



**ATTACHMENT A**

**Count One**  
**(Receipt of Child Pornography)**

From on or about December 30, 2018 through on or about March 7, 2019, in Ocean County, in the District of New Jersey and elsewhere, the defendant

**CHARLES F. BROWNE, JR.**

did knowingly receive child pornography, as defined in Title 18, United States Code, Section 2256(8)(A), that had been mailed, and using any means and facility of interstate and foreign commerce, shipped, and transported in and affecting interstate and foreign commerce by any means, including by computer.

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

**Count Two**  
**(Concealment of Objects to Impede a Federal Investigation)**

On or about April 8, 2019, in Ocean County, in the District of New Jersey, the defendant

**CHARLES F. BROWNE, JR.**

did knowingly alter, conceal, and cover up a record, document, and tangible object with the intent to impede, obstruct, and influence the investigation and proper administration of a matter that the defendant knew was within the jurisdiction of the Federal Bureau of Investigation, an agency of the United States.

In violation of Title 18, United States Code, Section 1519.

## **ATTACHMENT B**

I, Monica Cueto, am a Special Agent with the Federal Bureau of Investigation ("FBI"). I am fully familiar with the facts set forth herein based on my own investigation, my conversations with other law enforcement officers, and my review of reports, documents, and items of evidence. Where statements of others are related herein, they are related in substance and part. Because this complaint is being submitted for a limited purpose, I have not set forth each and every fact that I know concerning this investigation. Where I assert that an event took place on a particular date or time, I am asserting that it took place on or about the date or time alleged.

### **Dropbox Account**

1. On or about September 18, 2017, the cloud storage service provider Dropbox, Inc. ("Dropbox") noticed that approximately three images and sixty-three videos depicting child pornography (the "Illegal Files") had been uploaded to a Dropbox account created under the screen name "Charles Browne," and using the email address "cbrowne651@gmail.com" (the "cbrowne651 Email Account") (the "Charles Browne Gmail Dropbox Account").

2. The FBI opened an investigation into the child pornography activity involving the Charles Browne Gmail Dropbox Account upon learning of the Illegal Files and obtained the Illegal Files from Dropbox via search warrant.

3. Records obtained from Google reflect that the account subscriber for the cbrowne651 Email Account was "Charles Browne," with a listed recovery email account of "aljokr@aol.com" (the "aljokr Email Account").

4. Two of the images of child pornography obtained from the Charles Browne Gmail Dropbox Account did not match any known child pornography images or videos, as of in or about September 2017 (the "Unidentified Produced Images"). Metadata for the Unidentified Produced Images indicates that they were produced on or about August 21, 2017 with an Apple iPhone 5c. The Unidentified Produced Images were uploaded to the Charles Browne Gmail Dropbox Account on or about August 22, 2017.

5. Records obtained from Dropbox during the FBI's investigation reflect the following:

a. The Charles Browne Gmail Dropbox Account was created on or about December 12, 2015. The account had mobile information from a login on or about September 17, 2017 from an Apple iPad device.

b. The Charles Browne Gmail Dropbox Account contained approximately 110 videos that law enforcement determined depict child pornography, including the following:

i. A file containing a video approximately 15 seconds in length that depicts a naked prepubescent female child approximately four years old, with the focus on the child's naked chest and exposed genitals. The words "FUCK ME" with an arrow pointing to the child's genitals are drawn on the child's torso. The video depicts the child's vagina being penetrated by an adult penis.

ii. A file with a title that contained the phrase "5yo\_[REDACTED]\_get\_Cum\_in\_face," which contains a video approximately one minute, 4 seconds in length. The video depicts a naked prepubescent female child approximately four or five years old. The child appears to be lying on her back while an adult male penis hovers over her while masturbating over the child's chest and face. The child's genitals are exposed for a portion of the video. The video depicts the adult male penis penetrating the child's mouth and ejaculating into the child's mouth and on her face.

c. The Charles Browne Gmail Dropbox Account contained the two Unidentified Produced Images ("Image 1" and "Image 2"), which law enforcement determined depict child pornography and are described below:

i. Image 1 contains "Aug21" in the title. The image depicts a prepubescent female child who is unclothed and exposed. The image displays the child's upper thigh and buttocks, with the genitalia and anus exposed and the focus of the image. The child's anus is penetrated by what appears to be an adult's index finger.

ii. Image 2 also contains "Aug21" in the title. The image also depicts a prepubescent female child who is unclothed and exposed—possibly the same female child portrayed in the image above. The child appears to be bent over at the waist and the focus of the image is the child's genitals and anus, which are exposed.

d. In total, the Charles Browne Gmail Dropbox Account contained approximately 302 videos, 7 images, and two word documents. In addition to the child pornography referenced above, the account contained other videos and images that depicted child erotica, adult pornography, and other material, along with two copies of a resume for Charles Browne, Jr. listing a phone number ending in 5747 (the "5747 Phone Number").

e. One day after Dropbox discovered that the Charles Browne Gmail Dropbox Account contained suspected child pornography, on or about September 18, 2017, a Dropbox account was opened using the a1jokr Email Account, with the listed subscriber name "John Dough." I know from my

training and experience that Dropbox typically disables an account when Dropbox discovers that an account contains suspected child pornography.

### **Records from Apple**

6. Records obtained from Apple reveal the following:
  - a. “Charles Browne” registered an iCloud account using the a1jokr Email Account (the “Charles Browne iCloud Account”).
  - b. On or about October 16, 2014, a black iPad bearing a serial number ending in F189 (the “F189 IPAD”) was registered with the Charles Browne iCloud Account.
  - c. On or about August 5, 2015, a blue iPhone bearing a serial number ending in G2DL (the “G2DL IPHONE”) was registered with the Charles Browne iCloud Account.
  - d. From approximately October 2017 to April 5, 2019—all following the closure of the original Charles Browne Gmail Dropbox Account—the Charles Browne iCloud Account either updated or re-downloaded the Dropbox mobile application—which provides users with access to Dropbox services—to electronic devices approximately 43 times.
  - e. On or about April 25, 2017, the Charles Browne iCloud Account downloaded the “Stuffit Expander” program via iTunes to an iPad device. Stuffit is a file extractor program that can compress and decompress zipped files. Stuffit can also be used as an internet-enabled file sharing system to, among other things, send and receive files.

### **Interview with Charles F. Browne Jr.**

7. On or about the early morning of April 8, 2019, law enforcement observed Browne as he left his residence at an apartment complex in Toms River, New Jersey (the “Apartment”) and drove west on Kettle Creek Road. Law enforcement pulled over Browne’s vehicle (the “Browne Vehicle”) at approximately 7:55 a.m. near the intersection of Kettle Creek Road and Sherwood Lane (“Location 1”), at which time Browne was approximately one mile from the Apartment. Browne exited the Browne Vehicle, entered a law enforcement vehicle, and was driven to a location approximately 286 feet from the Browne Vehicle (the “Location 2”). Browne was Mirandized and interviewed by law enforcement about the FBI’s ongoing child exploitation investigation. During the encounter, one of the agents identified as working for the FBI.

8. Following the interview with the FBI at Location 2, at approximately 8:50 a.m., law enforcement transported Browne back to Location 1. Browne

attempted to open the driver's side door of the Browne Vehicle, which was locked. Browne became agitated and began pacing back and forth and eventually began walking towards Kettle Creek Road. At the time he was dropped off, the car keys that were previously in the Browne Vehicle's ignition had been removed by a separate member of law enforcement.

9. On that day, Browne was wearing a black t-shirt and a long-sleeved dark colored shirt, black pants, and white tennis shoes. Browne's clothing appeared to be splattered with paint.

10. Surveillance video from a business near Location 2 depicts, at approximately 8:58 a.m., a white male wearing black clothing was walking east on Kettle Creek Road and crossed over Kettle Creek Road in the vicinity of the business. It appeared that the male continued walking east on Kettle Creek Road.

11. At approximately 9:00 a.m., a person observed a balding white man wearing baggy pants and a black backpack over one shoulder, standing near the corner of Bay Terrace Road and another street ("Street 1") talking on a cellphone. The man was observed walking towards a pier located just north of the intersection of Bay Terrace Road and Street 1 that extended from a sandy beach area approximately 70 feet into Kettle Creek, a coastal waterway (the "Pier"). The man then was observed at the end of the Pier between two pilings. A person then observed the man at the end of the Pier get down on one knee and place an item into the water. The man then walked back to the beach area, sat at the picnic table, and placed a backpack on the table.

12. Further surveillance video reflects that an individual who appears to be Browne, holding a travel mug, and carrying a black backpack was walking south on Bay Terrace Road between Street 1 and Kettle Creek Road at approximately 9:24 a.m.

13. At approximately 9:40 a.m., Browne arrived on foot at the Apartment with a black backpack and a travel mug. Previously, when Browne was interviewed by law enforcement and left at the Browne Vehicle, he did not have a black backpack or travel mug on his person. When asked where he obtained those items, Browne told law enforcement, in sum and substance, that the Browne Vehicle was an old car and that he was able to gain access to the locked vehicle by jiggling the door open.

14. It appears that, during the time period after his encounter with law enforcement but before his return to the Apartment, Browne gained access to the Browne Vehicle, removed items from the Browne Vehicle, and concealed those items by placing them in the water adjacent to the Pier.

15. Records from Apple reflect that, on the following day, on or about April 9, 2019, the Charles Browne iCloud Account was registered to a pink iPhone.

16. On or about April 12, 2019, the Ocean County Sherriff's Office deployed a drone at the end of the Pier and located an object of interest that appeared to have a hard edge.

17. The same day, on or about April 12, 2019, FBI divers were deployed to the area under the dock on the east side of a property located near the intersection of Bay Terrace Road and Street 1, Toms River, New Jersey. The divers recovered from Kettle Creek the F189 IPAD and the G2DL IPHONE, both previously registered with the Charles Browne iCloud Account.

### **Records Recovered from the Submerged Devices**

18. The FBI was able to recover records from the G2DL IPHONE, including the following:

a. The G2DL IPHONE was configured with the Charles Browne iCloud Account.

b. The MSISN assigned to the G2DL IPHONE was the 5747 Phone Number.

c. The G2DL IPHONE's Bluetooth records showed that the device had paired to an iPad with MAC address 98:B8:E3:AF:1A:DB. A MAC address is a hardware-specific serial number. The aforementioned MAC address is the Bluetooth MAC address of the F189 IPAD.

d. Beginning at approximately 8:54 a.m. on April 8, 2019, the G2DL IPHONE made outgoing phone calls to users whose names are consistent with Browne's family members, and one of those phone calls lasted approximately 5 minutes.

e. The following "chats" were saved in the G2DL IPHONE:

i. an iMessage at approximately January 9, 2019, containing a link to a website containing "gangbang\_strap-on" in the URL; and

ii. an iMessage addressing the recipient of the message: "Hello Charlie."

f. The saved locations within the G2DL IPHONE reflect that on April 8, 2019:



i. At approximately 5:53 a.m., the device was located at or near the Apartment;

ii. At approximately 8:33 a.m., the device was located at Location 1 (the location where the Browne Vehicle was pulled over); and

iii. At approximately 9:15 a.m., the device was located in or near a body of water directly north of Bay Terrace Road and Street 1.

g. The G2DL IPHONE contained emails to and from both the cbrowne651 Email Account and the aljoker Email Account.

h. The G2DL IPHONE last auto connected to a Wireless Network named "Roxy" on or about April 7, 2019, at 10:57 a.m. Law enforcement has learned through the course of the investigation that Browne's wife made reference to "Roxy" as a family pet.

i. The G2DL IPHONE had deleted web history reflecting that the following websites were visited:

i. A website containing the phrase "petiteteenspussy" in the URL;

ii. A website containing the title "XXX Virgin Teen Sector";

iii. A website containing the title "Shocking Young Porn";

iv. A website with the word "raped" and "girl forced to have a threesome" in the URL; and

v. A website containing the phrase "innocent tiny vaginas" in the URL.

19. The FBI also recovered records from the F189 IPAD, which contained the following:

a. The F189 IPAD contained emails involving both the cbrowne651 Email Account and the aljoker Email Account.

b. On or about December 15, 2016, the cbrowne651 Email Account sent a series of emails to someone who appears to have tried to scam Browne. This series of emails included user cbrowne651@gmail.com stating the following:

i. Let's meet at . . . so I can kill you and your family after I violate them. They will love it. I'm hung like a horse. I want that innocence. The yelling you will here [sic] will be happiness so what it it's mine.

ii. I plan to make them into adults. They will get prostate massages.

iii. You can meet me. . . I'll wait if you want to watch.

iv. It is true your little [nationality] baby is born to please me. Maybe I'll send the little lover to [country] to my family to make some extra cash when I'm done.

c. On or about August 15, 2017, Browne utilized the cbrowne651Email Account to respond to an email about setting up his payroll.

d. The web history records deleted but recovered from the F189 IPAD reflect that, on or about October 23, 2018, the F189 IPAD was used to visit, inter alia, a website containing the title "Today's PEDO Gallery." From my training and experience, I am aware that the term "PEDO" is shorthand for "pedophilia" and indicates content depicting child pornography.

e. On or about December 30, 2018, a zip file titled "[VICTIM]-10yo.zip" was downloaded to the F189 IPAD. The zip file contained a video file—also located on the F189 IPAD—titled "[VICTIM]-10yo.mp4." The video is approximately two minutes and forty-four seconds and contains what law enforcement believes to be child pornography. The video depicts underage female children, including prepubescent girls, in various stages of undress performing sexual acts, such as masturbation and oral sex. At the conclusion of the video, the following text appears: "Want more? I have a very large collection of videos. Get access to it! Open the file 'index.html' select the video and download." The F189 IPAD contained index files that contain the name "[VICTIM]-10yo.avi.zip/Videos/".

f. On or about January 17, 2019, a zip file containing the phrase "6-YO-PUSSY-HARD-FUCK" in the filename was unzipped onto the F189 IPAD using the StuffIt application. Law enforcement believes that this zip file contains child pornography. One video in the aforementioned file depicts twelve screen captures with what appear to be different scenes, durations, and multiple prepubescent female children performing a variety of sexual acts. Two of the screen captures contain email and Torchat addresses. Three of the screen captures appear to depict the same prepubescent girl, who is believed to be approximately eight to ten years old. In one of the screen captures, she is naked, laying on her left side, wearing a pair of black, fishnet thigh-high stockings. An adult's hands are observed spreading apart the child's buttocks, exposing her anus.

g. On or about January 21, 2019, a zip file containing the phrase “10YO-PUUSY-ANAL-HARD” was unzipped onto the F189 IPAD using the Stuffit application. The unzipped file contained a video approximately one minute and forty-one seconds in length which law enforcement believes depicts child pornography. The video depicts prepubescent female children being penetrated anally, orally, and vaginally by the penises and fingers of several adult men. At the conclusion of the video, instructions on how to access to more child pornography were displayed.

h. On or about February 12, 2019, an email was sent from the F189 IPAD using the aljoker Email Account to an email address with a .ru (Russian) domain name, requesting: “Please send any I like screaming & crying best when forced.”

i. On or about March 9, 2019, the web history records deleted from, but saved onto, the F189 IPAD reflect that the F189 IPAD visited, *inter alia*, websites containing the titles “7 Y.O [VICTIM] FUCKED AND SUCK COCK,” “5 Y.O. [VICTIM] HARD FUCKED BY DAD,” and “[Website] [VICTIM]5YO\_ANALFUCK.”

j. The iPad also contained screen capture taken on March 7, 2019. This type of screen capture is taken automatically by the Apple operating system—without input from the user—when certain events occur. The screenshot displayed a list of files that were being “shared with iTunes,” including, *inter alia*, the files containing the following in the file names:

- i. ![VICTIM]-10yo;
- ii. 10yo-puusy-anal-hard;
- iii. 6-yo-pussy-hard-fuck; and
- iv. little\_pussy\_hard\_fuck.

k. On or about April 6, 2019, the web history records deleted from, but saved to, the F189 IPAD reflect that the F189 IPAD visited, *inter alia*, a website containing the title “BANNED RUSSIAN P.T.H.C” I know from my training and experience that the initials “P.T.H.C.” commonly refers to “preteen hardcore,” which is a shorthand descriptor for penetrative, hardcore child pornography involving prepubescent children.

l. On or about April 7, 2019, the web history records deleted but recovered from the F189 IPAD reflect that the F189 IPAD visited, *inter alia*, websites titled “ILLEGAL CH!LD PORN COLLECTION (5-15),” and “Only Small Kids.”

m. The F189 IPAD also included emails sent to the cbrowne651Email Account relating to his lease at the Apartment on or about September 14, 2017 and April 2, 2019.

n. The saved locations within the F189 IPAD reflect that, on or about April 8, 2019:

i. At approximately 2:33 a.m. and 7:04 a.m., the device was located at or near the Apartment; and

ii. At approximately 9:06 a.m., the device was located in the water directly north of the intersection of Bay Terrace Road and Street 1.

20. In addition to the above, location data recovered from the F189 IPAD reflects that the last wireless network that the F189 IPAD connected to was wireless network "Roxy" at approximately 6:43 a.m. on April 8, 2019.

21. Based on my training and experience and knowledge of the investigation, I believe that the child pornography videos recovered from the F189 IPAD referenced herein traveled in interstate commerce and that Browne received that child pornography onto the F189 IPAD from the Internet.