

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF FLORIDA

No. 17-MJ-02140-TORRES

UNITED STATES OF AMERICA

vs.

DONALD PAUL CLIPPINGER,

Defendant.

---

CRIMINAL COVER SHEET

1. Did this matter originate from a matter pending in the Northern Region of the United States Attorney's Office prior to October 14, 2003? \_\_\_\_ Yes X No
2. Did this matter originate from a matter pending in the Central Region of the United States Attorney's Office prior to September 1, 2007? \_\_\_\_ Yes X No

Respectfully submitted,  
WIFREDO A. FERRER  
UNITED STATES ATTORNEY

By: 

DANIEL CERVANTES  
Assistant United States Attorney  
Florida Bar No.40836  
U.S. Attorney's Office - SDFL  
99 N.E. 4th Street, Suite 600  
Miami, FL 33132-2111  
Telephone: (305) 961-9031  
Facsimile: (305) 536-4699  
Email: daniel.cervantes@usdoj.gov

# UNITED STATES DISTRICT COURT

for the

Southern District of Florida

United States of America  
v.  
DONALD PAUL CLIPPINGER,

Case No. 17-MJ-02140-TORRES

Defendant(s)

## CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of November 13, 20, and 23, 2015 in the county of Miami-Dade in the  
Southern District of Florida, the defendant(s) violated:

Code Section

Offense Description

18 U.S.C. § 2252(a)(4)(B) & (b)(2)

Access with intent to view visual depictions of minors engaged in sexually explicit conduct

This criminal complaint is based on these facts:

See Attached Affidavit

☒ Continued on the attached sheet.



Complainant's signature

Special Agent Alicia Centeno, HSI

Printed name and title

Sworn to before me and signed in my presence.

Date: 02/01/2017



Judge's signature

City and state: Miami, Florida

United States Magistrate Judge Edwin G. Torres

Printed name and title

**AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT**

I, Alicia Centeno, having been duly sworn, do hereby depose and state:

**I. BACKGROUND**

1. I am a Special Agent (SA) with Homeland Security Investigations (HSI), Immigration and Customs Enforcement (ICE), SAC-Miami, and have been so employed since April 2004. Since October of 2015, I have been assigned to the Cybercrimes/Child Exploitation Unit in the Miami Field Office where I investigate, among other violations of federal law, cases involving the sexual exploitation of children.

2. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18 of the United States Code. That is, I am an officer of the United States, who is empowered by law to conduct investigations of, and make arrests for, offenses enumerated in Title 18, United States Code, Sections 2422, 2423, 2251, and 2252, *et seq.*

3. As a federal agent I am also authorized, under Title 18, United States, Code, Section 3056, to conduct investigations of and execute warrants for offenses involving the exploitation of children, including those offenses enumerated in Title 18, United States Code, Sections 2422, 2423, 2251, and 2252, *et seq.*

4. As a federal agent, I have participated in investigations of persons suspected of violating federal child pornography laws, including Title 18, United States Code, Sections 2422, 2423, 2251, and 2252, *et seq.* These investigations have included the use of surveillance techniques, undercover activities, the interviewing of subjects and witnesses, and the planning and execution of arrest, search, and seizure warrants. In the course of these investigations, I have reviewed hundreds of still images and videos containing child pornography and images depicting minor children engaged in sexually explicit conduct on all forms of electronic media including

computers, digital cameras, and wireless telephones, and have discussed and reviewed these materials with other law enforcement officers. I have also participated in training programs for the investigation and enforcement of federal child pornography laws relating to the use of computers for receiving, transmitting, and storing child pornography.

5. This Affidavit is submitted in support of a criminal complaint charging that on or about November 13, 20, and 23, 2015, in Miami-Dade County, in the Southern District of Florida, and elsewhere, DONALD PAUL CLIPPINGER did knowingly access with intent to view, matter which contained any visual depiction that had been shipped and transported using any means and facility of interstate and foreign commerce, and in and affecting interstate and foreign commerce, and which was produced using materials which had been so shipped and transported, by any means, including by computer, and the production of such visual depiction having involved the use of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2), and such visual depiction was of such conduct, in violation of Title 18, United States Code, Section 2252(a)(4)(B) and (b)(2).

6. This Affidavit is based on my own investigation and information provided by other law enforcement officers and personnel specially trained in the seizure and analysis of computers and electronic media. Because this Affidavit is submitted solely for the purpose of establishing probable cause, I have not included each and every fact known to law enforcement about this investigation.

## II. PROBABLE CAUSE

7. In October 2015, law enforcement began conducting undercover operations on an Internet-based video conferencing application used by persons interested in exchanging child pornography and/or sexually abusing children, herein after referred to as “Application A.”<sup>1</sup>

8. “Application A” is designed for video conferencing on multiple device formats. To use this application, a user downloads the application to a computer, mobile phone or other mobile device (*e.g.*, tablet) via direct download from the company’s website. Once downloaded and installed, the user is prompted to create an account. “Application A” users can invite others to an online meeting “room,” which is an online location associated with a 10-digit number where each user can see and interact with the other users.

9. When a user chooses to enter a specific meeting room, the user enters the 10-digit room number and enters the username that he wants to use on that specific occasion, which does not have to be the same as the account username. “Application A” does not require a certain number of characters for a particular username. Consequently, a user can create a name with a single special character, such as “#” or a single letter, such as “a.”

10. During a meeting, users can show a live image or video of themselves to other users through the webcam feature. Users may also display the contents of their own computer desktops to the other users in the room. The ability to display their own computer desktops allows users to show videos and photos to other users in the room. “Application A” also allows users to send text

---

<sup>1</sup> The actual name of “Application A” is known to law enforcement. “Application A” remains active and disclosure of the name of the application would potentially alert its users to the fact that law enforcement action is being taken against users of the application, thereby provoking users to notify other users of law enforcement action, flee, and/or destroy evidence. Accordingly, to protect the confidentiality and integrity of the ongoing investigation involved in this matter, specific names and other identifying factors have been replaced with generic terms and the application will be identified herein as “Application A.”

messages visible to all of the users in the room, or private messages that are similar to instant messages sent between two users.

11. “Application A” permits users to conduct online video conferences for free for a limited number of minutes. Paid subscribers can conduct online video conferences for an unlimited amount of time. Some “Application A” users with a paid account permit their rooms to be accessed without a password such that anyone who knows the room number can enter and leave the room at any time.

12. “Application A” maintains IP address logs for each meeting room, which includes all of the IP addresses (and related usernames) for each user in a particular room on a specific day and the device that was used by each user. Each user’s unique IP address is logged to reflect the time that a particular user entered the room and the time the user exited the room. Users can enter and exit the room multiple times, thereby creating multiple sessions<sup>2</sup> within the logs of “Application A.” In other words, if a room is open and active for one hour, and in that hour, a user enters the room, leaves the room, and then re-enters the room, the “Application A” IP log records would reflect two sessions for that specific user (entry/exit, followed by second entry) in the same room on that date.

13. “Application A” also has a function that allows the meeting participants to record the main presentation. Even if a user does not use “Application A’s” recording function, the user can take screen shots or record the video session by using other publicly available software.

14. On or about November 13, 2015, law enforcement located in Phoenix, Arizona, acting in an undercover capacity and using a device connected to the Internet, signed into a meeting

---

<sup>2</sup> As used herein, a session refers to a particular user’s time in a specific “Application A” room.

room on “Application A” and observed users displaying or streaming videos of child pornography to other members of the room. During this undercover session, law enforcement was able to record the aforementioned video transmissions of suspected child pornography and other activity and messages in the room. While recording the activity in the room, the undercover agent observed that a meeting participant, with the display name “666prv,” began transmitting a streaming video to the room via a webcam. User “666prv” streamed a video of himself watching his computer screen. User “666prv” appeared to be a nude Caucasian adult male, who displayed his neck, stomach, and part of his upper legs and thighs. During the transmission of the video, “666prv” was observed rubbing his left nipple while sitting in what appears to be a black office style chair.

15. On or about November 20, 2015, law enforcement in Phoenix, Arizona, acting in an undercover capacity and using a device connected to the Internet, signed into a meeting room on “Application A” and observed users displaying or streaming videos of child pornography to other members of the room. During this undercover session, law enforcement was able to record the aforementioned video transmissions of suspected child pornography and other activity and messages in the room. Law enforcement observed user “666prv” transmit a streaming video of himself in the aforementioned meeting room approximately 4 minutes after streaming videos of suspected child pornography were being displayed to members of the meeting room. User “666prv” appeared to be the same nude Caucasian adult male and was displaying his neck, stomach, and part of his upper legs and thighs. During this transmission, user “666prv” appeared to have one hand positioned between his legs.

16. On November 23, 2015, law enforcement in Phoenix, Arizona, acting in an undercover capacity and using a device connected to the Internet, signed into a meeting room on “Application A” and observed users displaying videos of child pornography to other members of

the room. During this undercover session, law enforcement was able to record the aforementioned videos transmissions of suspected child pornography and other activity and messages in the room. Law enforcement observed user "666prv" transmit a streaming video of himself in the meeting room at times when streaming videos of suspected child pornography were being displayed to all members of the room. During this transmission, "666prv" appeared to be the same aforementioned nude Caucasian adult male. User "666prv" was observed displaying his neck, stomach, and part of his upper legs and thighs and was touching his penis.

17. Subpoenaed business records from "Application A" revealed that on the above-mentioned dates, user "666prv" accessed "Application A" utilizing an IP address registered to AT&T Corporation.

18. Subpoenaed business records from AT&T indicated the aforementioned IP Address utilized by "666prv" to access "Application A" was registered to CLIPPINGER, at his residence in Miami Shores, Florida ("CLIPPINGER's residence").

19. On January 25, 2017, the Magistrate Court in the Southern District of Florida, authorized a federal search warrant for CLIPPINGER's residence.

20. On January 31, 2017, law enforcement executed the aforementioned federal search warrant at CLIPPINGER's residence. Upon entering the residence, law enforcement encountered CLIPPINGER and his partner, Y.D. During the search of the residence, law enforcement seized multiple pieces of electronic media from the residence, including a DELL computer tower, from the office located on the second floor.

21. A review of the room where the DELL computer was located revealed that it is the same room depicted in the video that user "666prv" transmitted of himself into the meeting room. Law enforcement identified the chair, table, wall, outlet, floor, trashcan, and the bottom of a picture



frame, all of which were depicted in the videos that user "666prv" transmitted of himself into the meeting rooms.

22. An onsite, preliminary forensic examination of the DELL computer tower revealed the presence of "Application A," the "666prv" username, and Internet communications related to child exploitation via "Application A" and another Internet based video conferencing software. The preliminary examination revealed that the DELL computer user accessed "Application A" as recently as the day before the search warrant was executed. The preliminary examination also revealed one thumbnail image of child pornography on the DELL computer. The preliminary examination further revealed that the DELL computer user received a file on September 21, 2013, via conferencing software that had the title, "diaz 2010-pthc baby raamat 10.mp4," which is a title that is indicative of child pornography. I know, based on my training and experience, that "pthc" stands for pre-teen hard core and that "pthc" is a common term used to search for child pornography on the internet. The forensic examination is ongoing and has not been completed as of the date of this affidavit.

23. Law enforcement interviewed CLIPPINGER. Prior to questioning, CLIPPINGER was advised of his *Miranda* Rights in English, which he stated he understood and waived both verbally and in writing. CLIPPINGER stated that he had been living at that residence for several years. CLIPPINGER further stated that the aforementioned DELL tower computer belonged to him. CLIPPINGER admitted utilizing his DELL tower computer to enter "Application A" with the "666prv" username. CLIPPINGER stated that while logged into a meeting room of "Application A," he observed streaming videos of child pornography that were being transmitted by other users. CLIPPINGER explained that he usually accessed "Application A" in the mornings and sometimes in the afternoon.

24. CLIPPINGER then reviewed screen captures of two child pornography videos depicting prepubescent males performing oral sex on adult males, which were transmitted to the "Application A" meeting room on November 23, 2015. CLIPPINGER stated that he recognized the child pornography videos depicted in the screen captures and admitted remaining in the meeting room of "Application A" while files of child pornography were being transmitted. CLIPPINGER admitted to masturbating to images of child pornography and to describing himself on multiple occasions as a "Pedo" to other users on both "Application A" and other video conferencing software. The preliminary forensics examination confirmed that the user "666prv" on "Application A" had a conversation on January 20, 2016, with another "Application A" user where "666prv" stated, "perv ped bait the best." Based on my training and experience, I know that "pedo" or "ped" stands for pedophile, and individuals engaged in viewing and chatting about child pornography on the internet either describe themselves as "pedo" or "ped" and they use those words as search terms to search for videos of child pornography on the internet.

25. Law enforcement also showed CLIPPINGER a still frame image of the nude, Caucasian male depicted in the meeting room on November 20 and 23, 2015. CLIPPINGER admitted that he was the male depicted in the images.

26. Law enforcement also interviewed Y.D. Prior to questioning, Y.D. was advised of Y.D.'s *Miranda* Rights in English, which Y.D. stated that Y.D. understood and waived both verbally and in writing. Y.D. stated that Y.D. has been living at CLIPPINGER's residence since approximately June of 2016. Y.D. stated that CLIPPINGER owns the DELL computer and that Y.D. utilizes the computer on rare occasions to print documents for work. Y.D. utilizes the Toshiba laptop and cell phone for general Internet use. Y.D. is unfamiliar with "Application A" and has never observed child pornography before. Y.D. then reviewed a screen captured image of

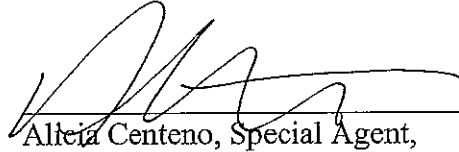
the aforementioned nude, Caucasian male transmitted via the "666prv" username to the "Application A" meeting room on November 20, 2015. Y.D. identified the person depicted in the screen capture as CLIPPINGER.

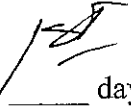
27. The preliminary forensic examination of Y.D.'s Toshiba laptop revealed no evidence of child exploitation or the presence of "Application A."

### III. CONCLUSION

28. Based upon the foregoing, I submit that there is probable cause to believe that, on or about November 13, 20, and 23, 2015, DONALD PAUL CLIPPINGER did knowingly access with intent to view a visual depiction of a minor engaged in sexually explicit conduct, in violation of Title 18, United States Code, Section 2252(a)(4)(B) and (b)(2).

**FURTHER YOUR AFFLIANT SAYETH NAUGHT.**

  
Alicia Centeno, Special Agent,  
Department of Homeland Security Investigations

Sworn and subscribed before me this  day of February 2017.

  
HONORABLE EDWIN TORRES  
UNITED STATES MAGISTRATE JUDGE