UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

CASE NO. 16-CR-20075-UNGARO

UNITED STATES OF AMERICA

vs.

ANTHONY DARON JOHNSON,

Defendant.
_____/

FINDINGS OF FACT AND CONCLUSIONS OF LAW

This cause came before the Court on June 6, 2016 for a bench trial after the Defendant knowingly and voluntarily waived his right to a jury trial. By way of background, the Defendant is charged in a two-count indictment. Count I charges that on or about June 8, 2014, the Defendant knowingly distributed child pornography in violation of 18 U.S.C.§2252(a)(2) and (b)(1). Count II charges that on or about November 20, 2014, the Defendant knowingly possessed child pornography in violation of 18 U.S.C.§2252 (a)(4)(B) and (b)(2).

Findings of Facts

1. The Defendant admits to the knowing possession of child pornography in violation of 18 U.S.C. §2252(a)(4)(B) and (b)(2).

2. On or about June 8, 2014, law enforcement, using investigative software, identified a computer on the ARES peer-to-peer (P2P) file sharing network with IP address 108.209.170.109 ("IP Address 109") listed as sharing at least thirty-seven files with hash values of images (including videos) matching the hash values of files known to law enforcement to contain child pornography.

AUTHENTICATED U.S. GOVERNMENT INFORMATION GPO

3. These file names included: ! 13y getting fucked by horny man.mpg; ! new ! (pthc) [name redacted] 8yr – fucking with daddy every day – may (2) .wmv; (moscow) 12-14y girls first experience (14 31).mpg; (pthc) 11y [name redacted] dad webcam (29 59).mpg; and ! new ! (pthc) 2006 [name redacted] 7yr masturbates and dad fingers ass.avi.

4. ARES employs a form of segmented file transfer whereby, upon the request of the user, a computer program downloads different portions of a file from various sources simultaneously and assembles the file on the user's destination computer data storage device. The file destination for ARES downloads is, by default, a "shared folder." In order to use ARES an individual must log-in and, once logged in, the program continues to run "in the background" giving other ARES users access to downloaded files in the "shared folder" unless and until either the user logs-off, changes the settings, or moves the file(s) from the "shared file" to another file on the destination device.

5. On or about June 8, 2014, law enforcement successfully downloaded one complete file and one partial file from the "shared file" at a device located at IP Address 109." In order to do so, the agents used ARESLE, a special software program used by law enforcement, that allows law enforcement to download from one user at a time, rather than portions from various computer files in various locations.

6. The complete file downloaded by law enforcement on June 8, 2014 was entitled "2.avi" and contains an approximately eighteen minute video that depicts a female under the age of eighteen sitting in front of a webcam wearing a shirt and boxer shorts with a blanket covering her lap. A small dog is sitting with the girl and she appears to be holding a can of something similar to cheez-whiz. At one point during the video the girl removes her boxer shorts so that she is naked from the waist down underneath the blanket. Eventually the girl removes the

blanket from her lap and begins spreading the food product on her vagina. The small dog then begins to lick the food product off of the girl's vagina. This activity is repeated multiple times and the girl appears to be intermittently typing on the computer keyboard during this activity.

7. The incomplete file downloaded by law enforcement on June 8, 2014 was entitled "!!!cum compilation 10 anos.avi" and contains a video that is a compilation of numerous short clips from multiple child pornography videos. One clip depicts a naked pre-pubescent female dancing erotically on a bed. Multiple clips within the video show naked female children under the age of twelve performing oral sex on adult males. Another clip within the video shows a pre-pubescent female laying on a bed masturbating. Two clips within the video depict naked pre-pubescent female children tied up and forced to perform oral sex on an adult male and being masturbated by an adult male.

8. The investigation revealed that the IP Address 109 is registered to AT&T Internet Services.

9. Business records from AT&T show that IP Address 109 was registered to an adult male ("Subject 1") residing at 9730 SW 162nd Street, Miami, Florida 33157 (the "Residence") on the date law enforcement downloaded the above-described child pornography videos.

10. On November 20, 2014, law enforcement executed a federal search warrant at the Residence and seized several electronic devices, including a Dell laptop computer (model number PP05XB, service tag DKV79C1) ("Dell Laptop"), from the Defendant's bedroom.

November 20, 2014 Interview of the Defendant

11. On November 20, 2014, law enforcement interviewed the Defendant at his place of employment.

12. The Defendant stated that he moved into the Residence in February 2014.

13. The Defendant stated that he had a laptop computer located in his bedroom, but that it broke at the beginning of the summer.

14. The Defendant stated that he used that laptop computer to access the internet via the Wi-Fi at the Residence.

15. The Defendant stated that he used ARES, a file sharing program, to search for adult pornography, but that ARES would sometimes give him child pornography instead.

16. The Defendant admitted that these child pornography downloads from ARES onto his laptop computer occurred sometime in the summer of 2014.

17. The Defendant admitted that over the few weeks or months that he downloaded adult pornography from ARES, he received approximately eighteen (18) videos and four or five photos of child pornography.

18. The Defendant admitted that the children in the videos were toddlers and older and the children in the pictures were between 12-16 years old.

November 26, 2014 Interview of the Defendant

19. On November 26, 2014, the Defendant was interviewed at the Homestead Resident Agency of the FBI.

20. The Defendant was advised of his *Miranda* rights and waived them in writing.

21. The Defendant stated that, in approximately 2000, he began using the LimeWire, a file sharing program.

22. The Defendant admitted that any search for pornography that was conducted on LimeWire resulted in some child pornography.

23. The Defendant stated that he learned how to locate files on his computer that he downloaded from LimeWire as well as how to specify a particular location for the downloaded files.

24. The Defendant admitted that on approximately 20 occasions he viewed child pornography on the ARES program.

25. The Defendant admitted that he knew that, when he was using LimeWire, he was sharing files that he downloaded with other LimeWire users.

26. The Defendant stated that he knew that if he was sharing files on LimeWire it would slow the amount of time it would take him to download a file.

27. The Defendant stated that he modified the setting on LimeWire so that he would not be sharing files.

28. The Defendant stated that, in approximately 2010, he began using the ARES program.

29. The Defendant admitted that he knew that whatever files he downloaded on ARES could be available to other ARES users.

30. The Defendant stated that on ARES, he would type a term in the search box, the results would populate, then he would choose the files to download.

31. The Defendant admitted that during the download he was able to preview what he was downloading prior to completion.

32. The Defendant admitted that if the download contained content he did not want, he was able to cancel the download.

33. The Defendant admitted that he was able to view the downloaded content through the ARES program or the destination folder.

34. The Defendant admitted that he had the ability to locate the destination folder and delete downloaded content.

35. The Defendant stated that while he would search the ARES program for movies, and some music, he also searched for a "shitload of porn."

36. The Defendant admitted that, he would type the search terms "stpenisburg" and "pthc" into the search box on ARES.

37. "Pthc" stands for pre-teen hardcore, and that is a commonly used search term by individuals seeking child pornography on the internet.

38. The Defendant stated that those search terms would always result in videos of child pornography.

39. The Defendant admitted that he had seen child pornography videos made up of children in every age range, and had seen videos depicting children being molested vaginally, anally and orally.

40. The Defendant admitted to viewing the Vicky series of child pornography videos.

41. The Defendant specifically admitted that he viewed a video of a girl spreading Cheez Whiz on her vaginal area and letting a Chihuahua lick it off.

42. The Defendant admitted that while he did not initially try to configure the ARES settings, eventually he restricted the program to only download one video at a time in order to reduce his download time.

43. The Defendant stated that he left ARES running in the background and by doing so, allowed other ARES users to download content that was in the shared folder on his computer.

44. The Defendant admitted that he was aware that child pornography was being downloaded to the shared folder on his computer, and subsequently being made available for other ARES users to upload.

45. The Defendant stated that he knew that child pornography was illegal.

Forensic Review of the Defendant's Laptop

46. On August 8, 2015, FBI Forensic Examiner Thomas Agrait examined the Dell Laptop that was seized on November 20, 2014 from the Defendant's bedroom.

47. The forensic review established that the ARES P2P program had been installed on the Dell Laptop.

48. The Dell Laptop's registry report showed that, among others, the following search terms had been entered into the ARES program: 12y sweety gets fucked; Sweety gets fucked; 12y; 12y sweety dad;12y sweety; Daddys girl; Pthc; Vicky; Hussyfan; Tiny4k; Tiny girl with glasses; Tiny girl; Tiny; Petite; Pthc high school; Ptch 2014; Pthc 2013; Pthc new; One girl; and teen.

49. The forensic review established that between May 23, 2012 and September 21, 2014, the Defendant downloaded from ARES approximately 341 files with titles indicative of child pornography.

50. The forensic review established that the Defendant modified the settings for three files, with titles indicative of child pornography, to prevent them from being shared with other ARES users.

51. The forensic review established that the Defendant did not modify the settings for 338 files, with titles indicative of child pornography, thereby allowing them to be shared with other ARES users.

52. During the forensic review, law enforcement located over 200 still images of child pornography and three videos described below:

a. a file entitled "Arestra_1st studio hd_125 (pthc 2012).avi" contains a video of two females under the age of eighteen wearing only their panties. The females are depicted on a bed kissing. Both females then remove their panties and continue kissing;

b. a file entitled "snowl vichatter girl 1 pussy 2011~1.avi" contains a video that is approximately five minutes long and depicts a pre-pubescent female who is exposing her breasts. The young girl then begins removing her pants enough to expose her vagina. The young girl then proceeds to masturbate for the duration of the video; and

c. a file entitled "chica ebria cojida.mpg" contains a video that is approximately three minutes and thirty seconds long and depicts a naked female under the age of eighteen laying naked on a bed. A naked adult male then enters the video and begins having intercourse with the female for the duration of the video.

Conclusions of Law

Count II (Possession)

Based on the totality of the evidence as set forth above and the Defendant's admission of guilt, the Defendant is guilty of knowing possession of child pornography in violation of 18 U.S.C. §2252(a)(4)(B) and (b)(2) as charged in Count II of the Indictment.

Count I (Distribution)

In Count I the Defendant is charged with knowingly distributing child pornography on June 8, 2014 in violation of Title 18, United States Code, Sections 2252(a)(2) and (b)(1). To prove this offense, the United States must establish beyond a reasonable doubt that:

(1) the defendant knowingly distributed a visual depiction (*i.e.*, the child pornography files);

(2) the depiction was transported in interstate of foreign commerce by any means, including computer;

(3) producing the visual depiction involved using a minor engaged in sexually explicit conduct;

(4) the depiction is of a minor engaged in sexually explicit conduct; and

(5) the defendant knew that at least one performer in the visual depiction was a minor and knew that the depiction showed the minor engaged in a sexually explicit conduct.

Eleventh Circuit Pattern Jury Instructions, Offense Instruction 83.2 (2010).

The United States and the Defendant have entered into a joint stipulation that satisfies three of the five elements, specifically 2,3 and 4. In that regard, the parties stipulated that on June 8, 2014, agents of law enforcement located in the State of Oklahoma were able to access and cause to be transported by computer, over the Internet, through the ARES peer-to-peer file sharing program, in or affecting interstate commerce, visual depictions from a computer that was using an Internet Protocol Address assigned to 9730 SW 162nd St. in Miami Florida to a computer in the State of Oklahoma. Further, the parties stipulated that these visual depictions were of minors engaging in sexual explicit conduct and the production of which involved using a minor engaged in sexually explicit conduct. Additionally, the Defendant admitted when interviewed that he knew the video downloaded by law enforcement on June 8, 2014 depicted a minor engaged in sexually explicit conduct, satisfying the fifth element above. Consequently, the only disputed element is whether the Defendant "knowingly distributed" a visual depiction of child pornography.

The defense argued that the United States failed to prove knowing distribution because "to distribute" means, as stated in the Eleventh Circuit Pattern Jury Instructions, Offense Instruction 83.2 (2010), "...to deliver or transfer possession of it to someone else, with or without any financial interest in the transaction." According to the defense, the evidence showed only that the Defendant passively maintained the child pornography in the "shared file" and that

such passive activity is insufficient to show transfer of possession citing to *United States v. Husman,* 765 F.3d 169 (3d Cir. 2014).

In *Husman,* 765 F.3d 169, the Third Circuit relied on the dictionary definitions of "distribute," the fact that Congress has legislated specific prohibitions against offering and promoting child pornography within the same statutory scheme in which it prohibits distribution of child pornography, and the use of the term "distribute" in other criminal law contexts, to hold that "distribute" in §2252(a)(2) should be narrowly construed and requires proof that a defendant's child pornography materials were completely transferred to or downloaded by another person. *Id.* at 176. Relying on that construction, the Third Circuit reversed the defendant's conviction for distribution of child pornography and remanded for resentencing because the Government had failed to introduce evidence that anyone downloaded child pornography from Husman's shared folder. *Id* Notably, the Third Circuit did not reverse based on lack of evidence of "knowing" distribution – it reversed on lack of evidence that child pornography images had actually been transferred.

Other appeals courts have ascribed more or less the same narrow meaning to "distribute", but have affirmed convictions for distribution of child pornography where the defendant, similar to the Defendant herein, maintained a "shared file," had a demonstrated familiarity with and history of using peer-to peer file sharing to obtain child pornography, and law enforcement was able to download images of child pornography from the shared destination file. *See United States v. Shaffer,* 472 F.3d 1219 (10th Cir. 2009)(construing "distribute" in accordance with dictionary definitions and affirming conviction for distribution where the defendant downloaded approximately 10 gigabytes of child pornography from a peer-to peer network, and law enforcement was able to download images of child pornography without difficulty); *United*

States v. Richardson, 713 F.3d 232 (5th Cir. 2013)(affirming conviction under §2252(a)(2) where defendant downloaded images and 144 videos containing child pornography from a peer-to-peer computer network and stored them in a shared file from which law enforcement was able to download a video containing child pornography); *United States v. Chiaradio*, 684 F.3d 265 (1st Cir. 2012) (construing "distribute" in §2252(a)(2) in accordance with its dictionary meaning and affirming conviction where defendant downloaded over 5000 images and videos of child pornography, and law enforcement using a modified program was able to download a file from the defendant's computer that contained child pornography. The modified program allowed agents to download a file from a single source).

These cases are consistent with the proposition that fact-finders can infer that users of a peer-to-peer program have a general understanding that they allow file sharing over the internet. *See, e.g., United States v. Creel*, 783 F.3d 1357 (11th Cir. 2015). The Eight Circuit in *United States v. Dodd*, 598 F.3d 449 (8th Cir. 2010) noted, "absent concrete evidence of ignorance-evidence that is needed because ignorance is entirely counterintuitive-a fact-finder may reasonably infer that the defendant knowingly employed a file sharing program for its intended purpose." *Dodd*, 598 F.3d at 452. Such a permissible inference holding comports with commonsense. Thus, in *United States v. Shaffer,* 472 F.3d 1219, 1223-24, the Tenth Circuit had "little difficulty" in concluding the defendant distributed child pornography by freely allowing access to his computerized stash of images and videos and thereby openly inviting them to take, or download, those items. The Court highlighted the fact that the defendant admitted he had downloaded child pornography from other users' shared files and understood that file sharing was the very purpose of the peer-to-peer program , that he admitted to having child pornography in his computer's shared folder, that the defendant could have, but did not, save the images in a

folder not susceptible to sharing and that he could have, but did not activate a feature that would have blocked others for the shared file.

This Court has carefully reviewed the above-cited authorities and like the Tenth Circuit concludes that for the purposes of 18 U.S.C.§2252(a)(2) an individual has knowingly distributed child pornography if he or she maintains a "shared destination file," has a reasonably sophisticated understanding of peer-to-peer file sharing for the purpose of obtaining child pornography, and law enforcement actually downloads images of child pornography from that file using the peer-to peer-file sharing program.

In this case, the United States proved beyond a reasonable doubt the Defendant's knowing distribution by three methods:

First, on November 26, 2014, the Defendant made several statements admitting that he was aware that he was distributing child pornography to other users of the ARES program. For instance, the Defendant admitted that he left ARES running in the background and by doing so, allowed other ARES users to download content that was in the shared folder on his computer. Further, the Defendant admitted that he was aware that child pornography was being downloaded to the shared folder on his computer, and subsequently being made available for other ARES users to upload. In sum, the Defendant admitted that he knew that child pornography was illegal, that he downloaded child pornography, and that he made child pornography available for other ARES users to download from him.

Second, beyond the Defendant's explicit and specific admissions as to his knowing distribution, his sophisticated knowledge of the ARES program as well as other shareware programs establishes his knowing distribution of child pornography. Among other things, during his November 26, 2014 interview, the Defendant admitted that he previously used LimeWire, he

was aware that he was sharing files that he downloaded with other LimeWire users. Further the Defendant admitted that he had modified the setting on LimeWire to limit the numbers of file he was sharing in order to more quickly download material. Similarly, during this interview, the Defendant admitted that while he did not initially try to configure the ARES settings, eventually he restricted the program to only download one video at a time in order to reduce his download time. Further, the Defendant admitted that he developed the ability to locate the destination folder and delete the downloaded content through shortcut commands. The Defendant's proficient knowledge is further demonstrated by the forensic review which established that he actively modified the settings on three files, with titles indicative of child pornography, to prevent their distribution to other users. The forensic review further established that the Defendant did not modify the settings for 338 images of child pornography, thereby allowing them to be distributed to other users of the ARES program.

Third, the forensic review of the Defendant's Dell Laptop revealed that, from May 2012 through September 2014, the Defendant was actively and prolifically downloading child pornography from other users of ARES. In fact, of the 551 complete files that the Defendant downloaded from the ARES program, 341 files were indicative of child pornography. The Defendant's extensive ARES use establishes that the Defendant knew that child pornography was being delivered and transmitted from his shared file..

In sum, the United States proved beyond a reasonable doubt that the Defendant used ARES to maintain a shared file that was a destination for child pornography, that the Defendant had a history of using peer-to-peer networks to obtain child pornography, that the Defendant knew how to manipulate ARES to terminate sharing, that the Defendant understood how the "shared file operated to allow others access to his cache of child pornography and that law

enforcement downloaded a video containing child pornography on or about June 8, 2014. Accordingly, the United States proved "knowing distribution" within the meaning of 18 U.S.C. §2252(a)(2).

Finally, the Court acknowledges that she voiced some concern at the conclusion of the bench trial with the Government's use of the modified program. However, the Court can readily infer from the evidence that that if the Government had used a non-modified program, the agents would still have been able to download the same images, albeit in re-aggregated form, and therefore, the use of the modified program is an immaterial consideration. [1]

ACCORDINGLY, for all the reasons set forth above, the Court finds and concludes that the Defendant knowingly possessed child pornography in violation of Title 18, United States Code Sections §2252(a)(4)(B) and (b)(2) on November 20, 2014 as charged in Count II and that the United States established that the Defendant knowingly distributed child pornography on June 8, 2014, in violation of Title 18, United States Code, Sections 2252(a)(2) and (b)(1) as charged in Count I, and that therefore the Defendant is guilty of Counts I and II of the Indictment.

DONE AND ORDERED this 8th day of June, 2016 at Miami, Florida.

DISTRICT JUDGE

cc. Counsel of Record

[1] *See, United States v. Budziak*, 697 F.3d 1105 (9th Cir. 2012) vacating conviction for distribution of child pornography and remanding for a determination whether the defense should have been provided with materials relevant to the modified program that the FBI used to download child pornography from the defendant's computer. Among other claims, the defense asserted that the FBI might have only downloaded fragments of child pornography files making it "more likely" that he did not knowingly distribute any complete child pornography files to the agents.