) (Obstruction of Sex Trafficking Enforcement), 18 U.S.C. Sec. 1591(a) and (b)(1) (Sex Trafficking of a Minor or by Force, Fraud and Coercion), 18 U.S.C. Secs. 1594(c) (Conspiracy to Commit Sex Trafficking by Force, Fraud and Coercion), and 18 U.S.C. Sec. 1956 (Money Laundering), as further detailed in Attachment B, will be found in Attachment A.

LANA K. SABATA
FBI Special Agent

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on the 15th of January, 2025.

HON. MITCHELL D. DEMBIN
U.S. Magistrate Judge

ATTACHMENT A

ITEM TO BE SEARCHED

A) a forensic image of one ASUS computer tower with connected media devices (hereinafter identified as **DEVICE 1)**; and

B) a forensic image of one white Samsung Galaxy S20 in a Red and Black case, IMEI 354268111077421 (hereinafter identified as **DEVICE 2).**

These images are currently stored on one Samsung Hard Drive at the Federal Bureau of Investigation (FBI) Headquarters, 10385 Vista Sorrento Parkway, San Diego, California.

ATTACHMENT B

Authorization is sought to search the items listed in Attachment A for evidence that relates to violations of 18 U.S.C. § 1591(d) (Obstruction of Sex Trafficking Enforcement), 18 U.S.C. § 1591(a) and (b)(1) (Sex Trafficking by Force, Fraud and Coercion), 18 U.S.C. § 1594(c) (Conspiracy to Commit Sex Trafficking by Force, Fraud and Coercion), and 18 U.S.C. § 1956 (Money Laundering).

Agents will search for all communications, records, or data, including but not limited to emails, text messages, photographs, audio files, videos, or location data, for the period of **January 1, 2015 through September 30, 2017** for:

a. Communications, records, or attachments relating to the operation, ownership, and control of businesses and websites used in the sex trafficking and money laundering conspiracy to include girlsdoporn.com, girlsdotoys.com, and pornwikileaks.com, as well as third party sites associated with these sites;

b. Communications, records, and attachments mentioning names, dates of birth and/or any other biographical information of women who appeared or attempted to appear in GirlsdoPorn (GDP) and GirlsDoToys (GDT) videos;

c. Communications, records, and attachments discussing the potential exposure of GDP and GDT models' true names and identifiers, and the true names and identifiers of others related to the GDP and GDT models.

d. Communications, records, and attachments tending to identify the account user's state of mind, including knowledge, motive, and voluntariness, regarding the crimes under investigation;

e. Communications, records, and attachments regarding Michal Pratt's or Donald Seoane's attempts to tamper with witnesses (to include former GirlsDoPorn/GirlsDoToys models and employees), and hinder or obstruct the investigation into GirlsDoPorn, GirlsDoToys, Pornwikileaks or any other criminal activity involving Pratt;

f. Communications, records, and attachments that provide context to any communications, records, videos, photographs and attachments described above, such as texting applications, electronic mail sent or received in temporal proximity to any relevant electronic mail and any electronic mail tending to identify the user(s) of the Devices to be searched; and

g. Communications, records and attachments tending to identify the user of, or persons with control over or access to the Devices.