[Cite as *State v. Mahan*, 2011-Ohio-5154.]

Court of Appeals of Ohio

EIGHTH APPELLATE DISTRICT
COUNTY OF CUYAHOGA

JOURNAL ENTRY AND OPINION
No. 95696

STATE OF OHIO

PLAINTIFF-APPELLEE

vs.

JAMES MAHAN

DEFENDANT-APPELLANT

JUDGMENT:
AFFIRMED AND REMANDED

Criminal Appeal from the
Cuyahoga County Court of Common Pleas
Case No. CR-525553

BEFORE: Sweeney, J., Stewart, P.J., and Celebrezze, J.

RELEASED AND JOURNALIZED: October 6, 2011

ATTORNEY FOR APPELLANT

Ronald L. Frey, Esq.
Ian N. Friedman & Associates, L.L.C.
1304 West Sixth Street
Cleveland, Ohio 44113

ATTORNEYS FOR APPELLEE

William D. Mason, Esq.
Cuyahoga County Prosecutor
By: T. Allan Regas, Esq.
Francine B. Goldberg, Esq.
Assistant County Prosecutors
The Justice Center, 9th Floor
1200 Ontario Street
Cleveland, Ohio 44113

JAMES J. SWEENEY, J.:

{¶ 1} Defendant-Appellant, James Mahan, appeals from the trial court's denial of his motion to suppress and his motion to compel. Appellant also appeals the sentence imposed upon him. For the reasons that follow, we affirm but remand with instructions to reclassify defendant as a Tier II sex offender as both parties conceded at oral argument defendant was improperly classified as a Tier III sex offender.[1]

[1]The sentencing transcript reflects that the court informed defendant he would be labeled a Tier II sex offender. Accordingly, the sentencing journal entry contains an obvious clerical error to the extent it provides that "defendant is a Tier III sex offender."

{¶ 2} In this case, defendant was indicted with 95 counts, including pandering sexually-oriented matter involving a minor, illegal use of a minor in nudity-oriented material or performance, and possessing criminal tools. The charges stemmed from the presence of certain files found on defendant's home computer as a result of an investigation conducted by Rick McGinnis ("McGinnis"). McGinnis is an investigator assigned to Ohio's Internet Crimes Against Children Task Force ("ICAC"). McGinnis utilized software known as "Peer Spectre," which identified an internet protocol ("IP") address associated with three files that he recognized from his experience as being child pornography. McGinnis prepared an affidavit and obtained a search warrant for defendant's residence.

{¶ 3} During the course of the proceedings, defendant filed a motion to compel certain information from the state, including a mirror image forensic copy of Peer Spectre and any and all instruction/operation and/or training manuals associated with Peer Spectre, and the software's source code. Defendant believed the information would reveal the functionality and calibration of the software, and asserted it was material to his defense in order to challenge the software's reliability and methodology.

{¶ 4} In opposition, the state maintained the requested discovery was not subject to disclosure by the state pursuant to Crim.R. 16. Specifically, the state indicated that Peer Spectre is maintained under the strict control and ownership of William Wiltse and is restricted to use by law enforcement. Wiltse supplied an affidavit wherein he averred

that "without the source code, it is not possible to authenticate the function of the application or validate its 'calibration.'" Wiltse averred that the source code is not distributed. Officers are trained how to validate the findings of Peer Spectre by "conducting similar searches on the Gnutella network using freely available software applications." The state confirmed that it did not own or have in its possession a copy of the source code and maintained that it could not produce what it did not have. The trial court denied the motion to compel discovery from the state and instructed that defendant could contact the software company regarding issues pertaining to programming.

{¶ 5} The trial court conducted a hearing on defendant's motion to suppress and the motion was denied. Defendant then entered a plea of no contest and was found guilty. The trial court imposed an aggregate prison sentence of 16 years comprised of the following: eight year concurrent prison terms on 11 counts to be served consecutively with eight year concurrent prison terms on 70 other counts; all concurrent with four and one year prison terms on the remaining counts.

{¶ 6} Defendant's appeal presents four assignments of error for our review:

{¶ 7} "I. The trial court erred when it denied the defendant-appellant's motion to suppress."

{¶ 8} "Appellate review of a trial court's ruling on a motion to suppress presents mixed questions of law and fact. An appellate court is to accept the trial court's factual findings unless they are clearly erroneous. We are therefore required to accept the factual

determinations of a trial court if they are supported by competent and credible evidence. The application of the law to those facts, however, is subject to de novo review." *State v. Polk*, (Internal citations omitted) Cuyahoga App. No. 84361, 2005-Ohio-774, at ¶2.

{¶ 9} Under this asserted error, defendant raises multiple issues that allege that: (1) the trial court erred in its findings of fact and conclusions of law; (2) the warrantless use of Peer Spectre constituted an unlawful search in violation of his constitutional rights; (3) the search warrant was issued without probable cause because it relied on information obtained from use of Peer Spectre; and (4) the probable cause finding for the search warrant was based upon an affidavit that contained substantive inaccuracies and omissions.

{¶ 10} The trial court conducted an evidentiary hearing on defendant's motion to suppress at which McGinnis was the only witness.

{¶ 11} McGinnis testified as follows: He obtained training on internet investigations of child pornography from Fox Valley Technical College, and the training included peer-to-peer network searches. As part of his training, he was instructed on the use of Peer Spectre, which is exclusively restricted to law enforcement. Peer Spectre is a search program that operates on the Gnutella network, which is a public peer-to-peer network where people share their computer files back and forth. The Gnutella network enables people to log onto the internet to search, find, retrieve, and download shared files from other computers, including child pornography. The search will reveal an IP address

and SHA1 values,[2] and from this information the user can download the desired file from the computer(s) that offered to share it.

{¶ 12} McGinnis repeatedly testified that all the information he obtained from using Peer Spectre he could have obtained using other publicly available software, such as LimeWire or Phex, the only difference being that with the other software he would have to manually enter the data to keep searching. McGinnis stated that Peer Spectre saves time.

{¶ 13} In short, Peer Spectre conducts an automated search that identifies file sharing of known or suspected child pornography associated with a specific IP address. While McGinnis acknowledged that he did not create Peer Spectre and was unaware of the technical aspects of it, he testified that he was trained how to operate it and understood that it reads publicly available advertisements from computers that are sharing files over the Gnutella peer-to-peer network.

{¶ 14} Each time that Peer Spectre is used by a law enforcement agency anywhere in the world, the results are compiled in a centralized server. The information that is logged into the central database includes the IP address, the port that it came from, and

---

[2]SHA1 stands for Secure Hash Algorithm 1, which consists of 32 digits and functions as a file's digital signature or unique identifier, which cannot be altered. McGinnis testified that SHA1 values are accurate in identifying a file to the 160th degree, which is "better than DNA." There is a certainty exceeding 99.99 percent that two or more files with the same SHA1 value are identical copies of the same file regardless of the file name.

the date and time of the search. Law enforcement agencies are then enabled to query the information that Peer Spectre recorded into the central server.

{¶ 15} On May 23, 2008, McGinnis used this technology to search for IP addresses that were active in Ohio in May of 2008 and had been recorded as sharing known or suspected child pornography. McGinnis retrieved a "hit list" for the IP addresses at issue, which identified each file's SHA1 value, the date and time the file was made available for sharing, and the file's size, geographical location, and description. The records identified a particular IP address as a computer that made available for sharing known or suspected child pornography on May 12, 2008. From his experience, McGinnis recognized some of the SHA1 values as known child pornography. McGinnis nonetheless personally reviewed each file just to ensure that it was what he believed it to be. Portions of these files were played during defendant's suppression hearing and corroborated McGinnis's testimony as to their content of child pornography.

{¶ 16} Each IP address is unique to a certain computer at a given time. McGinnis subpoenaed the internet service provider ("ISP") for the subscriber associated with that IP address at that time. He received the customer name and account holder, which was defendant, however, this information does not identify who was actually using the computer at the relevant time. Therefore, McGinnis was not targeting defendant but instead he sought and obtained a search warrant for the residential address based upon his belief that a computer at that address contained the suspected contraband.

{¶ 17} McGinnis prepared a lengthy affidavit setting forth the basis upon which he was seeking the search warrant, which the court subsequently issued. McGinnis stated that this search warrant was executed in conjunction with approximately 60 other similar search warrants as part of Operation Safety Net. During the search, the known child pornography files that had been identified by Peer Spectre were found on defendant's computer.

{¶ 18} McGinnis testified that this was the first time he had used information gained from Peer Spectre to obtain search warrants, however, he was aware of Peer Spectre's accuracy from other law enforcement agencies. By the suppression hearing, it had become McGinnis's experience that whenever they located a computer through the use of Peer Spectre, they found child pornography on the computer unless the hard drive had been wiped clean. Under cross-examination, McGinnis stated that he could not testify to the technological processes Peer Spectre uses when it is functioning. However, he knew that Peer Spectre logs onto the same peer-to-peer network as any other publicly available software in order to perform its functions. The defense elicited an admission from McGinnis that he did not know if the files were located in a "shared folder."

{¶ 19} While McGinnis more than once testified that he did not know if Peer Spectre went beyond shared folders of a computer, he consistently confirmed that the information recorded by Peer Spectre is "identical to the information that you would get from running a search in LimeWire if you were running it at that time that the IP address

had a computer sharing file." Peer Spectre simply automated the process. There was no evidence introduced that these publicly available software programs search beyond shared files on the network; in fact, McGinnis testified that he was unaware of that ever happening.

{¶ 20} With regard to defendant's assignment of error, it is well settled that "the protections of the Fourth Amendment only extend to places where 'the defendant can claim a reasonable expectation of privacy.'" *United States v. Norman* (Sept. 24, 2010), M.D. Ala. No. 2:09-CR-118-WKW, quoting *Katz v. United States* (1967), 389 U.S. 347, 360, 88 S.Ct. 507, 9 L.Ed.2d, 576, other citations omitted. "'What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.'" Id., quoting *Katz*, 389 U.S. at 351.

{¶ 21} The state maintains that the use of Peer Spectre without a warrant did not violate defendant's constitutional right to be free from unreasonable searches and seizures because it simply automated the ability to search information that had been placed in the public domain. In other words, the program searches those files that have been placed in a public file-sharing network. Therefore, the first issue becomes whether defendant had a reasonable expectation of privacy in the subject files.

{¶ 22} At least one federal court that has confronted this issue concluded there is no reasonable expectation of privacy over files searched using Peer Spectre. *Norman,* supra (finding "a 'search' is not at issue unless the defendant first establishes that he or

she had a reasonable expectation of privacy in the area(s) searched. In other words, Mr. Norman must establish that he has standing to assert a Fourth Amendment violation in the first place. This he cannot do").

{¶ 23} In *Norman*, the court observed, "courts addressing this issue have uniformly held that there is no reasonable expectation of privacy in files made available to the public through peer-to-peer file-sharing networks." Id., citing *United States v. Stults* (C.A.8, 2009), 575 F.3d 834, 842-843; *United States v. Ganoe* (C.A.9, 2008), 538 F.3d 1117, 1127; *United States v. Perrine* (C.A.10, 2008), 518 F.3d 1196, 1205; *United States v. Laduea* (Apr. 7, 2010), D.Mass. No. 09-40021-FDS; *United States v. Brese* (Apr. 9, 2008), W.D.Okla. No. CR-08-52-D.

{¶ 24} Defendant asserts that McGinnis's inability to testify as to the specific functionality of Peer Spectre wrongly placed the burden of proof on him. However, defendant has not challenged or refuted the evidence that indicated the files from an IP address assigned to his computer were being shared over a peer-to-peer network on May 12, 2008, and therefore he has not established a reasonable expectation of privacy. Where there is no reasonable expectation of privacy over the shared files, the technical aspects of the law enforcement software are not at issue. *Norman*, supra.

{¶ 25} Next we address defendant's argument that, as a means of establishing probable cause, McGinnis's affidavit could not be based on information he obtained through Peer Spectre in the absence of testimony concerning the technical functionality of

the software. However, "probable cause is a fluid concept — turning on the assessment of probabilities in particular factual contexts — not readily, or even usefully, reduced to a neat set of legal rules." *Illinois v. Gates* (1983), 462 U.S. 213, 232, 103 S.Ct. 2317, 76 L.Ed.2d 527; *State v. Akers*, Butler App. No. CA2007-07-163, 2008-Ohio-4164.

{¶ 26} Crim.R. 41(C) provides in part:

{¶ 27} "(1) A warrant shall issue on either an affidavit or affidavits sworn to before a judge of a court of record or an affidavit or affidavits communicated to the judge by reliable electronic means establishing the grounds for issuing the warrant. The affidavit shall name or describe the person to be searched or particularly describe the place to be searched, name or describe the property to be searched for and seized, state substantially the offense in relation thereto, and state the factual basis for the affiant's belief that such property is there located. * * *

{¶ 28} "(2) * * * The finding of probable cause may be based upon hearsay in whole or in part, provided there is a substantial basis for believing the source of the hearsay to be credible and for believing that there is a factual basis for the information furnished. * * *."

{¶ 29} The gravamen of defendant's position is that probable cause was lacking because McGinnis was unable to testify as to the technical functionality of Peer Spectre and whether it was somehow able to search beyond what is shared, because he did not know Peer Spectre's standard of error. Defendant has not provided us with a single

authority, in Ohio or otherwise, that found suppression was warranted where law enforcement obtained a search warrant based on the use of technology that searches open peer-to-peer networks. Instead, defendant equates information gathered from Peer Spectre to information gathered from a confidential informant. As such, defendant maintains, McGinnis was required to set forth underlying circumstances from which he concluded that the software was credible or reliable.

{¶ 30} Assuming without deciding that the use of computer software is equivalent to obtaining information from a confidential informant, the affidavit supplied a probable cause basis to believe that the software was credible and reliable.

{¶ 31} In *Gates v. Illinois* (1983), 462 U.S. 213, 217, 103 S.Ct. 2317, 76 L.Ed.2d 527, the United States Supreme Court considered "the application of the Fourth Amendment to a magistrate's issuance of a search warrant on the basis of a partially corroborated anonymous informant's tip." In *Gates*, the Court reasoned, "[a]n informant's 'veracity,' 'reliability,' and 'basis of knowledge' are all highly relevant in determining the value of his report. * * * [T]hese elements * * * should be understood simply as closely intertwined issues that may usefully illuminate the common sense, practical question whether there is 'probable cause' to believe that contraband or evidence is located in a particular place." Id. at 230.

{¶ 32} "Sufficient information must be presented to the magistrate to allow that official to determine probable cause; his action cannot be a mere ratification of the bare

conclusions of others." Id. at 239. For example, an officer's statement that he has received "reliable information from a credible person" and does "believe" that contraband would be found at a home, is insufficient standing alone to create probable cause to support a search warrant. Id. Conversely, "an affidavit relying on hearsay 'is not to be deemed insufficient on that score, so long as a substantial basis for crediting the hearsay is presented.' * * * [E]ven in making a warrantless arrest an officer 'may rely upon information received through an informant, rather than upon his direct observations, so long as the informant's statement is reasonably corroborated by other matters within the officer's knowledge.'" Id. at 242.

{¶ 33} *Gates* directs appellate courts to employ a totality of the circumstances analysis to determine whether probable cause supported the issuance of a search warrant. Id. at 238. *Gates* also provides that "after-the-fact scrutiny by courts of the sufficiency of an affidavit should not take the form of de novo review. A magistrate's 'determination of probable cause should be paid great deference by reviewing courts.'" Id. at 236, other citation omitted; see, also, *State v. George* (1989), 45 Ohio St.3d 325, 330.

{¶ 34} There is a presumption of the validity of a warrant affidavit, which the defendant can overcome by an offer of proof showing the affidavit contained a knowing, intentional, or reckless falsity. *State v. Roberts* (1980), 62 Ohio St.2d 170, 178, citing *Franks v. Delaware*, 438 U.S. 154, 98 S.Ct. 2674, 57 L.Ed.2d 667. However, the validity of the affidavit will not be overcome by such showing if, when the "affidavit material

alleged to be false is excluded from the affidavit, there remains sufficient content in the affidavit to support a finding of probable cause." Id., citing *Franks*, 438 U.S. at 171-172.

{¶ 35} The questions before us are (1) whether, under the totality of the circumstances, the affidavit provided a substantial basis for the judge's conclusion that there was a fair probability that child pornography would be found on a computer in the defendant's residence, and (2) whether there remains sufficient content in the affidavit to support the warrant after any false information is excluded. In each regard, we find in the affirmative.

{¶ 36} McGinnis's affidavit and testimony adequately provided a substantial basis for concluding that the information obtained from Peer Spectre was credible and reliable, including, but not limited to the following: McGinnis has many years of experience investigating internet child pornography. He was aware of Peer Spectre's accuracy based on information he learned from other agencies. He was trained specifically on the use of Peer Spectre and knew that Peer Spectre searches peer-to-peer, or file sharing, networks. McGinnis had used other software programs to search peer-to-peer networks and obtained the same information he got from using Peer Spectre. He has never known the other programs to search beyond shared files.

{¶ 37} McGinnis located an IP address recorded as sharing files on May 12, 2008, three of which he recognized as being child pornography from his years of experience. He independently corroborated this by viewing the files. McGinnis obtained the account

holder information associated with that IP address from the ISP. Accordingly, there was a sufficient factual basis to establish probable cause to believe that a computer containing child pornography files was located at defendant's residence.

{¶ 38} Defendant maintains that probable cause is lacking unless law enforcement downloaded or confirmed that the suspect files from the computer were contraband before obtaining the search warrant. In order to support a probable cause determination, the totality of the circumstances need only indicate a fair probability, not a certainty, that the contraband will be found at the place to be searched. *United States v. Cartier* (C.A.8, 2008), 543 F.3d 442. In *Cartier*, the court upheld the denial of a motion to suppress where the FBI relied on information supplied by the Spanish Guardia that defendant had downloaded child pornography from a peer-to-peer file sharing network. Cartier, like defendant, argued that probable cause for the search warrant was lacking because the FBI had not verified the reliability of the software prior to obtaining the warrant. The court rejected the argument finding the evidence established that the FBI knew the Spanish Guardia "to be a reliable law enforcement agency that used a trustworthy means of computer forensics." Id. at 446. McGinnis's testimony likewise establishes his knowledge that Peer Spectre is a trustworthy source of information used by law enforcement agencies.

{¶ 39} Defendant's first assignment of error is overruled.

{¶ 40} "II. The Trial Court erred when it denied the defendant-appellant's motion to compel and failed to hold a hearing or issue findings of fact or conclusions of law."

{¶ 41} The granting or denial of a motion to compel discovery is reviewed under an abuse-of-discretion standard. The inquiry is whether the trial court's decision is unreasonable, arbitrary, or unconscionable. *State ex rel. V. Cos. v. Marshall* (1998), 81 Ohio St.3d 467, 469, 692 N.E.2d 198.

{¶ 42} The trial court denied defendant's motion to compel a mirror image forensic copy of Peer Spectre used in the investigation, any and all instruction/operation and/or training manuals associated with the software, and Peer Spectre's source code. The court's order instructed defendant to contact the software company regarding issues pertaining to the programming of Peer Spectre.

{¶ 43} Defendant had urged the court to compel production of the information from the state pursuant to Crim.R. 16(B)(1)(c),[3] which provided:

{¶ 44} "(c) Documents and tangible objects. Upon motion of the defendant the court shall order the prosecuting attorney to permit the defendant to inspect and copy or photograph books, papers, documents, photographs, tangible objects, buildings or places, or copies or portions thereof, *available to or within the possession, custody or control of the state, and which are material to the preparation of his defense, or are intended for use*

[3]Amendments to Crim.R. 16 took effect on July 1, 2010 and now set forth equivalent provisions in Crim.R. 16(B)(3).

by the prosecuting attorney as evidence at the trial, or were obtained from or belong to the defendant." (Emphasis added.)

{¶ 45} Defendant also cites to the provisions of Crim.R. 16, which require the production of mental examinations and scientific tests within the possession, custody or control of the state, evidence known or which may become known to the state that is favorable to defendant, and material relevant to either guilt or punishment.

{¶ 46} The information sought by defendant is not a mental examination or scientific test and was not subject to production on that basis. While defendant speculates that the information may have been favorable to him in challenging the reliability of the software's results, the state maintains that it did not have possession, custody or control of the information. The evidence supports the state's position. Peer Spectre's owner, Wiltse, averred in his affidavit that Peer Spectre is copyrighted, the source code is not distributed to anyone, and the use of Peer Spectre is restricted to trained law enforcement officers. Wilste averred that defendant could not discern how the software application used by the state operated without the source code.

{¶ 47} Alternatively, the state contends the information is not material to the defense, and the release of the restricted use software would compromise a worldwide network of trained law enforcement personnel and possibly the database.

{¶ 48} Defendant asserts that the information would enable him to challenge the reliability of the results of the software. However, the evidence establishes that an

expert would be unable to test the reliability of the software without the source code, which was not available to, or accessible by, the state. At least one federal court has denied a similar request for production of the FBI's proprietary enhanced LimeWire program, finding that its production would not yield any information material to the defense, particularly because the source code was locked and, therefore, the expert could not discern how it operates. See *United States v. Budziak* (May 14, 2009), N.D.Cal. No. CR08-00284. That logic applies equally here.

{¶ 49} Because the state was not in possession of the source code, and without it one cannot discern how the software operates, the trial court did not abuse its discretion by denying the motion to compel, and this assignment of error is overruled.

{¶ 50} "III. The defendant-appellant's right to due process of law as guaranteed by Article 1, Section 10 of the Ohio State Constitution and the Fourteenth Amendment to the United States Constitution was violated when he was sentenced to sixteen (16) years."

{¶ 51} "IV. The court's imposition of consecutive sentences, without making appropriate findings and reasons as required by R.C. §2929.14, violated the defendant-appellant's right to due process of law as guaranteed by Article I, Section 10 of the Ohio State Constitution and the Fourteenth Amendment to the United States Constitution."

{¶ 52} The third and fourth assignments of error are overruled.

{¶ 53} The two-fold analysis for reviewing sentences is first to determine whether the trial court complied with all applicable rules and statutes when imposing the sentence such that the sentence is not "clearly and convincingly contrary to law," and if so, second, to examine if the trial court's sentence constitutes an abuse of its discretion. *State v. Kalish*, 120 Ohio St.3d 23, 2008-Ohio-4912, 896 N.E.2d 124, ¶4.

{¶ 54} Defendant contends his sentence is not supported by clear and convincing evidence and is contrary to law. He also argues that the trial court abused its discretion by imposing a 16-year sentence.

{¶ 55} The trial court imposed the maximum sentence of eight years on 81 counts of the indictment. Then the court grouped the offenses into categories. The court segregated Counts 1 through 11, which involved images defendant made available for sharing, from Counts 12 through 81, which were based on images/videos found on defendant's computer hard drive that depicted children involved in sexual acts. For all counts in each grouping, defendant received maximum but concurrent eight-year prison terms, however, the sentences in Counts 1 through 11 were to be served consecutively to the sentences in counts 12 through 81, for an aggregate term of 16 years in prison. The court then imposed a four year prison sentence for Counts 82 through 94, which involved images that depicted nude children but did not involve any sexual acts, and imposed a one-year prison term on the final count for possessing criminal tools, i.e., the computer.

The court ordered those sentences to be served concurrently with the 16-year prison term.[4]

{¶ 56} Defendant argues that the maximum sentence on 82 counts, as well as the imposition of consecutive sentences, was not supported by sufficient reasoning and does not comport with the purposes of felony sentencing set forth in R.C. 2929.11 and 2929.12. The court was not, and is not presently, required to make findings on the record prior to imposing maximum or consecutive sentences. *State v. Foster*, 109 Ohio St.3d 1, 2006-Ohio-856, 845 N.E.2d 470; *State v. Hodge*, 128 Ohio St.3d 1, 2010-Ohio-6320, 941 N.E.2d 768.[5] Rather, the court is bound to consider Ohio's felony sentencing statutes. *Foster*, 2006-Ohio-856; see, also, *State v. Mathis*, 109 Ohio St.3d 54, 62, 2006-Ohio-855, 846 N.E.2d 1.

{¶ 57} In imposing its sentence, the court noted that it is "well-known the defendant has otherwise been a law-abiding, productive citizen." The record reflects a long marriage to his wife and that they raised a daughter who is successful. Defendant's wife, daughter, and others in their community continued to support him throughout these proceedings and advocated on his behalf at sentencing. According to the record,

---

[4]The sentencing order further addressed forfeiture specifications and terms of postrelease control, which are not at issue in this appeal.

[5]We note that on September 30, 2011, amendments to Ohio's sentencing law will take effect.

defendant immediately commenced treatment, which he continued throughout the two years the matter was pending in the lower court, reportedly attending more than 100 meetings and participating in group and individual therapy. Defendant maintained gainful employment until his arrest, after which he sought and obtained new employment. The state emphasized the fact that defendant's career was largely spent around young children as an aquatics instructor, suggesting this should be considered within the context of his offenses. The court noted that defendant had never been accused of engaging in the type of conduct depicted in the images he possessed or shared, and he could not be sentenced based upon potential future offenses. A polygraph test indicated that he had never molested any children. Defendant's Static-99 score placed him in the lowest possible category for recidivism risk. Defendant cooperated with police, although the state insisted that he minimized his culpability by indicating the individuals involved were girls between 12 and 18, rather than younger.

{¶ 58} The court emphasized that defendant's conduct victimized the subjects of the child pornography every time the media is viewed, shared, or downloaded. Defendant recognized this harm, which he discussed during his allocution. Defendant stated he had an addiction, which escalated as he focused on younger and younger subjects. The court cited this admission during sentencing. Defendant acknowledged the heinous nature of the crimes, which was echoed by the state as well as the court. The state described other sexually explicit content found on defendant's computer, including

96,000 photographs. Furthermore, the parties stipulated that the state was seeking sentencing regarding the 52 victims who formed the basis for defendant's indictment.

{¶ 59} The record establishes that defendant's conduct was "relentless and ongoing" for a period of eight years until he was stopped by law enforcement intervention. With respect to the images found on defendant's computer, the court expressed, "[e]verything you could possibly imagine occurred on this computer. And everything you could possibly imagine was shared with other individuals."

{¶ 60} Defendant asserts that his sentence is inconsistent with sentences imposed for similar crimes by similar offenders. He refers us to sentencing journal entries from other cases in this district where individuals convicted of multiple counts of pandering sexually-oriented matter involving a minor received lesser sentences than his, ranging from community control sanctions to four years in prison. According to defendant, all of those individuals were also indicted as a result of Operation Safety Net. However, these journal entries tell us little, if anything, of the offender characteristics and provide no information beyond the convictions and terms of the sentences.

{¶ 61} On the other hand, our research has revealed that in at least one other case an individual who was indicted in the same investigation received the same 16-year sentence as defendant, which this court upheld. See *State v. Cooper,* Cuyahoga App. No. 93308, 2010-Ohio-1983, ¶19-21.

{¶ 62} Cooper was indicted following an investigation by Ohio's ICAC, which indicated he was using file sharing software to access child pornography. *Cooper*, 2010-Ohio-1983, ¶4. Cooper pled guilty to four counts of pandering sexually-oriented material involving a minor and possessing criminal tools. Cooper also cooperated with the investigation and gave a statement to police. Similar to this case, Cooper's ex-wife spoke on his behalf at sentencing, indicating that "he has been working hard to get help." Cooper, like defendant, was actively involved in AA and was obtaining counseling prior to his sentencing. He expressed remorse for his behavior, which was noted as being "considerable." While a similarly situated offender, Cooper was convicted of significantly fewer counts than defendant but still received a 16-year prison term. Defendant's sentence was consistent with Cooper's sentence.

{¶ 63} We acknowledge that a 16 year prison term imposed on a first-time offender who has, by all accounts, led an otherwise productive, law abiding life is a harsh sentence and is perhaps not one that we may have imposed. Nonetheless, the sentence was significantly less than what the court could have imposed based on defendant's 95 convictions. There was ample testimony in the record of the harm that has been, and continues to be, inflicted upon the victims who are the subjects of the material being viewed in these types of cases. The images, once uploaded, continue to circulate on the internet where individuals, like defendant, view them and make them available for viewing by others. The wide range of sentences that have been apparently imposed on

defendants convicted of similar offenses is the result of the discretion vested in the trial court. Defendant's sentence was within the statutory range, lawful, and supported by the record, thus we cannot say it was unconscionable or otherwise an abuse of the trial court's discretion.

{¶ 64} The third assignment of error is overruled.

{¶ 65} Judgment affirmed, and the case is remanded to correct the sentencing journal entry to accurately reflect defendant's classification as a Tier II sex offender.

It is ordered that appellee recover of appellant its costs herein taxed.

The Court finds there were reasonable grounds for this appeal.

It is ordered that a special mandate issue out of this Court directing the Common Pleas Court to carry this judgment into execution. The defendant's conviction having been affirmed, any bail pending appeal is terminated. Case remanded to the trial court for execution of sentence.

A certified copy of this entry shall constitute the mandate pursuant to Rule 27 of the Rules of Appellate Procedure.

JAMES J. SWEENEY, JUDGE

MELODY J., STEWART, P.J., and
FRANK D. CELEBREZZE, JR., J., CONCUR