UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
JACKSONVILLE DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

vs. CASE NO. 3:12-cr-134-J-34TEM

ARNOLD BERNARD CONRAD, JR.,

Defendant.

REPORT AND RECOMMENDATION[1]

I. Status

This matter is before the Court on referral by the Honorable Marcia Morales Howard for a report and recommendation on Defendant Arnold Bernard Conrad Jr.'s Motion to Suppress and Memorandum of Law in Support (Doc. 43), filed January 25, 2013. The United States filed a response in opposition on February 14, 2013 (Doc. 54). In his motion, Defendant moves to suppress and exclude as evidence any and all fruits of the execution of the search warrant for Defendant's computers and hard drives. Defendant argues the evidence should be suppressed because (1) the warrant was facially invalid because it lacked particularity and was overbroad; (2) the warrant was executed in an unreasonable manner; and (3) the government agents did not act in good faith.

[1] As a matter of course, within fourteen (14) days after service of this document, specific, written objections may be filed in accordance with 28 U.S.C. § 636, Rule 59, Federal Rules of Criminal Procedure, and Rule 6.02, Local Rules, United States District Court, Middle District of Florida. Failure to file a timely objection waives a party's right to review. Fed. R. Crim. P. 59.

An evidentiary hearing was held before the undersigned on March 14, 2013.[2] The Court heard testimony from Detective Gary M. Snyder with the Jacksonville Sheriff's Office. With leave of the Court, Defendant filed a post-hearing memorandum on April 8, 2013 (Doc. 79). The United States submitted a response on April 15, 2013 (Doc. 80). Defendant filed a reply on April 18, 2013 (Doc. 83). The United States filed a sur-reply on April 25, 2013 (Doc. 84).

Upon consideration of the arguments from counsel and the evidence presented, the undersigned respectfully recommends the motions to suppress be **DENIED** for the reasons set forth herein.

II. Background

On December 2, 2011, Detective Gary M. Snyder ("Snyder") of the Jacksonville Sheriff's Office ("JSO") submitted an affidavit in support of an application for a search warrant for a home located at 12330 Old Kings Road, Jacksonville, Florida (*see* Doc. 54-1, Affidavit for Search Warrant). The affidavit indicates that on October 7, 2011, Snyder determined that a computer located in Duval County, Florida had downloaded and shared child pornography on the Internet between September 26, 2011 and September 29, 2011 using a peer-to-peer file sharing program called Gnutella.[3] Affidavit at 12. Snyder used

[2] The transcript of the evidentiary hearing (Doc. 77) will hereinafter be referred to as "Tr." followed by the appropriate page number.

[3] The affidavit explains that peer-to-peer file sharing is a method of communication available to Internet users through the use of special software to facilitate the trading of files, images, and videos. Users of the peer-to-peer file sharing software install the software on their computers to directly trade or exchange files between computers. The user must knowingly choose to install the publicly available software to facilitate the trading of files. Installing the software program onto a computer allows the users to share digital files with one another while connected to the Gnutella network. Files are shared among (continued...)

software available to law enforcement that runs on the Gnutella network. The software reads publicly available advertisements or offers to share files from computer users, captures the SHA-1 value for any image or file that contains known or suspected images of child pornography, and documents the related IP address for that computer location.[4] *Id.* at 10. A complementary law enforcement software program then organizes the collected data to provide the total number of times a particular computer located at a particular IP address has been identified as advertising files of child pornography based on the identified SHA-1 value. *Id.* at 11. This software also provides information regarding the specific date and time of the advertisement and the state and city where the computer is likely located. *Id.*

Using these tools, Snyder viewed a list of approximately 418 files that were identified as available for downloading from the computer assigned IP address 74.178.241.103 between September 26, 2011 and September 29, 2011. *Id.* at 13. Many of the files were titled in a manner that suggested the content included sexual exploitation of children. *Id.* The data provided by the law enforcement program indicated that 174 of the files had SHA-1 values that were designated by law enforcement as suspected child pornography. *Id.* at

---

[3](...continued)
users as a result of being located in a specific folder on the user's computer, referred to as a "shared" folder.

[4] Secure Hash Algorithm Version 1 or SHA-1 is a file recognition method. Every computer file has a specific, unique SHA-1 value that is "similar to a fingerprint for the file." Affidavit at 4. Any change to a file, no matter how small, will result in a new SHA-1 value assigned to that file. *Id.* This method of file recognition is used by file sharing programs on peer-to-peer networks like Gnutella. *Id.*

The National Center of Missing and Exploited Children ("NCMEC") has a database list of unique SHA-1 values that are known to law enforcement to correspond to specific images of children being sexually exploited (Affidavit at 6; Tr. 19).

13-14. Snyder selected two SHA-1 files from the list of 174, which were reported to be offered for downloading from IP address 74.178.241.103 and confirmed that the files depicted child pornography. *Id.* at 14-15. Snyder conducted an Internet search and determined the IP address 74.178.241.103 was owned and issued by AT&T. *Id.* at 16. Snyder issued a subpoena to AT&T and learned that the Defendant was the subscriber associated with IP address 74.178.241.103. *Id.*

On December 15, 2011, Snyder obtained a search warrant from the Circuit Court of the Fourth Judicial Circuit in and for Duval County, Florida (Doc. 54-2, Search Warrant). The warrant stated there was probable cause to believe that a computer or other digital device capable of accessing the internet was knowingly used as an instrumentality of the crime of creating, possessing or promoting child pornography and contained evidence of that crime. *Id.* at 2. The warrant authorized the seizure, and off-site search and analysis, of the following items:

> 1. Computer hardware to include any and all computer equipment used to collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. Hardware includes (but is not limited to) any data-processing devises (such as central processing units, personal computers to include "laptop" or "notebook" or "pocket" computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, and other electronic media devices).
>
> 2. Computer input and output devices to include but not limited to keyboards, mice, scanners, printers, monitors, network communication devices, modems and external or connected devices used for accessing computer storage media.
>
> 3. Computer storage media and the digital content to include but not limited to floppy disks, hard drives, tapes, DVD disks, CD-ROM disks or other magnetic, optical or mechanical storage which can be accessed by computers to store or retrieve data or images of child pornography.

4. Computer software and application software installation and operation media.

5. Computer software, hardware or data related to the sharing of Internet access over wired or wireless networks allowing multiple persons to appear on the Internet from the same IP address.

6. Manuals and other documents (whether digital or written) which describe operation of items or software seized.

7. Items containing or displaying passwords, access codes, usernames or other identifiers necessary to examine or operate items, software or information seized.

8. Correspondence or other documents (whether digital or written) pertaining to the possession, receipt, origin or distribution of images involving the sexual exploitation of children.

9. Correspondence or other documents (whether digital or written) exhibiting an interest or the intent to sexually exploit children and to identify a particular users of the materials or contraband and any data or text which tends to prove the identity of the computer user at a time that may be relevant to prove the possession or distribution of child pornography or the sexual exploitation of children. Items may include, but are not limited to, pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, and tape recordings, "trophies," grooming aids or other items demonstrating an interest in the exploitation of children.

10. Items that would tend to establish ownership or use of computers and ownership or use of any Internet service accounts accessed to obtain child pornography to include credit card bills, telephone bills, correspondence and other identification documents.

11. Items that would tend to show dominion and control of the property or premises searched, to include utility bills, telephone bills, correspondence, rental agreements and other identification documents.

12. Data maintained on the computer, or computer related storage devices such as floppy diskettes, tape backups, computer printouts, and "zip" drive diskettes, in particular, data in the form of images and/or videos and any accompanying text associated with those images, and/or log files recording the transmission or storage of images, as they relate to violations of Florida law cited herein as related to the possession and distribution of child pornography.

Id. at 2-3.

The search warrant was executed that same day. Agents seized two laptop computers and three external hard drives from Defendant's home. The computer systems and media were delivered to Special Agent James C. Greenmun ("SA Greenmun") of the Department of Homeland Security ("DHS") Homeland Security Investigations ("HSI") Jacksonville Field Office for a computer forensics examination (Doc. 43-8). Between December 29, 2011 and January 3, 2012, SA Greenmun created mirror images of the computer hard drives and electronic files (Tr. 56; Doc. 43-8 at 2). SA Greenmun completed the computer forensic evaluation on May 14, 2012. *Id.* at 1. The evaluation found 649 child pornographic computer files located on one of the laptops and two of the external hard drives. *Id.* at 5. The other laptop and external hard drive were believed to be used primarily by Defendant's wife and did not contain any child pornographic computer files.[5] (Tr. 60-61; Doc. 43-8 at 10, 11).

Defendant was indicted on August 22, 2012 (Doc. 1) and arrested on August 24, 2012. Defendant's counsel entered an appearance on August 27, 2012 (Doc. 8). On August 29, 2012, the United States provided discovery to Defendant (Doc. 54-3). On September 20, 2012, the United States filed a bill of particulars indicating its intent to forfeit Defendant's laptop computer and two external hard disk drives (Doc. 21).

In October 2012, counsel for the parties discussed the return of the non-contraband items contained in Defendant's computer media, as well as the laptop and external hard disk drive used by Defendant's wife that did not contain any contraband (Tr. 27). On October 22, 2012, defense counsel sent an email to counsel for the United States with two

[5] The main user for this laptop was labeled "Therese Conrad," and the external hard drive appeared to be a backup for her computer information.

attached draft motions seeking the return of this property (Exhibit 5). During a subsequent telephone call, counsel discussed this issue and agreed that such items could be returned. Counsel for Defendant confirmed this agreement by correspondence dated October 29, 2012 (Doc. 54-4; Exhibit 6). On December 7, 2012, counsel for the parties met at the HSI office to inspect and review the digital evidence contained on defendant's computer media (Tr. 28). During this meeting, counsel confirmed the non-contraband items could be returned to Defendant and arrangements would be made to do so, including that Defendant would provide a clean hard disk drive to law enforcement for the purpose of removing the non-contraband items contained on the laptop used by Defendant (Tr. 28-29).

On January 25, 2013, Defendant filed motions for return of non-contraband property, which indicated that the United States objected to the relief sought (Docs. 39 & 40). On February 1, 2013, the United States filed responses to the motions, indicating its agreement that the requested property could be returned (Docs. 47 & 48). Thereafter, counsel for the parties discussed the matter by telephone, and counsel for the United states requested defense counsel provide a clean external hard disk drive to HSI to accomplish the return of the non-contraband items on Defendant's computer. During a telephone call on February 6, 2013, defense counsel confirmed that the return process of the requested items would be initiated. During a telephone conference call on February 12, 2013, defense counsel again advised counsel for the United States and SA Greenmun that he would send a clean external hard disk drive to HSI by mail and would arrange for the pickup of the non-contraband items (Tr. 29-30). On February 18, 2013, the United States delivered the hard drive with the information requested in the motions for return of

seized property, and Defendant subsequently withdrew his motions for return of non-contraband property (Doc. 57).

At the hearing, Snyder testified the government was still in possession of the laptop computer used by Defendant's wife (Tr. 86). Snyder testified the laptop was available for turnover at that point, but Defendant had not picked it up yet. *Id.* The Order Setting Conditions of Release prohibits Defendant from possessing or using any computer or accessing the Internet except from work purposes (Doc. 13). Snyder also testified that it was HSI's standard operating procedure to wait until they received a report from NCMEC before returning non-contraband items (Tr. 62-63).[6] Snyder testified that if there is an unidentified victim within the child pornography, the agents will go through non-contraband movies or images on the computer media to attempt to identify the victim (Tr. 27). Snyder testified that, typically, non-contraband items are returned when requested (Tr. 63).

On March 15, 2013, Defendant's counsel notified the United States that he had procured an alternative location (other than Defendant's residence) to store the clean laptop and external hard drive (Doc. 80 at 3). On March 20, 2013, Snyder notified Defendant's counsel that the items were available for pick-up. *Id.* Defendant's counsel picked up the items on March 22, 2013. *Id.*

III. Conclusions of Law and Analysis

In the instant motion, Defendant moves to suppress and exclude as evidence any and all fruits of the execution of the search warrant for Defendant's computers and hard drives. Defendant argues (1) the warrant was facially invalid because it lacked particularity

[6] It is not clear to the undersigned when the NCMEC report was received by the government. However, this uncertainty does not affect the undersigned's determination as to whether the government acted in a reasonable manner.

and was overbroad; (2) the warrant was executed in an unreasonable manner; and (3) the government agents did not act in good faith.[7]

A. Whether the warrant was facially invalid because it lacked particularity and was overbroad

The Fourth Amendment provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV. "The requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another." *Marron v. United States*, 275 U.S. 192, 196 (1927). "A warrant which fails to sufficiently particularize the place to be searched or the things to be seized is unconstitutionally over broad." *United States v. Travers*, 233 F.3d 1327, 1329 (11th Cir. 2000). However, "elaborate specificity in a warrant is unnecessary" to satisfy the particularity requirement. *United States v. Peagler*, 847 F.2d 756, 757 (11th Cir. 1988). "A description is sufficiently particular when it enables the searcher to reasonably ascertain and identify the things authorized to be seized." *United States v. Wuagneux*, 683 F.2d 1343, 1348 (11th Cir. 1982).[8]

---

[7] Defendant's motion to suppress originally raised four grounds for suppression. On April 1, 2013, Defendant filed a motion to withdraw Ground I, in which he alleged the warrant lacked probable cause because it was based on information obtained from an unlawful search (Doc. 75). The Court granted the motion on April 2, 2013 (Doc. 76).

[8] "Search warrants must be specific. Specificity has two aspects: particularity and breadth. Particularity is the requirement that the warrant must clearly state what is sought. Breadth deals with the requirement that the scope of the warrant be limited by the probably cause on which the warrant is based." *United States v. Hill*, 459 F.3d 966, 973 (9th Cir. 2006) (citing *United States v. Towne*, 997 F.2d 537, 544 (9th Cir. 1993)).

In the instant case, Defendant argues the warrant lacked particularity because it was not limited by reference to the alleged crime and/or search methodology to confine the scope of the computer searches. Defendant argues only three of the twelve numbered items in the warrant were limited by reference to child pornography, while nine of the numbered items "permitted the government to go on a fishing expedition through every nook and cranny of the computers and external hard drives at Defendant's home" (Doc. 43 at 24). Additionally, Defendant argues the warrant was overbroad because it authorized a general rummaging through Defendant's computers and hard drives, and allowed the government to search and seize property which fell outside the scope of probable cause.

As an initial matter, the undersigned notes five of the twelve numbered items in the search warrant reference child pornography:

> 3. Computer storage media and the digital content to include but not limited to floppy disks, hard drives, tapes, DVD disks, CD-ROM disks or other magnetic, optical or mechanical storage which can be accessed by computers to store or retrieve data or images of child pornography.
>
> 8. Correspondence or other documents (whether digital or written) pertaining to the possession, receipt, origin or distribution of images involving the sexual exploitation of children.
>
> 9. Correspondence or other documents (whether digital or written) exhibiting an interest or the intent to sexually exploit children and to identify a particular users of the materials or contraband and any data or text which tends to prove the identity of the computer user at a time that may be relevant to prove the possession or distribution of child pornography or the sexual exploitation of children. Items may include, but are not limited to, pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, and tape recordings, "trophies," grooming aids or other items demonstrating an interest in the exploitation of children.
>
> 10. Items that would tend to establish ownership or use of computers and ownership or use of any Internet service accounts accessed to obtain child pornography to include credit card bills, telephone bills, correspondence and other identification documents.

> 12. Data maintained on the computer, or computer related storage devices such as floppy diskettes, tape backups, computer printouts, and "zip" drive diskettes, in particular, data in the form of images and/or videos and any accompanying text associated with those images, and/or log files recording the transmission or storage of images, as they relate to violations of Florida law cited herein as related to the possession and distribution of child pornography.

(Doc. 54-2, Search Warrant at 2-3) (emphasis added). The warrant also stated that there was probable cause to believe that a computer or other digital device capable of accessing the internet was knowingly used as an instrumentality of the crime of creating, possessing or promoting child pornography and contained evidence of that crime. *Id.* at 2.

Although not every numbered item in the warrant contained a reference to child pornography, it is abundantly clear that the agents were permitted to seize and search computer hardware, software, data and documents that would evidence possession or distribution of child pornography. The scope of the warrant was restricted to a search for evidence of child pornography crimes and did not permit a free-ranging search. *Cf. United States v. Rosa,* 626 F.3d 56, 62 (2d Cir. 2010) ("The warrant was defective in failing to link the items to be searched and seized to the suspected criminal activity – i.e., any and all electronic equipment potentially used in connection with the production or storage of child pornography and any and all digital files and images relating to child pornography contained therein – and thereby lacked meaningful parameters on an otherwise limitless search of Rosa's electronic media."); *United States v. George*, 975 F.2d 72, 76 (2d Cir. 1992) ("Mere reference to 'evidence' of . . . general criminal activity provides no readily ascertainable guidelines for the executing officers as to what items to seize. . . . [A]uthorization to search for 'evidence of *a* crime,' that is to say, any crime, is so broad as to constitute a general warrant."). The search warrant in this case did not authorize a

search for evidence of "general criminal activity" but for evidence of child pornography contained on a computer or other digital device capable of accessing the internet located at Defendant's residence. The fact that some of the specific numbered items in the search warrant do not reference child pornography is unremarkable under the circumstances. The agents had probable cause to believe a computer located at Defendant's residence contained child pornography, but did not know which computer that might be. Therefore the warrant authorized the seizure of all "computer hardware," "computer input and output devices" and "computer storage media" for off-site analysis to search for evidence of child pornography, i.e. "documents (whether digital or written) pertaining to the possession, receipt, origin or distribution of images involving the sexual exploitation of children"; "documents (whether digital or written) exhibiting an interest or the intent to sexually exploit children"; and "[d]ata maintained on the computer, or computer related storage devices . . . related to the possession and distribution of child pornography."

Federal courts applying a reasonableness analysis on a case-by-case basis "have rejected most particularity challenges to warrants authorizing the seizure and search of entire personal or business computers." *United States v. Richards*, 659 F.3d 527, 539 (6th

Cir. 2011) (collecting cases).[9] This is in recognition of the unique challenges posed by computer searches.

> Unlike warrants seeking readily identifiable evidence such as narcotics or firearms, an onsite search of a computer for the evidence sought by a warrant is not practical or even possible in some instances. *See Guest v. Leis,* 255 F.3d 325, 335 (6th Cir. 2001) (discussing cases that permitted taking computers off site for forensic searches and explaining that "[b]ecause of the technical difficulties of conducting a computer search in a suspect's home, the seizure of the computers, including their content, was reasonable in these cases to allow police to locate the offending files"). Computers store millions of documents, and as some courts have recognized, the onsite search (and accompanying occupation to conduct such a search), might be more off putting to an individual than the seizure of a computer for an off-site determination as to whether it stores any information that falls within the scope of the warrant.

---

[9] *See, e.g., United States v. Sherman*, 372 Fed. Appx. 668, 676 (8th Cir. 2010) ("The search warrant necessarily needed to include all computer equipment and systems to effectively allow law enforcement to recognize and seize the materials described." (internal quotations omitted)); *United States v. Grimmett*, 439 F.3d 1263, 1270 (10th Cir. 2006) (upholding search warrant that authorized the search of "'any [computer] equipment' that can create or display computer data" and encompassed "any and all computer software")*; United States v. Upham,* 168 F.3d 532, 535 (1st Cir.1999) ("As a practical matter, the seizure and subsequent off-premises search of the computer and all available disks was about the narrowest definable search and seizure reasonably likely to obtain the images. A sufficient chance of finding some needles in the computer haystack was established by the probable-cause showing in the warrant application; and a search of a computer and co-located disks is not inherently more intrusive than the physical search of an entire house for a weapon or drugs. We conclude . . . that the first paragraph [of the warrant, authorizing the seizure of "any and all computer software and hardware, . . . computer disks, disk drives . . ."] was not constitutionally overbroad."); *United States v. Lacy,* 119 F.3d 742, 746 (9th Cir.1997) (warrant permitting "blanket seizure" of computer equipment from defendant's apartment was not insufficiently particular when there was probable cause to believe that computer would contain evidence of child pornography offenses); *United States v. Wunderli*, No. 4:11 CR 538 JAR/DDN, 2012 WL 1432606, at *6 (E.D. Mo. Mar. 27, 2012) (holding the Fourth Amendment's particularity requirement was satisfied where warrant authorized police to seize "many types of electronic and other devices capable of being used in the possession and distribution of child pornography images, the renderings of such images, and the records thereof, wherever in the residence at 3031 Ventnor Place they may be found."); *United States v. Albert,* 195 F.Supp.2d 267, 275–76 (D. Mass. 2002) (upholding warrant for seizure of computer and all related software and storage devices where such an expansive search was "the only practical way" to obtain images of child pornography).

United States v. Metter, 860 F.Supp.2d 205, 213 (E.D.N.Y. 2012). Thus, the warrant did not lack particularity and was not overbroad because it permitted the seizure of all "computer hardware," "computer input and output devices" and "computer storage media" for off-site analysis.[10] Further, the warrant did not lack particularity due to the absence of a search protocol or methodology. *See Richards*, 659 F.3d at 538 ("[G]iven the unique problem encountered in computer searches, and the practical difficulties inherent in implementing universal search methodologies, the majority of federal courts have eschewed the use of a specific search protocol . . ."); *United States v. Burgess*, 576 F.3d 1078, 1093-94 (10th Cir. 2009) ("It is unrealistic to expect a warrant to prospectively restrict the scope of a search by directory, filename or extension or to attempt to structure search methods – that process must remain dynamic. . . . [I]t is folly for a search warrant to attempt to structure the mechanics of the search and a warrant imposing such limits would unduly restrict legitimate search objectives."); *United States v. Khanani,* 502 F.3d 1281, 1290 (11th Cir. 2007) (rejecting defendants' argument that "the lack of a written 'search protocol' required the district court to suppress all evidence agents seized as a result of the search of the defendants' computers"); *United States v. Brooks,* 427 F.3d 1246, 1251 (10th Cir. 2005) ("This court has never required warrants to contain a particularized computer search strategy."); *United States v. Maali*, 346 F.Supp.2d 1226, 1245 (M.D. Fla. 2004) ("[T]he lack

[10] Courts have also upheld the seizure of "[i]tems that would tend to show dominion and control of the property or premises searched" (numbered item 11). *See United States v. Horn*, 187 F.3d 781, (8th Cir. 1999) ("[T]he words '[r]ecords, documents, receipts, keys, or other objects showing access to, and control of, the residence" were sufficiently particular to preclude the exercise of any illegal discretion by the executing officers.").

of a detailed computer 'search strategy' does not render the warrant deficient as to the search and seizure of computers.").[11]

The particularity requirement of the Fourth Amendment was satisfied here because the warrant identified the types of property authorized to be seized and indicated the crimes involved for which evidence was sought. *Cf. United States v. Riccardi*, 405 F.3d 852, 862 (10th Cir. 2005) ("Our case law therefore suggests that warrants for computer searches must affirmatively limit the search to evidence of specific federal crimes or specific types of materials. The warrant in this case was not limited to any particular files, or to any particular federal crime. . . . By its terms, the warrant thus permitted the officers to search for anything – from child pornography to tax returns to private correspondence.") (internal citations omitted). The warrant in this case limited the search to computer equipment, digital storage devices, and accessories that could contain contraband and evidence linked to the child pornography offenses specified in the warrant. *See United States v. Gabel*, No. 10-60168, 2010 WL 3927697, at *10 (S.D. Fla. Sept. 16, 2010) (holding search warrant satisfied particularity requirement where it limited search to computers, digital storage devices, accessories, and other materials that could contain child pornography), *aff'd*, 470

[11] Defendant relies heavily on a case from the Western District of Washington in which the magistrate judge denied the government's application for a warrant to seize "any computers or digital devices" that may be located at the defendant's residence to search for "evidence relating to the crimes of copyright infringement or trafficking in counterfeit goods" as overbroad because the supporting affidavit contained no reference to a search filter term and no promise to foreswear reliance on the plain view doctrine. *In re United States of America's Application for a Search Warrant to Seize and Search Electronic Devices from Edward Cunnius*, 770 F.Supp.2d 1138, 1141, 1152 (W.D. Wash. 2011). In light of the case law previously cited, in which the overwhelming majority of courts have upheld search warrants similar to the one in this case, the undersigned declines to follow the reasoning in *In re United States of America's Application*. The Fourth Amendment does not require the level of surgical precision advocated by Defendant.

Fed. Appx. 853 (11th Cir. 2012). The warrant supplied enough information "to guide and control the agent's judgment in selecting what to take." *Upham*, 168 F.3d at 535. Moreover, the search was carried out in a controlled manner, not in flagrant disregard for the limitations of the warrant. *See Richards,* 659 F.3d at 542 (holding warrant that authorized search of computer servers for evidence of child pornography was not unconstitutionally overbroad and considering the fact that there was no actual claim that the search process was abused by the federal agents); *Grimmett*, 439 F.3d at 1270 ("There is no evidence of exploratory rummaging through files, or inadvertent discoveries. No wholesale searching occurred here, despite the broad authority the warrant may have granted.") (internal citations omitted).

The warrant was not unconstitutionally overbroad because non-contraband items contained within the computer (such as bank statements, professional records, personal photographs and music) were also subject to seizure. Again, federal courts have consistently recognized that computer searches pose unique challenges that may result in "some innocuous documents [being] examined, at least cursorily in order to determine whether they are, in fact, among those papers authorized to be seized." *Andersen v. Maryland*, 427 U.S. 463, 482 n.11 (1976). The district court for the Eastern District of New York explained:

> Computers and electronic information present a more complex situation, given the extraordinary number of documents a computer can contain and store and the owner's ability to password protect and/or encrypt files, documents, and electronic communications. As a result, the principle of permitting law enforcement some flexibility or latitude in reviewing paper documents just described, has been extended to computerized or electronic evidence. Courts have applied the principles recognized in *Andresen* "in analyzing the method used by the police in searching computers and have afforded them leeway in searching computers for incriminating evidence within the scope of materials specified in the warrant." *Graziano,* [558

> F.Supp.2d 304, 317 (E.D.N.Y. 2008)]; *see also United States v. Scarfo,* 180 F.Supp.2d 572, 578 (D.N.J.2001) ("Where proof of wrongdoing depends upon documents or computer passphrases whose precise nature cannot be known in advance, law enforcement officers must be afforded the leeway to wade through a potential morass of information in the target location to find the particular evidence which is properly specified in the warrant."). Thus, courts developed a more flexible approach to the execution of search warrants for electronic evidence, holding the government to a standard of reasonableness. *See Graziano,* 558 F.Supp.2d at 316 ("[T]he manner of the execution of the warrant" in computer searches is "subject to judicial review under a 'reasonableness' standard.").

Metter, 860 F.Supp.2d at 213-14; *see also United States v. Riley,* 906 F.2d 841, 845 (2d Cir. 1990) ("It is true that a warrant authorizing seizure of records of criminal activity permits officers to examine many papers in a suspect's possession to determine if they are within the described category. But allowing some latitude in this regard simply recognizes the reality that few people keep documents of their criminal transactions in a folder marked 'drug records.'"); *United States v. Santarelli,* 778 F.2d 609, 615-16 (11th Cir. 1985) (finding search reasonable even though agents removed a large number of documents that were unrelated to loansharking activity because "the agents were entitled to examine each document in the bedroom or in the filing cabinet to determine whether it constituted evidence they were entitled to seize under the warrant"); *Maali*, 346 F.Supp.2d at 1245 ("The fact that many records other than those responsive to a search warrant are likely to be stored on computers does not render seizure of computers for offsite searching impermissible."). Additionally, the Eleventh Circuit has held that "absent a 'flagrant disregard' of the terms of the warrant, the seizure of items outside the scope of a warrant will not affect admissibility of items properly seized." *Wuagneux*, 683 F.2d at 1354 (quoting *United States v. Heldt*, 668 F.2d 1238, 1259-60 (D.C. Cir. 1981)). The undersigned does not find "flagrant disregard" for the terms of the warrant under the facts of this case.

Accordingly, the undersigned finds the warrant was neither insufficiently particular nor impermissibly overbroad.

B. Whether the warrant was executed in an unreasonable manner

Defendant argues the execution of the search warrant was unreasonable because government agents seized and retained for more than thirteen months non-contraband items that fell outside the warrant's scope, including computer equipment that contained no evidence relating to child pornography. Defendant relies on two recent decisions of the Eleventh Circuit to argue that the delay unreasonably infringed on Defendant's possessory interests protected by the Fourth Amendment. *See United States v. Mitchell*, 565 F.3d 1347 (11th Cir. 2009); *United States v. Laist*, 702 F.3d 608 (11th Cir. 2012).

In *Mitchell*, two agents seized the hard drive of the defendant's computer, acting on probable cause that the computer contained images of child pornography. *Mitchell*, 565 F.3d at 1349. Twenty-one days after the initial seizure of the hard drive, one of the agents applied for and received a warrant to search the computer.[12] *Id.* The court found the government had not provided adequate justification for the delay and rejected the argument that there was no harm in the delay in applying for the search warrant.

> The purpose of securing a search warrant soon after a suspect is dispossessed of a closed container reasonably believed to contain contraband is to ensure its prompt return should the search reveal no such incriminating evidence, for in that event the government would be obligated to return the container (unless it had some other evidentiary value). In the ordinary case, the sooner the warrant issues, the sooner the property owner's possessory rights can be restored if the search reveals nothing incriminating.

---

[12] Three days after the seizure, one of the agents left town to attend a two-week training course. *Id.* at 1349. He did not apply for the search warrant until after his return. *Id.* The agent testified he did not feel any urgency to apply for the warrant before he left town because the defendant had admitted the hard drive contained child pornography. *Id.* at 1351.

> If anything, this consideration applies with even greater force to the hard drive of a computer, which is the digital equivalent of its owner's home, capable of holding a universe of private information.

Id. at 1352 (internal quotation marks and citations omitted). The Eleventh Circuit explained that an otherwise lawful seizure can violate the Fourth Amendment and infringe upon an owner's possessory interests if the police act with unreasonable delay in securing a search warrant. *Id.* at 1350. The court directed that the reasonableness of the delay be determined in light of all the facts and circumstances on a case-by-case basis and reflecting a careful balancing of governmental and private interests. *Id.* at 1350-51.

In *Laist*, FBI agents conducted a "knock and talk" to interview the defendant and request his consent to seize and search his computer. *Laist*, 702 F.3d at 610. The defendant admitted there was child pornography on his computer, signed a consent form authorizing the search and seizure of his computer and hard drives, and accessed the computer to show the agents an image that appeared to be child pornography. *Id.* at 610-11. Before seizing the computer, the agents allowed the defendant to copy some school documents onto an external hard drive. *Id.* at 611. One week later, the defendant's attorney sent a letter to the FBI revoking the defendant's consent. *Id.* Twenty-five days after receipt of the letter revoking the defendant's consent, the agents submitted an application for a search warrant to a magistrate judge, who issued the warrant six days later. *Id.* at 611-12. The Circuit court found the twenty-five day delay in applying for the warrant was reasonable under the circumstances. *Id.* at 616-17. The court found the defendant's possessory interest was diminished because he had been afforded the opportunity to remove the files he needed for school, and he had admitted the presence of contraband on his computer. *Id.* at 616. The court found "[t]he government's efforts

were sufficiently diligent to pass muster under the Fourth Amendment" under the totality of the circumstances considering that the government had submitted a detailed affidavit that contained valuable information and took time to draft and edit, and the agents were "extremely busy" with other matters. *Id.* at 617.

In both of these cases, agents seized computer media without a warrant and held it for a period of time before obtaining warrants to search their contents. Because the agents in this case seized Defendant's computers pursuant to a valid search warrant, *Mitchell* and *Laist* are distinguishable and inapposite. Here, the undersigned finds no unreasonable conduct in the government's execution of the search warrant. Approximately five months passed between the seizure of the computers and the completion of the forensic examination. Snyder testified that the delay was caused by the amount of workload facing forensic examiners (Tr. 55-56). Snyder testified the amount of time it takes to complete a computer forensic examination varies depending on the circumstances (Tr. 56). Snyder testified that the examination is a painstaking process and the length of the examination depends on the number of files that must be reviewed (Tr. 57).[13] The undersigned finds no evidence that the government was not diligent in its efforts to complete the forensic examination of Defendant's computer media. *See United States v. Lovvorn*, No. 1:11-cr-208-WKW-TFM, 2012 WL 3743975 (M.D. Ala. Apr. 24, 2012) (finding the nineteen month delay between the seizure of a computer and completion of the forensic examination was reasonably attributable to a "backlog of cases" and noting there was no evidence that the defendant sought to have his property returned or was prejudiced in any

[13] Snyder also testified that it was HSI's standard operating procedure to wait until they receive a report from NCMEC before returning noncontraband items (Tr. 62-63).

way) . Further, the undersigned can find no case law to support Defendant's argument that the government's retention of the non-contraband items between the completion of the forensic examination and Defendant's request for their return justifies suppression of lawfully seized evidence. *See United States v. Foster*, 100 F.3d 846, 852 (10th Cir. 1996) ("[T]he extreme remedy of blanket suppression should only be imposed in the most 'extraordinary' of cases."). The government agreed to return all non-contraband items upon Defendant's request, and the majority of the delay in the completion of such return was due to Defendant's failure to provide a clean external hard drive as well as the necessity of arranging storage of the property that would comply with Defendant's conditions of release.

C. Whether the government agents acted in good faith

Defendant argues the warrant in this case was facially invalid and no reasonable agent could have presumed it to be valid. Defendant argues "it should have been apparent to a government-trained agent that a warrant authorizing the search of 'any and all computer equipment used to collect . . . data' (item 1) without any reference to a crime lacked the requisite specificity" (Doc. 43 at 45).

"The good faith exception may be applied to a search conducted pursuant to an overly broad warrant." *United States v. Travers*, 233 F.3d 1327, 1330 (11th Cir. 2000) (citing *United States v. Accardo*, 749 F.2d 1477, 1481 (11th Cir. 1985)). When an officer has obtained a search warrant from a judge or magistrate and acted within its scope in good faith, "there is no police illegality and thus nothing to deter." *United States v. Leon*, 468 U.S. 897, 921 (1984). "The officers do not act in objective good faith, however, if the warrant is so overly broad on its face that the executing officers could not reasonably have presumed it to be valid." *Travers*, 233 F.3d at 1330 (citing *Accardo*, 749 F.2d at 1481). In

determining whether the good-faith exception should apply in a particular case, the "inquiry is confined to the objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal despite the magistrate's authorization." *Leon*, 468 U.S. at 922 n.23.

Here, the undersigned has determined the warrant did not lack particularity and was not overbroad. However, even if the Court were to find it so, the warrant was not "so facially deficient – i.e., failing to particularize the place to be searched or the things to be seized – that the executing officers could not have reasonably presumed it to be valid." *Travers*, 233 F.3d at 1330 (quoting *Accardo*, 749 F.2d at 1481). There is no evidence that the agents intentionally deceived the issuing judge or deliberately exceeded the scope of the warrant in the items seized during the search. The warrant indicated there was probable cause to believe that a computer located at Defendant's residence contained child pornography, and it was sufficiently detailed that a reasonable officer would have believed in good faith that the warrant was valid. This is not a situation where "even a cursory reading of the warrant would have revealed a glaring deficiency that any reasonable police officer would have known was constitutionally fatal." *Groh v. Ramirez*, 540 U.S. 551, 564 (2004). *See Riccardi*, 405 F.3d at 864 (holding good faith exception applied, even though warrant lacked particularity because it authorized the seizure of all computer equipment and did not reference the alleged crime).

Further, Defendant argues that even if it was not obvious that the warrant was facially invalid, the agents did not act in good faith because the government unreasonably executed the warrant by failing to return any of Defendant's computers and hard drives after making duplicate images of them. As discussed above, the undersigned finds the

government's execution of the warrant was reasonable. The undersigned does not find any evidence that the officers intentionally delayed the investigation or acted in bad faith.

IV. Conclusion

Based on the foregoing, the undersigned respectfully recommends Defendant Arnold Bernard Conrad Jr.'s Motion to Suppress and Memorandum of Law in Support (Doc. 43) be **DENIED**.

DONE AND ENTERED at Jacksonville, Florida this 14th day of May, 2013.

Thomas E. Morris

THOMAS E. MORRIS
United States Magistrate Judge

Copies to:
Hon. Marcia Morales Howard
All counsel of record