IN THE COURT OF COMMON PLEAS OF LYCOMING COUNTY, PENNSYLVANIA

COMMONWEALTH OF PENNSYLVANIA	:	
	:	**CR-2117-2015**
v.	:	
	:	
MARCUS BOGDEN,	:	**OMNIBUS PRETRIAL**
Defendant	:	

OPINION AND ORDER

On April 5, 2016, the Defendant, Marcus Bogden, filed an Omnibus Pretrial Motion. The hearing was held on August 8, 2016. Briefs were submitted on the Motion to Suppress with the Commonwealth's response brief filed October 10, 2016.

Background

On October 7, 2015, Special Agent Brittany Lauck of the Pennsylvania Office of Attorney General's Child Predatory Unit was conducting an online investigation on the BitTorrent network for offenders sharing child pornography. Lauck located a computer that was sharing child pornography using the BitTorrent file sharing network. She directed her investigation specifically to IP (Internet Protocol) number 50.152.126.16 because it was associated with a torrent with an infohash that references 694 files, one of which was identified as being a file of investigative interest to her child pornography investigations. Lauck was able to download the file of investigative interest: lsv-018-077.jpg from IP address 50.152.126.12.[1] IP address 50.152.126.16 is referred to as the "suspect device" in Lauck's affidavit of supporting her request for a search warrant.[2]

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

[1] Commonwealth's Exhibit #2. lsv-018-077.jpg. The image downloaded by Lauck on October 7, 2015, from Defendant's laptop computer.
[2] Commonwealth's Exhibit #3. The search warrant with affidavit of probable cause and the receipt inventory.

user must use a "client" on his internet-connected computer. A BitTorrent client is a computer program that implements the BitTorrent protocol. The suspect device was making use of BitTorrent client software – BT9750-BitTorrent 7.9.5. File sharing software is designed to upload to/download from other users simultaneously. Users are not downloading a file from one location but rather download bits of files from various locations making download times faster. Unlike when private citizens are using BitTorrent to download files from various sources/locations, when law enforcement conducts searches of BitTorrent, they are able to download from one individual source only[3]. N.T. 12/11/2015 at 9. Additionally, law enforcement is able to determine the IP address associated with the download. Id.

IP numbers are a unique set of numbers consisting of four (4) parts separated by dots. The IP number identifies devices on the Internet/Network. Every device that connects to the internet has a unique IP number that can be used to track the location of the device. An IP address is associated with a specific modem. After Lauck was able to determine the IP address that was suspected of sharing child pornography, she checked which Internet Service Provider (ISP) was providing internet service to that device through the free online database available at http://www.arin.net. The Internet Service Provider to 50.152.126.16 on that date in question was Comcast Cable Communications.

Lauck completed an administrative subpoena directing Comcast Cable Communications to release subscriber, and other pertinent information regarding the user identified with the aforementioned IP address at the date, and time the image was downloaded. Comcast Cable Communications indicated in their response that

[3] Commonwealth's Exhibit #1. Transcipt of Preliminary Hearing held on December 11, 2015.

"Melinda Bogden" is the account holder and subscriber assigned to the IP address in question. Comcast also provided the service address of 70 E. Houston Ave. Montgomery, PA 17752. As such, Lauck's affidavit of probable cause states

that there is probable cause to believe that a use of the computer and or device located at **70 E. Houston Ave Montgomery Pennsylvania, 17752 Lycoming County** has evidence pertaining to an ongoing child exploitation investigation. Finally individuals involved in the possession and dissemination of child pornography… tend to maintain their collections at a secure private location for long periods of time. There is probable cause to believe that evidence of the offense of possessing child pornography as well as criminal use of communications facilities is currently located at **70 E. Houston Ave Montgomery Pennsylvania Lycoming County.**

The Application for Search Warrant identified the items to be searched and seized as "all computer hardware, including, but not limited to, any equipment which can collect analyze create display convert store conceal or transmit electronic, magnetic optical or similar computer impulses or date. Any computer processing units, internal and peripheral storage devices (such as fixed disks, external hard disks, discs, backup media, flash media, and optical storage device, peripheral input/output devices (such as keyboards, printers, scanners, video displays, switches and disc media readers), and related communication devices such as network Internet devices, cable and connections recording equipment as well as any devices , mechanisms or parts that can be used to restrict access to computer hardware. These items will be seized and later searched for **evidence relating to the possession and/or distribution of child pornography** [emphasis Courts own].

Other items requested to be seized were Software, Documentation, Passwords and Security Devices.

The Affiant explained that

searching and seizing information from computers often requires investigators to seize all electronic storage devices (along with related peripherals) to be searched later by a qualified computer expert in a laboratory or other controlled environment. This is true because

1. Computer storage devices and the like store the equivalent of hundreds of thousands of pages of information. A suspect may try to conceal criminal evidence in random order or with deceptive file names or deceptive file extension. This requires the search authorities to examine all the stored date to determine which particulars files are evidence of instrumentalities of crime. This sorting process can take weeks or months depending on the volume of data stored, and it is impractical to attempt a comprehensive data search on site.

2. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment.

On November 19, 2015, Agents of the Office of Attorney General executed the search warrant of 70 E. Houston Ave. Montgomery, Pennsylvania 17752. Present at the residence were Defendant and Tiffany Herb. Agents Hasenauer and Lauck spoke to Defendant in an upstairs of the bedroom of the residence. He was advised of his *Miranda*[4] warnings and agreed to speak with Agents without an attorney present.

Defendant advised the agents that he resided in the home as well as his parents, Timothy and Melinda Bogden, and his two adult sisters: Tiffany Herb and Breanna Bogden. Tiffany and her husband Sean live in the third floor of the residence. Defendant stated that no other individuals have lived or stayed for a prolonged period of time. He indicated that the family's Internet Service Provider was Comcast. He stated that the wireless signal was password protected. Agents confirmed that the wireless signal was password protected and Defendant indicated he did not give out the wireless internet password. He told that the Agents that he owns a computer, a tablet, and a phone. He stated that he had used the BitTorrent program in the past to download games but no longer did so no longer as his laptop had crashed. He denied ever downloading child pornography but indicated that he had searched the BitTorrent program for "lesbian" and teen". He indicated that other people living at the residence may have downloaded child pornography and though he had not downloaded child pornography, he may have seen child pornography.

Agents interviewed the other residents of the home. Tiffany and Breanna (Defendant's sisters) stated they do not use file sharing programs or their brother's

[4] Miranda v. Arizona, 384 U.S. 436, 86 S.Ct. 1602, 16 L.Ed.2d 694 (1966).

computer but that the family is very open about sex and sexuality. Sean Herb (brother-in-law) stated that he has a computer at the residence but rarely uses it. He denied using Defendant's computer or downloading anything to it. Lauck reiterated the substance of these interviews at the preliminary hearing.

Defendant's mother admitted that she uses a file sharing program called "Share bear" however she has never used it to download child pornography. Agents Goodrow and Lauck explained to Defendant's father (Timothy) that a search warrant was obtained for his residence because child pornography had been downloaded from someone located at the address. Timothy reiterated his family's openness towards sex and sexual preferences. He also denied using his son's computer to download anything. Agents questioned Timothy, Sean and Defendant in the same room. Timothy and Sean denied downloading child pornography and Defendant had no explanation as to how child pornography was on his computer.

Agent Zahm of the Computer Forensics Unit assisted with the on scene preview of the electronic storage devices at the residence. Zahm examined Defendant's Dell N5010 computer, which was located in the office of the residence. Zahm advised that Defendant's computer had the program for UTorrent installed. Zahm indicated that the IP address 50.152.126.16 matched his computer. Zahm identified 28 images of apparent child pornography at the time of the in home search. A preview of Defendant's cell phone, Samsung SCH-1200p, yielded search terms including "PTHC." He was arrested and charged with 28 counts of Sexual Abuse of Children (Child

Pornography)[5], and one count of Criminal Use of a Communication Facility[6] and one count of Sexual Abuse of Children (Distribution of Child Pornography)[7].

Seized property from Defendant's home were

(1) Digiland tablet from office.

(2) Dell Inspiron Laptop Computer N5010 containing a Western Digital hard drive from office (Defendant's laptop).

(3) Dell Inspiron Laptop Computer P20G containing a Segate hard drive (recovery location not listed).

(4) Samsung cell phone model SCH-1200PP from Defendant's person.

Zahm explained that in order to search for example the computers listed above

We take the hard drives, remove the hard drives from the computer, and we what' s called an imaging process and that's a bit for bit copy, exact replica of everything that' s on the disc and we call it e01 file, it's an image file. We take the image file and we use our EnCase Software, which is an industry standard software to do an analysis on what's on the image file, it's the most purest form of forensics. Usually forensics you have to take some, destroy a little bit of it to see to get the results; but with the computer forensics we're not destroying any piece of the original evidence. We have write blockers that keep us from putting anything on the evidence. We can't change it. Once we get the software piece loaded into EnCase I'll go though and look at every image, every video, every user created file and a few things that are on there and from that I'll print out difference report pieces that are included in my report.[8] Image reports I'll make note of notable images, I'll make note of apparent child pornography, I'll make note of anything else. In this particular case I would make note of anything that had to deal with any kinds of crimes against children and then the report is assembled and here we are.

N.T. 8/18/2016 at 12.

[5] 18 Pa.C.S. § 6312(d).
[6] 18 Pa.C.S. § 7512(a).
[7] 18 Pa.C.S. § 6312(c).
[8] Commonwealth's Exhibit #4. Matthew J. Zahm Special Agent Computer Forensics Unit Computer Forensics Analysis Summary Report 56-1556, BOGDEN, Dated August 18, 2016.

I. Habeas Corpus

A prima facie case exists when the Commonwealth produces evidence of each of the material elements of the crime charged and establishes probable cause to warrant the belief that the accused committed the offense. Furthermore, the evidence need only be such that, if presented at trial and accepted as true, the judge would be warranted in permitting the case to be decided by the jury. Commonwealth v. Karetny, 880 A.2d 505, 583 Pa. 514, 529 (Pa. 2005).

The elements of sexual abuse of children (child pornography) are

> (d) Child pornography. --
> (1) Any person who intentionally views or knowingly possesses or controls
> (2) any book, magazine, pamphlet, slide, photograph, film, videotape, computer depiction or other material depicting a child under the age of 18 years
> (3) engaging in a prohibited sexual act or in the simulation of such act commits an offense.

Intentionally views and prohibited sexual act are defined in the same statutory section:

> "*Intentionally views*." --The deliberate, purposeful, voluntary viewing of material depicting a child under 18 years of age engaging in a prohibited sexual act or in the simulation of such act. The term shall not include the accidental or inadvertent viewing of such material.
> "*Prohibited sexual act*." --Sexual intercourse as defined in section 3101 (relating to definitions), masturbation, sadism, masochism, bestiality, fellatio, cunnilingus, lewd exhibition of the genitals or nudity if such nudity is depicted for the purpose of sexual stimulation or gratification of any person who might view such depiction.

18 PA.C.S. § 6312 (G).

On October 7, 2015, Lauck was able to download file name lsv-018-077.jpg from 50.152.126.16 i.e. Defendant's laptop. Lauck testified that this specific image has a

SHA-1 value. The Internet Crimes against Children (ICAC) Task Force have compiled all the known SHA values of images that are indicative of child pornography. N.T. 12/11/2015 at 13. MDJ Kemp viewed the image at the preliminary hearing. Id. A description of the image:

> **Description**: This color .jpg image file depicts a naked pubescent female sitting on a gold-colored cloth in a studio setting and with her legs spread apart. The camera is zoomed in on the girl's vagina, anus and her vaginal opening in its entirety. The photo also depicts the logo "LS Models", in the upper right of the photo.

Of the recovered items from Defendant's home, one was a Dell Laptop N5010 that was identified as a Defendant's. Zahm found six images of apparent child pornography which were located within the computer's recycling bin. There were also 22 notable images of child pornography which was also located on the computer. Id. at 19-20. The BitTorrent software identified by Lauck off site was also located on the computer. Defense counsel stipulated for purposes of the preliminary hearing that those images meet the definition of child pornography. Id. at 21.

Lauck testified at the preliminary hearing to the statements Defendant's family members made when interviewed by investigators on the day the search warrant was executed as described above. The hearsay evidence was properly considered by the issuing authority in determining that a prima facie case had been established. Pa.R.Crim.P. 542(E). If all the statements are accepted as true, it seems certain that the Defendant did possess a laptop that did contain child pornography. It is also reasonable to believe that he viewed the images found on his personal computer. Though not testified to at the preliminary hearing, the Affidavit of Probable Cause in support of the arrest warrant indicated that (1) Defendant admitted he may have seen child pornography and (2) an on-site search of his cell phone found the search term

"PTHC" and acronym that stands for pre teen hard core, a popular search term to find child pornography. Those two circumstances, if accepted as true, move the evaluator from assuming Defendant viewed the images to presuming that he did: he admits he "may" have seen child pornography and his search history shows that someone searched his phone for child pornography.

The elements of Dissemination of Child Pornography include

(c) Dissemination of photographs, videotapes, computer depictions and films. --

Any person who knowingly sells, distributes, delivers, disseminates, transfers, displays or exhibits to others, or who possesses for the purpose of sale, distribution, delivery, dissemination, transfer, display or exhibition to others, any book, magazine, pamphlet, slide, photograph, film, videotape, computer depiction or other material depicting a child under the age of 18 years engaging in a prohibited sexual act or in the simulation of such act commits an offense.

Lauck was able to download from Defendant's personal laptop computer a pornographic image of a pubescent female (description above). Defendant admits to having utilized the BitTorrent software and denies using it to search for and disseminate child pornography. There may be some argument that Defendant did not knowingly disseminate the material. It is possible that he believed he was only using the software to download games as he admits to, or download child pornography, which he denies.

A person acts knowingly with respect to a material element of an offense when:

(i) if the element involves the nature of his conduct or the attendant circumstances, he is aware that his conduct is of that nature or that such circumstances exist; and

(ii) if the element involves a result of his conduct, he is aware that it is practically certain that his conduct will cause such a result.

18 PA.C.S. § 302.

The Court finds that knowingly, in the context of dissemination of child pornography, involves the former and that there is sufficient evidence in the preliminary hearing record that indicates Defendant knowingly disseminated child pornography. For example, Defendant admitted to downloading pornography. N.T. 12/11/2015 at 26. He also admitted to using the search terms “lesbian” and “teen” when searching for pornography. Id. There was no statement by Lauck that Defendant knew that by using BitTorrent software on his personal computer that he would be sharing any of the information he downloaded; however, given the general description as to how BitTorrent software works:

> P2P client software allows the user to set up files and directories on a computer to be shared with others on a like network…During the installation of typical BitTorrent network client programs, various settings are established which configure the host computer to share files…Once the BitTorrent network client has downloaded part of a file, it may immediately begin sharing the file with other users on the network…

The Court finds that Defendant was aware that his computer was sharing the file that Lauck was able to download from his computer.

Criminal Use of a Communication Facility is defined as follows:

> A person commits a felony of the third degree if that person uses a communication facility to commit, cause, or facilitate the commission or the attempt thereof any crime which constitutes a felony under this title …As used in this section, the term "*communication facility*" means a public or private instrumentality used or useful in the transmission of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part, including, but not limited to, telephone, wire, radio, electromagnetic, photoelectronic or photo-optical systems or the mail.

18 PA.C.S. § 7512.

In Commonwealth v. Crabill, 2007 PA Super 161; 926 A.2d 488 (Pa. Super. 2007), the Superior Court upheld a conviction under the same section noting that Appellant used his computer, gained access to an internet chat room, and communicated lewd messages to a person he believed to be a twelve-year-old girl, in

furtherance of his felonious efforts to have unlawful contact with a minor. In the case at bar, it appears that Defendant used his computer, to gain access to the internet, to intentionally view child pornography (28 images were found on Defendant's laptop during the at home search as well the "PTHC" search term on Defendant's cell phone). Under the statute, Criminal Use of a Communication Facility "every instance where the communication facility is utilized constitutes a separate offense under this section"; therefore, Defendant being called to answer to one count is appropriate.

II. Motion to Suppress

The Defendant argues that the search warrant that led to the search of his residence was issued in violation of his rights under Article 1 Section 8 of the Pennsylvania Constitution and under the Fourth Amendment to the United States Constitution. Defendant alleges that the search warrant 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 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[9] and Commonwealth v. Melvin[10] 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 A.3d 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.

[9] 88 A.3d 983 (Pa.Super 2014).
[10] 103 A.3d 1 (Pa. Super 2014).

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.

The Defendant also alleges that the warrant was issued without probable cause as the only information in the affidavit that establishes the possible location of the electronic device which may have been used was the IP address of the Defendant. Defendant asserts that affiant 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. 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.[11] The Background supra states the facts as the were presented to the MDJ in Lauck's affidavit.

> 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 Lauck 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 laptop. Again, devices without the file sharing software or the capability of downloading photos would not be searched and/or seized as there would be no chance that the materials would be found within.

---

[11] At any hearing on a motion for return of or suppression of evidence, or for suppression of the fruits of evidence, obtained pursuant to a search warrant, no evidence shall be admissible to establish probable cause other than the affidavits provided for in paragraph (B). Paragraph (B) states "No search warrant shall issue but upon the probable cause of supported by one or more affidavits sworn to before the issuing authority….the issuing authority, in determining whether probable cause has been established, may not consider any evidence outside the affidavits."

The Court additionally finds that the description of the image downloaded from Defendant's laptop sufficiently meets the definition of child pornography.

Description: This color .jpg image file depicts a naked pubescent female sitting on a gold-colored cloth in a studio setting and with her legs spread apart. The camera is zoomed in on the girl's vagina, anus and her vaginal opening in its entirety. The photo also depicts the logo "LS Models", in the upper right of the photo.

Naked pubescent female means a girl in late school years or early teenage years who has begun to develop secondary sexual characteristics but is still a minor. Additionally, the position of this naked pubescent female is precisely what the statute prohibits: a lewd exhibition of the genitals.

III. Motion to Modify Condition of Bail

An Order of Court filed August 25, 2016, modified the conditions of bail.

IV. Motion for Return of Property

As Items (2) and (4) were found to contain no child pornography, see Commonwealth's Exhibit #4, Computer Forensics Examination Summary Report, the Commonwealth agreed to return Items (2) and (4) at the August 18, 2016, hearing. Items (1) and (3) will be retained by the Commonwealth as derivative contraband.

ORDER

AND NOW, this 14th day of December, 2016, based upon the foregoing Opinion,

(1) The Motion for Habeas Corpus is DENIED.

(2) The Motion to Suppress is DENIED.

(3) The Motion for Return of Property is DENIED in part and GRANTED in part. The Commonwealth is ORDERED and DIRECTED to return Items (2) and (4) to the Bogden family if it has not already done so.

BY THE COURT,

Nancy L. Butts, P.J.

cc: Peter Campana, Esq.
Christopher Jones, Esq.
Office of Attorney General
Strawberry Square
16th Floor
Harrisburg, PA 17120-0001
Gary Weber, Esq. Lycoming Law Reporter
Susan Roinick, Law Clerk