IN THE COURT OF COMMON PLEAS OF LYCOMING COUNTY, PENNSYLVANIA

COMMONWEALTH OF PENNSYLVANIA	:	
	:	**CR-191-2015**
v.	:	
	:	
ERIC GREEN,	:	**CRIMINAL DIVISION**
Defendant	:	

OPINION AND ORDER

On April 24, 2016, the Defendant filed an Omnibus Pretrial Motion in the form of a Motion to Suppress. A hearing on the motion was held June 30, 2016.

I. Background

On December 28, 2014, Corporal Gerald Goodyear (Goodyear) of the Pennsylvania State Police (PSP) Computer Crimes Unit was conducting undercover investigations into the sharing of child pornography on the internet. He was able to locate a computer that was sharing child pornography using the BitTorrent file sharing network. Bit Torrent is a communications protocol of peer-to-peer file sharing (P2P) used to distribute music and electronic files over the internet. To send or receive files, the user must use a "client" on his internet-connected computer. A BitTorrent client is a computer program that implements the BitTorrent protocol. The computer was making use of the uTorrent 3.3 client software. File sharing software is designed to upload/download to and from other users simultaneously. Goodyear was able to download contraband digital files from the computer one of which was viewed and determined to be an image of a nearly naked prepubescent girl. On the image in the upper left hand corner was depicted a company identifier "LS Island".

Once the image was determined to be contraband, the IP or internet protocol address was then identified and the internet service provider was determined. The IP

address was assigned to Comcast Cable Communications. On January 9, 2015, a court order was obtained for subscriber information from Comcast identifying Eric Green (Defendant) as the subscriber with a physical address located at 105 N. 5th Street, Apartment 7, Hughesville, PA. Subsequently on January 15, 2016, PSP obtained and executed a search warrant on the Defendant's residence.

PSP met the Defendant at his residence in Lycoming County, read him his *Miranda*[1] warnings and he was willing to speak. He acknowledged owning a Samsung Galaxy Note 2 and that he had the uTorrent client software installed on the device. He also said that only he had use of the phone and owned it since October of 2014. Upon examination of the phone, four (4) additional similar images were observed on the device with two (2) having the same "LS Island" logo. On January 15, 2015, PSP filed a criminal complaint against Defendant charging him with 4 counts each of Sexual Abuse of Children[2] and Criminal Use of a Communication Facility[3]. Defendant was arrested on January 15, 2015, and he waived his preliminary hearing on January 23, 2015. On March 15, 2016, the information by agreement of the parties was to amend an additional 96 counts of each offense.

Warrant to search violated the Defendant's rights as it is overbroad

Defendant alleges that the search warrant obtained by PSP is overbroad in that it permits the police to seize and analyze and search any and all electronic equipment which would be used to store information "without limitation to account for any non-criminal use" of said equipment. Defense believes that to allow the police to search any

[1] Miranda v. Arizona, 384 U.S. 436, 86 S.Ct. 1602, 16 L.Ed.2d 694 (1966).
[2] 18 Pa. C.S. Section 6312(d).
[3] 18 Pa. C.S. Section 7512 (a).

and all files on the electronic device regardless of whether the files were used for criminal or noncriminal purposes is unduly broad.

"[N]o Warrants shall issue, but upon probable cause . . . and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. Amend. IV. "[N]o warrant to search any place or to seize any person or things shall issue without describing them as nearly as may be, nor without probable cause..." Pa. Const. Art. I § 8. In Orie, the Pennsylvania Supreme Court explained the "as nearly as may be" requirement of Article I, Section 8:

> It is a fundamental rule of law that a warrant must name or describe with particularity the property to be seized and the person or place to be searched…the particularity requirement prohibits a warrant that is not particular enough and a warrant that is overbroad. A warrant unconstitutional for its overbreadth authorizes in clear or specific terms the seizure of an entire set of items, or documents, many of which will prove unrelated to the crime under investigation. An overbroad warrant is unconstitutional because it authorizes a general search and seizure. Consequently, in any assessment of the validity of the description contained in a warrant, a court must initially determine for what items probable cause existed. The sufficiency of the description must then be measured against those items for which there was probable cause. Any unreasonable discrepancy between the items for which there was probable cause and the description in the warrant requires suppression. An unreasonable discrepancy reveals that the description was not as specific as was reasonably possible.

88 A.3d at 1002-03 (quoting Commonwealth v. Rivera, 816 A.2d 282, 290-291 (Pa. Super. 2003)).

Defense counsel cites to Commonwealth v. Orie[4] and Commonwealth v. Melvin[5] to support the position of overbreadth. In Orie, the police thought that they would find evidence of a crime in a flash drive belonging to Defendant. The Superior Court held that the warrant was over broad because it sought "any contents contained within the flash drive without limitation to account for any noncriminal use of the flash drive." 88

[4] 88 A.3d 983 (Pa.Super 2014).
[5] 103 A.3d 1 (Pa. Super 2014).

A3d. at 1008. The police also believed that evidence of criminal activity would be found in messages contained within an email account managed by the Defendant and obtained a search warrant for "all stored communications and other files between August 1, 2009, to the present..." Id. at 1005-1006. The Court also held that this request was overbroad because it "did not justify the search of all communications during that time period. Id. at 1008-9. The Court in Melvin also determined that warrants issued for the contents of email accounts were overbroad and did not account for any noncriminal activity.

In this case the search warrant sought only "evidence relating to the possession and/or distribution of child pornography." Unlike the cases cited by Defense Counsel, the Court is satisfied that the scope of the warrant was sufficiently narrow as to exclude evidence of non criminal behavior. Digital storage systems must be seized in their entirety and then searched at a later time. Orie at 1008. As the Affiant explained in the affidavit of probable cause supporting the application for the search warrant:

> searching computerized information for evidence or instrumentalities of a crime commonly requires investigators to seize all of the computer system's input/output peripheral devices, related software, documentation and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment.

The Court finds that in the context of electronic device searches that the search warrant was not overbroad and stated with particularity the purpose behind the seizure.

Warrant to search was issued without probable cause

Defendant also alleges that the warrant was issued without probable cause as the only information in the affidavit which establishes the possible location of the electronic device which may have been used was the IP address of the Defendant.

Defendant asserts that PSP is required to establish that the device used in the download was physically located at the location of the IP address. In addition, the Defense argues that since there was no information given to establish that the electronic equipment used to download the child pornography would be found within the residence at the time of the execution of the search warrant that device could be found anywhere. In addition, because the information provided does not identify the device used, it could have been someone accessing the internet using the Defendant's account from outside the residence.

Pa. R. Crim. P. 203 (D) sets forth the standard to determine whether probable cause exists to support issuance of a warrant; the court is confined to the four corners of the affidavit of probable cause attached to the warrant. The affidavit sets forth the pertinent portion:

> On December 28, 2014, at 0815 hours Corporal Goodyear was conducting undercover investigations into the Internet sharing of child pornography. He was able to locate a computer which was sharing child pornography on the BitTorrent file sharing network using client software which was reported as uTorrent 3.3. He determined that the user of this computer system configured his BitTorrent client software to "seed" files.
>
> Goodyear was subsequently able to download contraband digital files from this user. The downloaded files were viewed and one of them is described as follows:
>
> Name of file: I SM – 024–074.JPG
> Type of file: image
> Description: this image file depicts a prepubescent girl approximately 12 years old sitting on a rocky outcropping in front of an unidentified body of water. The girl has brown hair which is braided and is wearing a multicolored sheer piece of fabric and various bracelets on both wrists. She appears otherwise nude and has her legs spread so as to display her general area which is clearly visible. In the upper left corner of the image is printed a company logo "LS island".
>
> I have since viewed this file and agree with the description as provided by Corporal Goodyear.

Search Warrant issued January 14, 2015, MDJ Kemp.

The task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, including the 'veracity' and 'basis of knowledge' of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place.

Commonwealth v. Gray, 503 A.2d 921, 925 (Pa. 1985) (quoting Illinois v. Gates, 462 U.S. 213, 238 (1983)).

A reviewing court may not conduct a de novo review of the issuing authority's probable cause determination. The role of both the reviewing court and the appellate court is confined to determining whether there is substantial evidence in the record supporting the decision to issue the warrant.

Commonwealth v. Huntington, 924 A.2d 1252, 1259 (Pa. Super. 2007) (internal citations omitted).

Upon review of the information provided by Goodyear as set forth in the affidavit of probable cause, the Court finds that the photograph referred to in the affidavit gives the Commonwealth sufficient probable cause to search to believe that the photograph was downloaded to the IP address associated with the residence.

In addition, although there would be no guarantee that due to the portable nature of most computer devices, the actual device would be present within the residence, the device which contained the file sharing software was the Defendant's phone. Again, devices without the file sharing software would not be searched and/or seized as there would be no chance that the materials would be found within.

As for the theory that someone might have compromised Defendant's account the Court finds this argument without merit. The photos were downloaded by a device with an IP address belonging to Defendant. A warrant was issued to search Defendant's residence for any devices which would contain the photograph which was downloaded, or other child pornography. If after the execution of the search warrant, the PSP found no devices containing file sharing software and/or the photos in question,

the Defendant would not be charged with any offenses. Based upon the Court's knowledge of computers, if someone would have "tapped into" the Defendant's network and downloaded photos using the network it would not have automatically downloaded the documents onto every device that shares the network. Only the devices which initiated the download would contain those files. Defendant's phone contained both the file sharing software as well as the images described in the affidavit; Defendant also acknowledged that only he had access to the device. Therefore the Court is satisfied that no one else was using the Defendants network to cause these items to be downloaded onto Defendant's phone.

III. Conclusion

The Commonwealth had probable cause to search the Defendant's residence for electronic devices responsible for downloading the documents in question. The warrant was not overbroad. There is no evidence that anyone else could have used the network at Defendants residence which caused the photographs to be downloaded onto Defendant's phone without his knowledge.

ORDER

AND NOW, this _____ day of December, 2016, based upon the foregoing Opinion, it is ORDERED and DIRECTED that the Defendant's Motion to Suppress is hereby DENIED.

BY THE COURT,

Nancy L. Butts, P.J.

cc: Peter Campana, Esq.
Martin Wade, Esq.