AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

District of New Jersey

United States of America
v.
Carlos Santiago Gomez

Case No. 18-MJ-1006 (AMD)

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 April 2016 through March 27, 2018 in the county of Atlantic in the _____ District of New Jersey, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C., Sections 2252A(a)(2)(A) and (b)(1)	Count 1 -- receipt of child pornography, in violation of 18 U.S.C. Sections 2252A(a)(2)(A) and (b)(1); and Count 2 -- distribution of child pornography, in violation of 18 U.S.C. Sections 2252A(a)(2)(A) and (b)(1); as more fully described in Attachment A hereto.

This criminal complaint is based on these facts:

Affidavit (See Attachment B)

☑ Continued on the attached sheet.

Complainant's signature

Daniel A. Garrabrant, FBI Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 06/01/2018

Judge's signature

City and state: Camden, New Jersey

Hon. Ann Marie Donio, U.S. Magistrate Judge

Printed name and title

CONTENTS APPROVED

UNITED STATES ATTORNEY

By: 

DIANA VONDRA CARRIG
Assistant U.S. Attorney

Date: June 1, 2018

ATTACHMENT A

Count 1 – Receipt of Child Pornography

From in or about April 2016 through on or about March 27, 2018, in Atlantic County, in the District of New Jersey, and elsewhere, defendant

CARLOS SANTIAGO GOMEZ,

did knowingly receive more than 3 images of child pornography, as defined in Title 18, United States Code, Section 2256(8), which had been saved to his cellular telephone and flash drive, each of which images had been shipped and transported in and affecting interstate and foreign commerce by any means, including by computer.

In violation of Title 18, United States Code, Sections 2252A(a)(2)(A) and (b)(1).

Count 2 – Distribution of Child Pornography

From in or about April 2016 through on or about March 27, 2018, in Atlantic County, in the District of New Jersey, and elsewhere, defendant

CARLOS SANTIAGO GOMEZ,

did knowingly distribute more than 3 images of child pornography, as defined in Title 18, United States Code, Section 2256(8), which had been distributed via computer device to include a cellular telephone, each of which had been shipped and transported in and affecting interstate and foreign commerce by any means, including by computer.

In violation of Title 18, United States Code, Sections 2252A(a)(2)(A) and (b)(1).

ATTACHMENT B

1. I, Daniel A. Garrabrant, am a Special Agent with Federal Bureau of Investigation ("FBI") within the United States Department of Justice. I have personally participated in this investigation and am aware of the facts contained herein based upon my own investigation as well as information provided to me by other law enforcement officers. Since this Affidavit is submitted for the sole purpose of establishing probable cause to support the issuance of a complaint, I have not necessarily included each and every fact known to the Government concerning this investigation.

2. I am the Child Exploitation Task Force Coordinator ("CETF") for the FBI's Atlantic City Resident Agency ("ACRA"). This Task Force is comprised of investigators from the Atlantic County Prosecutor's Office, Atlantic County Sheriff's Office, New Jersey State Police, and the New Jersey Human Services Police. This Task Force specializes in investigations related to the sexual exploitation of children.

3. On or about February 20, 2018, the Atlantic City FBI Child Exploitation Task Force received a lead from the Denver Field Office of the FBI concerning a suspect whom the Denver Field Office had been investigating. That lead included the following information, in summary and in part:

a. During the summer of 2017, a child pornography suspect in the Denver Field Office consented to the Denver Innocent Images Task Force ("IITF") taking over the suspect's KIK[1] account. Upon accessing the KIK account, IITF members observed the viewing, discussion, and distribution of child pornography in four KIK groups.

[1] KIK is an instant messaging application that may be downloaded onto mobile devices. Users are identified through an unconfirmed name and a unique KIK user name. Users also provide an email address at the time of registration, but confirmation of a valid email address is not necessary to use the application.

b. Group member "robochicken90" was observed trading child pornography on multiple dates, including July 29, 2017 and August 30, 2017, in the KIK group(s) whose names ended in "VIP" and/or "VIPII."

c. In reviewing the material being traded by KIK user "robochicken90," law enforcement noted that the account name was "Aaron Licht." User "robochicken90" posted a welcome message on or about September 27, 2017, stating: "New comers, welcome. There are just some rules to keep in mind when posting and maintaining your position. 1. Girls only 2. No Toddler 3. Videos only, no links no pictures. 4. Goes without saying but be active. Thanks and enjoy."

d. On or about October 2, 2017, the user "robochicken90" also directed traders to beware, stating: "If you're using FREENET, you might as well call the cops and turn yourself in. TOR, though not 100% safe by default, is slow but way better than FREENET."

e. In response to other(s) who posted images of adult pornography, user "robochicken90" scolded during posts on September 30, 2017: "The last one is 18+ Please don't post adult videos. Thanks."

4. Your affiant reviewed Denver's IITF lead, including the videos and images that user "robochicken90" received, posted, traded and distributed. Those images depict prepubescent females being filmed while being sexually assaulted by adult males and/or engaging in sexually explicit acts. Specifically,

a. On July 29, 2017, the user "robochicken90" posted a video which showed a prepubescent female lying on her back while a male she referred to as "daddy" masturbated and ejaculated on the child.

b. On July 29, 2017, the user "robochicken90" posted a video which showed a prepubescent female with blond hair, with her legs spread digitally penetrating her vagina with her finger.

c. On July 29, 2017, the user "robochicken90" posted a video which showed a prepubescent female with blond hair in a bright pink shirt exposing her anus and vaginal area.

d. On August 30, 2017, the user "robochicken90" posted a video which showed what appears to be a minor female in a purple shirt lying on her back while an adult male masturbated and ejaculated on her face.

e. On August 30, 2017, the user "robochicken90" posted a video which showed a very young naked prepubescent female on top of a male that has his penis between her legs and appears to be trying to penetrate her with his penis.

5. Law enforcement have identified the KIK user "robochicken90" as the defendant CARLOS SANTIAGO-GOMEZ of Absecon, New Jersey, through various means, including as described *supra.*

6. On July 19, 2017, law enforcement officers served a subpoena on KIK for information on multiple users, including "robochicken90." On July 25, 2017, KIK responded to the subpoena with subscriber and IP information for "robochicken90," including that the user "robochicken90" had signed up for KIK on July 21, 2017 with email address gmastercarlos11@hotmail.com. The subpoena response included 122 pages of IP login information. Law enforcement's review of the IP login information revealed that for the majority of logins, user "robochicken90" used a New Jersey IP address 73.150.187.45, which was provided by the internet service provider Comcast.

7. On December 12, 2017, law enforcement served a subpoena to Comcast requesting the subscriber information affiliated with the IP address 73.150.187.45 on various specific dates and times (corresponding to the KIK information pertaining to user

"robochicken90"). That same day, Comcast responded to the subpoena and advised that during the requested specific dates and times, the IP address was assigned to CARLOS SANTIAGO, at an address in Absecon, New Jersey, and with telephone number XXX-XXX-8976. Comcast IP history indicates that IP address 73.150.187.45 was leased by CARLOS SANTIAGO from on or about June 16, 2017 through December 11, 2017.

8. Law enforcement ran database checks and confirmed that the defendant CARLOS SANTIAGO, having the date of birth XX/XX/1990, and a social security known to law enforcement, resided at the Absecon address provided by Comcast.

9. In addition, New Jersey motor vehicle records indicate that defendant CARLOS SANTIAGO used the Absecon address as his address of record for his driver's license and also has a Black Volkswagen Passat with New Jersey registration C91GJB registered to him at that address.

10. Law enforcement officers conducted surveillance at the Absecon residence on the evening of March 6, 2018, and the defendant CARLOS SANTIAGO GOMEZ was observed in the area of the above stated Absecon residence. Law enforcement observed CARLOS SANTIAGO GOMEZ getting out of the previously described black Volkswagen Passat with a woman whom law enforcement later identified as his fiancée and a child who was approximately two to three years of age. CARLOS SANTIAGO GOMEZ, his fiancée and the child exited the Passat and walked up the steps and into the Absecon residence.

11. Law enforcement reviewed various social media platforms on March 9, 2018, and found the below described accounts affiliated with the email address gmastercarlos11@hotmail.com:

a. An Apple account;

b. Two Skype accounts were located:

   i. one using the user name "live:Santiago0621" which is listed under CARLOS SANTIAGO GOMEZ and telephone number XXX-XXX-8976; and

   ii. the other using the username "live:gmastercarlos" which is listed under CARLOS SANTIAGO with the same telephone number XXX-XXX-8976;

c. A Facebook account with the display name CARLOS SANTIAGO, and affiliated with telephone number XXX-XXX-8976. The Facebook account included posts which indicated that CARLOS SANTIAGO was an IT specialist for a computer software company. CARLOS SANTIAGO also indicated in Facebook posts that he has held previous jobs in the IT field. Law enforcement compared the image of CARLOS SANTIAGO depicted in the Facebook account to the New Jersey driver's license photograph for CARLOS SANTIAGO GOMEZ, and confirmed that the photographs are of the same person, that is, the defendant CARLOS SANTIAGO GOMEZ.

d. An Instagram account; and

e. A Google account with the display name of CARLOS SANTIAGO-GOMEZ.

12. Through social media database checks on March 9, 2018, law enforcement also found an account on "Telegram"[2] corresponding to the telephone number XXX-XXX-8976, which was associated with user ID: 514241860 and a display name of "Aaron Licht." Telegram indicated that the user was last online on January 16, 2018.

[2] Telegram is an instant messaging and voice over IP service through which users can send messages, exchange photos, videos, audio and other files.

13. On March 27, 2018, Investigators assigned to the FBI's ACRA/CETF executed a search warrant at the defendant CARLOS SANTIAGO GOMEZ'S Absecon residence. This search warrant was signed by the Honorable Jeffrey Waldman, New Jersey Superior Court Judge for Atlantic County, New Jersey. During the search, law enforcement officers seized multiple items of digital evidence, including cell phones, CD discs, thumb drives, hard drives and computers.

14. Defendant CARLOS SANTIAGO GOMEZ was present at the time the search warrant was executed and consented to an interview. During that interview, which was non-custodial, the defendant admitted to possessing child pornography and directed law enforcement to a thumb drive that was located in his backpack in the dining room area of the residence. During that interview, the defendant CARLOS SANTIAGO GOMEZ stated the following, in sum and substance:

a. SANTIAGO GOMEZ used his cellular phone (Google Pixel 2XL), flash drive (recovered from his back pack) and home computer network including Wifi to download and view child pornography and to distribute child pornography to other KIK users and/or users on other platforms on the Internet.

b. SANTIAGO GOMEZ was actively involved with two KIK Messaging groups, namely, the two groups referenced in paragraph 3 above, both of which were established for "like minded" individuals who were interested in exchanging child pornography.

c. SANTIAGO GOMEZ used the display name "Aaron Licht" with his "robochicken90" KIK account.

d. SANTIAGO GOMEZ became the administrator of the KIK group whose name ended in "VIPII" and provided rules to its members, including his preference for girls under 18, but not toddlers.

e. SANTIAGO GOMEZ advised that although he preferred child pornography of girls between approximately 8 and 12 years of age, he maintained pornographic images of other children, including toddlers, infants and boys. SANTIAGO GOMEZ advised that he maintained these images to share and trade with other people in the group who were interested in toddlers, infants and boys.

15. Although the forensic analysis of all of the items seized from SANTIAGO GOMEZ's residence (and pursuant to the search warrant) is not yet complete, law enforcement officers have conducted examinations of various items seized at SANTIAGO GOMEZ's residence, including his cellular telephone (Google Pixel 2XL) and the thumb drive recovered from SANTIAGO GOMEZ's backpack in the dining room area. Those preliminary findings show that those two devices alone – the cell phone and thumb drive – each contained more than 1,000 images of child pornography. Although some of the images and videos were on both devices, several images and videos appeared to be represented exclusively on one device or the other. In addition, the preliminary findings show that SANTIAGO GOMEZ received and distributed the bulk of the child pornography beginning in or about April 2016.

16. The thumb drive utilized by CARLOS SANTIAGO GOMEZ was a dual-sided device, with a normal USB side and a micro USB side. This dual-sided device allowed defendant CARLOS SANTIAGO GOMEZ to download files from both a conventional computer using a USB connector or from a device such as a cellular telephone with a micro USB connector. Examination of SANTIAGO GOMEZ's thumb drive revealed that it contained approximately

1,763 videos, 2,161 pictures and 88 unknown files. The files on the thumb drive were arranged into the following file names: Asian; Black; Boy; Latina; MOM, Pictures, Unorganized and White. I viewed each of the images described below – one from each of the above listed files on SANTIAGO GOMEZ's thumb drive and, based upon my training and experience, believe each of the below described videos to contain child pornography. The children in the below listed chart, appear to range in age from toddlers to young adolescents. It should be noted that videos and images of what were clearly infants, being sexually assaulted appeared on both SANTIAGO GOMEZ's cell phone and thumb drive. For the videos listed below, law enforcement is aware of the file name and path associated with each video.

FILE FOLDER	DESCRIPTION
Asian	Video of a young, pre-pubic, Asian female being sexually assaulted and digitally penetrated by what appears to be an adult male
Black	Video of a black minor female getting into the shower and digitally penetrating her vagina
Boy	Video of two Hispanic male minors, performing oral sex on each other
Latina	Video of a Hispanic minor female lying on her back with her vaginal area exposed as she digitally penetrated her vagina
White	Video of a white minor female displaying her unclothed anus and vaginal area.
Mom	Video of an adult female performing oral sex on a young pre-pubic Hispanic male
Unorganized	Video of a pre-pubic Asian female showing her vaginal area a while male digitally penetrated her

17. FBI personnel analyzed the thumb drive (flash drive) using the FBI's Loose Media Kiosk to obtain the "MD5 hash values" for each file. A "hash value" is shorthand for cryptographic hash function value. Hash values are used to identify with extreme precision almost any digital file, including but not limited to a movie file, still image file, word processing document or even the entire contents of a computer hard drive. Hash values are obtained through the use of a mathematical algorithm that maps data of arbitrary size (*e.g.*, a 1 MB image file or a 1 GB movie file) to a bit string of a fixed size (which is a hash value). The hashing

function is designed to be a one-way function, that is, it is impossible to invert that function and create the original file from the hash value itself. If an original file remains unaltered then the hash value is replicable, *i.e.*, repeatedly hashing the same original file using the same hash algorithm will produce the same value. However, if the original file has been altered in even a miniscule way, such as cropping a digital photograph to remove even one or two pixels, then the resultant hash value will be completely different. Examples of hash algorithms include the SHA-1, which produces a 40-character hexadecimal formatted hash value (an example of which might be "2fd4e1c67a2d28fced849ee1bb76e7391b93eb12"), and the MD5, which produces a 32-character hexadecimal formatted hash value (an example of which might be "79054025255fb1a26e4bc422aef54eb4"). An MD5 hash value has been referred to as a digital finger print.

18. These MD5 hash values were sent to the National Center for Missing and Exploited Children ("NCMEC") to be compared against known hash values associated with identified child pornography. SANTIAGO GOMEZ's thumb drive contained a total of 4,012 hash values, comprised of:

a. 873 files which were positively identified by NCMEC as known child pornography, that is, the unique MD5 hash values obtained from the files on SANTIAGO GOMEZ's thumb drive matched the unique MD5 hash values of known images and files of child pornography (from fully identified child victims) on file at NCMEC.

b. 1,379 files were known or recognized hash values. Although not dispositive with respect to the determination regarding whether such files contain child pornography, a recognized hash value indicates that the file was previously

submitted by law enforcement officers to NCMEC in conjunction with another investigation but which do not as of yet correspond to an identified child victim.

c. 1,760 unrecognized hash values. Even when a file appears to contain child pornography, it may have an unrecognized hash value for various reasons, including that the file may not have previously been seen or identified as child pornography, or an original known file (with an identified victim) may have been modified in a way that changed the hash value (*e.g.*, cropping a photograph).

19. On March 29, 2018, law enforcement analyzed defendant CARLOS SANTIAGO GOMEZ's Google Pixel 2XL cellular telephone, MSISDN: XXX-XXX-8976, IMEI: 358034085686779 and IMSI: 311480378283903 with the Cellebrite tool and UFED Physical Analyzer. I am aware that not all phones and applications are fully analyzed by the Cellebrite tool, but rather the Cellebrite tool extracts more data from some phones than others. SANTIAGO GOMEZ's Google Pixel phone contained only nine categories of Cellebrite extractable data: Calendar, Call Log, Contacts, Device Locations, MMS Messages, SMS Messages, Audio, Images and Video.

20. I reviewed the images from SANTIAGO GOMEZ's cell phone, which contained approximately 15,414 images. Based upon my training and experience, in excess of 1,000 images are child pornography. I also reviewed the 475 videos on SANTIAGO GOMEZ's cell phone, and based upon my training and experience believe that more than 100 of those videos contain child pornography.

21. Due to the volume of flash drives, computer devices and/or hard drives recovered from SANTIAGO GOMEZ's residence, law enforcement are still conducting forensic examinations.

22. Based upon my education, training, and experience, and my discussions with other law enforcement officers and my review of the evidence, the images described in paragraphs 4 and 16 *infra*, were shipped and transported in and affecting interstate or foreign commerce, including by computer.