[Cite as *State v. Fielding*, 2014-Ohio-3105.]

IN THE COURT OF APPEALS OF OHIO

TENTH APPELLATE DISTRICT

State of Ohio,	:	
Plaintiff-Appellee,	:	No. 13AP-654 (C.P.C. No. 12CR-2800)
v.	:	No. 13AP-655 (C.P.C. No. 13CR-1564)
Matthew N. Fielding,	:	
Defendant-Appellant.	:	(REGULAR CALENDAR)

D E C I S I O N

Rendered on July 15, 2014

Ron O'Brien, Prosecuting Attorney, and *Seth L. Gilbert*, for appellee.

Tyack, Blackmore, Liston & Nigh Co., L.P.A., and *Jonathan T. Tyack*, for appellant.

APPEALS from the Franklin County Court of Common Pleas.

BROWN, J.

{¶ 1} In this consolidated appeal, defendant-appellant, Matthew N. Fielding, appeals the judgment of the Franklin County Court of Common Pleas in case No. 12CR-2800, in which the court found him guilty, pursuant to a bench trial, of three counts of pandering sexually oriented matter involving a minor in violation of R.C. 2907.322(A)(5), felonies of the fourth degree; and the judgment of the Franklin County Court of Common Pleas in case No. 13CR-1564, in which the court found him guilty, pursuant to a bench trial, of three counts of pandering sexually oriented matter involving a minor in violation of R.C. 2907.322(A)(5), felonies of the fourth degree, and one count of pandering sexually oriented matter involving a minor in violation of R.C. 2907.322(A)(1), a felony of the second degree.

{¶ 2} Upper Arlington Police Officer John Priest, an investigator and computer forensics examiner assigned to the multi-jurisdictional Internet Crimes Against Children ("ICAC") Task Force, monitors peer-to-peer file-sharing networks, including Gnutella, for distribution of child pornography. Peer-to-peer networks such as Gnutella allow users both to share with other network users files they have created or downloaded and to access files created or downloaded by other network users. The Gnutella network is accessible through a number of free file-sharing programs available for download on the internet, including the Shareaza program.

{¶ 3} On June 22, 2010, Officer Priest was searching for files containing titles indicative of child pornography via a software program utilized by law enforcement known as "Roundup." "Roundup" permits the downloading of files from a remote computer onto an investigative computer accessible only to law enforcement. Officer Priest identified a particular internet protocol address ("IP address") that contained file names commonly associated with child pornography.[1] Officer Priest established a direct connection with the computer associated with the IP address, downloaded a video file from that computer, and confirmed that the file contained child pornography. He subsequently determined that the computer associated with the IP address belonged to an AT&T internet customer.

{¶ 4} Based on these findings, Officer Priest prepared an investigative subpoena, which was signed by a Franklin County Municipal Court judge, to obtain from AT&T the subscriber information associated with the IP address. In response to the subpoena, AT&T, via a facsimile transmission, identified appellant as the internet subscriber assigned to the IP address in question and provided appellant's home address, home telephone number, and e-mail address. Officer Priest forwarded this information to a fellow ICAC Task Force member, Detective Jane Junk of the Columbus Division of Police, who thereafter obtained a search warrant for appellant's residence.

{¶ 5} Detective Junk and Franklin County Sheriff's Office Detective Marcus Penwell, another member of the ICAC Task Force, executed the search warrant at

[1] Officer Priest defined an IP address as "a series of numbers that identify a physical location, much like a mailbox and a postal address identifies a physical location[,] that's used to direct Internet traffic to a specific router or house where the router exists." (Apr. 4, 2013 Tr., 25.)

appellant's residence on September 7, 2010. Pursuant to the search, a laptop computer and an external hard drive were seized from a bedroom office. Subsequent forensic analysis of both devices revealed multiple files containing child pornography.

{¶ 6} As a result, a Franklin County Grand Jury returned two separate eight-count indictments against appellant. The first, issued on June 5, 2012 in case No. 12CR-2800, charged appellant with four counts of pandering sexually oriented matter involving a minor in violation of R.C. 2907.322(A)(1), second-degree felonies, stemming from four separate files allegedly transferred onto the external hard drive on August 1, 2007, July 23, May 21, and April 19, 2008 (Counts 1, 2, 3, and 4), and four counts of pandering sexually oriented matter involving a minor in violation of R.C. 2907.322(A)(5), fourth-degree felonies, arising out of the September 7, 2010 discovery of those files on the external hard drive (Counts 5, 6, 7, and 8). The second indictment, returned on March 21, 2013 in case No. 13CR-1564, charged appellant with four counts of pandering sexually oriented matter involving a minor in violation of R.C. 2907.322(A)(1), second-degree felonies, stemming from four separate files allegedly downloaded onto the laptop computer on June 22, July 8, July 11-12, and June 21, 2010 (Counts 1, 2, 3 and 4), and four counts of pandering sexually oriented matter involving a minor in violation of R.C. 2907.322(A)(5), fourth-degree felonies, arising out of the September 7, 2010 discovery of those files on the laptop computer (Counts 5, 6, 7, and 8).[2]

{¶ 7} Appellant filed a pre-trial motion to suppress under both case numbers. Appellant argued that law enforcement illegally obtained his subscriber information from AT&T; accordingly, the subscriber information, as well as all derivative evidence, including the search of his residence, all evidence seized during the search, and all statements appellant made during the search, should be suppressed. Following consolidation of the cases, the matter proceeded for hearing on the motion to suppress. At the conclusion of the hearing, the trial court denied the motion.

{¶ 8} Appellant waived his right to a jury trial and agreed to have the consolidated cases tried to the bench. The parties stipulated that all evidence and testimony presented at the suppression hearing would be incorporated into the trial proceeding. Following the

[2] At trial, the state, without objection by appellant and with the trial court's authorization, amended the date of Count 5 of the indictment in case No. 13CR-1564 to June 22, 2010.

bench trial, the court issued decisions finding appellant guilty in case No. 12CR-2800 of Counts 6, 7, and 8 (pandering sexually oriented matter involving a minor in violation of R.C. 2907.322(A)(5)), and guilty in case No. 12CR-1654 of Count 1 (pandering sexually oriented matter involving a minor in violation of R.C. 2907.322(A)(1)) and Counts 5, 6, and 7 (pandering sexually oriented matter involving a minor in violation of R.C. 2907.322(A)(5). The court acquitted appellant of the other crimes charged in the indictments.

{¶ 9} Following a July 2013 sentencing hearing, the trial court sentenced appellant to a seven-day jail term, a five-year term of community control, and ordered that he register as a Tier II sex offender. Thereafter, the trial court issued a judgment entry memorializing its decisions and sentencing.

{¶ 10} In a timely appeal, appellant asserts the following three assignments of error:

> I. THE TRIAL COURT ERRED IN OVERRULING APPELLANT'S MOTION TO SUPPRESS ALL EVIDENCE ARISING OUT OF OR RESULTING FROM THE INVESTIGATIVE SUBPOENA SENT TO AT&T BY LAW ENFORCEMENT FOR THE PURPOSE OF DETERMINIG APPELLANT'S IDENTITY.
>
> II. THE TRIAL COURT ERRED IN OVERRUING APPELLANT'S MOTION FOR JUDGMENT OF ACQUITTAL AS TO ALL COUNTS IN BOTH INDICTMENTS PURSUANT TO RULE 29 OF THE OHIO RULES OF CRIMINAL PROCEDURE.
>
> III. APPELLANT'S CONVICTIONS ARE AGAINST THE MANIFEST WEIGHT OF THE EVIDENCE.

{¶ 11} Appellant argues in his first assignment of error that the trial court erred in denying his motion to suppress. "Appellate review of a motion to suppress presents a mixed question of law and fact." *State v. Burnside*, 100 Ohio St.3d 152, 2003-Ohio-5372, ¶ 8. In a motion to suppress, the trial court assumes the role of fact finder and thus is in the best position to resolve factual questions and evaluate witness credibility. *Id.*, citing *State v. Mills*, 62 Ohio St.3d 357, 366 (1992). An appellate court must therefore accept the trial court's factual findings if they are supported by competent, credible evidence. *Id.*

at ¶ 8, citing *State v. Fanning,* 1 Ohio St.3d 19 (1982). Accepting those facts as true, an appellate court must then independently determine as a matter of law, without deference to the trial court's conclusion, whether the facts satisfy the applicable legal standard. *Id.* at ¶ 8, citing *State v. McNamara,* 124 Ohio App.3d 706 (4th Dist.1997).

{¶ 12} Appellant maintains the trial court erroneously failed to suppress all evidence stemming from law enforcement's illegal obtainment of his subscriber information through the investigative subpoena process. Specifically, appellant first contends that law enforcement obtained his subscriber information in violation of the Electronic Communications Privacy Act, Section 2701, et. seq., Title 18, U.S.C. ("ECPA"), which regulates the disclosure of electronic communications and subscriber information. In pertinent part, 18 U.S.C. 2703(c)(1) provides: "[a] governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity * * * (A) obtains a warrant using the procedures described * * * (in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction * * * (B) obtains a court order for such disclosure under subsection (d) of this section [or] (C) has the consent of the subscriber or customer to such disclosure." Pursuant to subsection (d), a court order "shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." Appellant contends the investigative subpoena did not qualify as a "court order" under the ECPA.

{¶ 13} Appellant also contends the investigative subpoena was invalid under R.C. 2935.23, which controls the application process for subpoenas used to aid felony investigations. Pursuant to R.C. 2935.23, witnesses must appear for examination under oath by the prosecuting attorney, the court or magistrate. In addition, the examination must be taken in writing and filed with the court or magistrate. Appellant contends the investigative subpoena was invalid because AT&T failed to appear to testify under oath.

{¶ 14} Appellant argues that he had a reasonable expectation of privacy in his subscriber information, such that the warrantless acquisition of that information through

the flawed investigative subpoena process utilized by law enforcement violated his rights under the Fourth Amendment to the United States Constitution and Ohio Constitution, Article I, Section 14.

{¶ 15} The Fourth Amendment to the United States Constitution, as applied to the states through the Fourteenth Amendment, and Ohio Constitution, Article I, Section 14, protects individuals against "unreasonable searches and seizures" by the government and protects privacy interests where an individual has a reasonable expectation of privacy. *See Smith v. Maryland,* 442 U.S. 735, 740 (1979). An expectation of privacy is protected by the Fourth Amendment where (1) an individual has exhibited a subjective expectation of privacy, and (2) that expectation of privacy is one that "society is prepared to recognize as 'reasonable.' " *Id.,* quoting *Katz v. United States,* 389 U.S. 347, 361 (1967) (Harlan, J., concurring). Generally, any evidence obtained in violation of the Fourth Amendment, as well as any evidence seized subsequent to such violation, must be suppressed as "fruit of the poisonous tree." *Wong Sun v. United States,* 371 U.S. 471, 488 (1963).

{¶ 16} Appellant acknowledges that this court and at least one other Ohio appellate court have considered and rejected the arguments raised in his motion to suppress. In *State v. Thornton,* 10th Dist. No. 09AP-108, 2009-Ohio-5125, this court noted the general principle that "[a]n individual cannot be said to have a reasonable expectation of privacy in that which he knowingly exposes to the public." *Id.* at ¶ 11, citing *State v. Lopez,* 2d Dist. No. 94-CA-21 (Sept. 28, 1994), citing *Katz.* Applying that principle, we held that Thornton had no reasonable expectation of privacy in either computer files he had made available to the public using file-sharing software or in the IP address associated with his computer. *Id.* at ¶ 12, citing *United States v. Ganoe,* 538 F.3d 1117, 1127 (9th Cir.2008); *United States v. Borowy,* 577 F.Supp.2d 1133, 1136 (D.Nev.2008); *United States v. Forrester,* 512 F.3d 500, 510 (9th Cir.2008); *United States v. Li,* S.D. Cal. No. 07 CR 2915 JM (Mar. 20, 2008). We noted that in such situations, "Fourth Amendment protections are not implicated because a search does not occur." *Thornton* at ¶ 12, citing *State v. Keith,* 10th Dist. No. 08AP-28, 2008-Ohio-6122, ¶ 16.

{¶ 17} We also addressed Thornton's assertions that his internet provider violated the ECPA in providing subscriber information to law enforcement without the subscriber's consent. *Id.* at ¶ 13-14. We found that, even if the internet provider's

disclosure violated the ECPA, the remedy for such violation "is a civil action for damages, not suppression." *Id.* at ¶ 14, citing *United States v. Perrine*, 518 F.3d 1196, 1202 (10th Cir.2008); *United States v. Beckett*, 544 F.Supp.2d 1346, 1350 (S.D.Fla.2008); *United States v. Sherr*, 400 F.Supp.2d 843, 848 (D.Md.2005); *United States v. Kennedy*, 81 F.Supp.2d 1103, 1110 (D.Kan.2000). Thus, we concluded that violation of the ECPA "would not provide [Thornton] with a basis to suppress the subscriber information." *Thornton* at ¶ 14. Finally, we determined that "a customer does not have a reasonable expectation of privacy in subscriber information given to an internet service provider." *Id.*, citing *Perrine* at 1204; *Sherr* at 848.

{¶ 18} The Twelfth District Court of Appeals has held similarly. In *State v. Hamrick*, 12th Dist. No. CA2011-01-002, 2011-Ohio-5357, Hamrick argued that law enforcement illegally obtained his subscriber information from his internet provider through use of an investigative subpoena pursuant to R.C. 2935.23. Specifically, Hamrick argued that the investigative subpoena did not qualify as a "court order" under the ECPA and that law enforcement failed to comply with R.C. 2935.23 in applying for the investigative subpoena. Concluding that the remedy of suppression was not available to Hamrick for violation of the ECPA, the court declined to address whether the investigative subpoena constituted a valid "court order" under the statute. The court further held that "[Hamrick's] constitutional rights were not violated when law enforcement obtained his subscriber information from Time Warner because he has not demonstrated an objectively reasonable expectation of privacy in this information." *Id.* at ¶ 18. After noting the well-settled general principle that " 'a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties,' " *id.* at ¶ 18, quoting *Smith* at 744, the court stated that "[w]hen appellant entered an agreement with Time Warner for internet service, he knowingly revealed the subscriber information associated with his IP address, including his name, address and telephone number." *Id.* at ¶ 19. Accordingly, the court determined that "even if law enforcement used an invalid court order to obtain [Hamrick's] subscriber information, this statutory violation would not provide [him] with a basis to suppress this information or any evidence stemming therefrom." *Id.* at ¶ 20.

{¶ 19} In *State v. Lemasters,* 12th Dist. No. CA2012-12-028, 2013-Ohio-2969, the court affirmed its holding that "a subscriber does not have a reasonable expectation of privacy with respect to his subscriber information, including the IP address associated with his internet service." *Id.* at ¶ 9, citing *Hamrick* at ¶ 19. The court also addressed Lemasters' contention that law enforcement violated the ECPA by obtaining his subscriber information from his internet provider via an investigative subpoena rather than a warrant. Noting Lemasters' argument that the investigative subpoena utilized by law enforcement was not a court order as contemplated in the ECPA because it did not follow state guidelines for a proper court order as stated in R.C. 2935.23, the court found, as it did in *Hamrick,* that the remedy Lemasters sought for the alleged violation, i.e., suppression of the evidence, was unavailable to him. The court further averred that "[w]hile Lemasters argues that his constitutional rights have been violated so that suppression is a valid remedy under the ECPA, we have already stated that Lemasters' Fourth Amendment rights were neither implicated nor violated because he had no reasonable expectation of privacy in his IP address information or the files he shared." *Id.* at ¶ 28. The court concluded, "[h]aving found that Lemasters did not have a reasonable expectation of privacy, that [law enforcement's] obtaining information from Time Warner was not a search that implicated the Fourth Amendment, and that suppression is not a valid remedy contemplated by the ECPA, the trial court did not err in denying Lemasters' motion to suppress." *Id.* at ¶ 29.

{¶ 20} Beyond Ohio, "[f]ederal courts have uniformly held that 'subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation' because it is voluntarily conveyed to third parties." *United States v. Christie,* 624 F.3d 558, 573 (3d Cir.2010), quoting *Perrine* at 1204. The court reasoned that " 'IP addresses are not merely passively conveyed through third party equipment, but rather are voluntarily turned over in order to direct the third party servers.' " *Id.* at 574, quoting *Forrester* at 510. *See also United States v. Suing,* 712 F.3d 1209, 1213 (8th Cir.2013) (defendant who chose to share pornographic files via a peer-to-peer network " 'had no expectation of privacy in [the] government's acquisition of his subscriber information, including his IP address and name from third-party service providers' "). *Id.*, quoting *United States v. Stults,* 575 F.3d 834, 842 (8th Cir.2009); *Guest v. Leis,* 255 F.3d

325, 336 (6th Cir.2001) (no Fourth Amendment privacy interest in subscriber information voluntarily communicated to systems operators); *United States v. Sawyer*, 786 F.Supp.2d 1352, 1355 (N.D.Ohio 2011) (no Fourth Amendment privacy interest in information made available on a public peer-to-peer filing sharing program, since the individual's expectation of privacy in that shared information is not objectively reasonable).

{¶ 21} Appellant contends the foregoing jurisprudence must be re-examined in light of the United States Supreme Court's decision in *United States v. Jones*, 132 S.Ct. 945 (2012). There, the Supreme Court considered whether the warrantless installation of a GPS tracking device on the defendant's vehicle violated his Fourth Amendment rights. *Id.* at 948. The Court found that the defendant's "Fourth Amendment rights do not rise or fall with the *Katz* [reasonable-expectation-of-privacy] formulation." *Id.* at 947. Rather, the Court found that the defendant's vehicle was an "effect" and that the warrantless physical trespass of that "effect" to obtain information constituted an unreasonable search under the Fourth Amendment. *Id.* at 948. Thus, the Court made clear that the Fourth Amendment is implicated where the "[g]overnment physically occupie[s] private property for the purpose of obtaining information." *Id.* at 949. However, the Court also confirmed that "[s]ituations involving merely the transmission of electronic signals without trespass would remain subject to [the] *Katz* analysis." (Emphasis omitted.) *Id.* at 953. That is, the Court stated that the "*Katz* reasonable-expectation-of-privacy test has been added to, not substituted for, the common-law trespassory test." *Id.* at 952. Relying primarily on this language and the concurring opinions of Justice Sotomayor and Justice Alito, appellant contends that *Jones* affords him a greater expectation of privacy in the subscriber information he provided to AT&T than that afforded by pre-*Jones* judicial precedent.

{¶ 22} Courts addressing this same argument have rejected it. As the court explained in *Lemasters:*

> [T]he *Jones* holding does not stand for the proposition that a person has a reasonable expectation of privacy in information that he freely shares with third parties or to files that are shared openly with others through a file-sharing program. While Lemasters spends a great amount of time in his brief quoting and referencing the concurring opinions in *Jones* that suggest that the Fourth Amendment should be stretched to

> include other privacy rights, we are bound only by the majority opinion of the court, rather than questions raised and suggestions made within the dicta of concurring opinions. Therefore, the rule of law from *Jones* that governs Fourth Amendment jurisprudence is that the placement of a GPS on one's car is trespassory in nature and that such placement requires a warrant.
>
> The trespassory nature of installing a GPS is clearly absent from the current facts of this case. Just as Hamrick freely shared his information with Time Warner, Lemasters did the same thing when he registered his information in order to make use of the Time Warner internet service. Lemasters also opened his filed for public sharing and exhibited absolutely no expectation of privacy in them. Lemasters did nothing to make his information private or to protect any expectation of privacy, and [law enforcement] did not perform any trespass in order to obtain from Time Warner the information that Lemasters openly and freely shared regarding his IP address. We decline to extend *Jones* in the manner advocated by Lemasters.

Id. at ¶ 13-14.

{¶ 23} In *Lemasters*, the court noted that its refusal to extend *Jones* to hold that a person has a reasonable expectation of privacy in information freely shared with third parties or in files shared openly with others through a file-sharing program was in accord with federal jurisprudence. The court particularly cited *United States v. Nolan*, E.D.Mo. No. 1:11 CR 82 CEJ (Mar. 6, 2012) (stating defendant's reliance on *Jones* was "misdirected"); *United States v. Brooks*, E.D.N.Y. No. 12-CR-166 (RRM) (Dec. 17, 2012) (finding defendant's attempt to apply *Jones* to be misplaced); *United States v. Conner*, 6th Cir. No. 12-3210 (Apr. 11, 2013) (court never discussed law enforcement's use of file-sharing program or obtaining IP address information as the trespassory invasion or physical intrusion contemplated by *Jones*); and *United States v. Stanley*, W.D.Pa. No. 11-272 (Nov. 14, 2012) (despite *Jones*, the court did not analyze the police investigation of the defendant's IP address as a trespassory search invoking the defendant's Fourth Amendment rights). The *Lemasters* court concluded that "[w]ell-settled legal pronouncements regarding reasonable expectation of privacy as it relates to file-sharing

and IP address information have not changed in the wake of *Jones*, and this court will not diverge from established precedent to hold otherwise." *Id.* at ¶ 22.

{¶ 24} Courts in addition to *Lemasters* and those referenced therein have refused to extend *Jones* in the manner urged by appellant. *See, e.g., Commonwealth of Virginia v. Do,* 86 Va.Cir. 483 (June 4, 2013) (rejecting Do's reliance on *Jones* because no physical intrusion occurs in the use of a search tool to monitor a peer-to-peer network and identify an IP address); *United States v. Dennis,* N.D.Ga. No. 3:13-cr-10-TCB (May 12, 2014) ("[t]he government did not use a tracking device, such as at issue in *Jones*; instead, it merely obtained information publicly available on shared files via a software program that connected with defendant's computer on which defendant had installed a file-sharing program. Thus, there was no Fourth Amendment violation tied to common law notions of trespass in this case."); and *United States v. Brashear,* M.D.Pa. No. 4:11-CR-0062 (Nov. 18, 2013) ("[s]everal courts have rejected the application of *Jones* to the investigation of file sharing programs [and] [t]his court concurs with the rationale of these decisions. The investigation of a file sharing program does not involve any physical trespass onto a constitutionally protected area.").

{¶ 25} As in the foregoing cases, and in contrast to *Jones*, there was no physical trespass onto a constitutionally protected area in the present case. Rather, Officer Priest obtained information publicly available on shared files via a software program that connected with the computer on which appellant had installed a file-sharing program. We concur in the rationale of the above-noted authorities and thus conclude that appellant's Fourth Amendment rights were not implicated by Officer Priest's obtaining appellant's subscriber information from AT&T based upon appellant's IP address. Accordingly, the trial court did not err by denying appellant's motion to suppress. Appellant's first assignment of error is overruled.

{¶ 26} We address appellant's second and third assignments of error together. In them, appellant argues that his convictions are not supported by sufficient evidence and are against the manifest weight of the evidence.

{¶ 27} Sufficiency of the evidence is a legal standard that tests whether the evidence introduced at trial is legally adequate to support a verdict. *State v. Thompkins*, 78 Ohio St.3d 380, 386 (1997). Whether the evidence is legally sufficient to support a

verdict is a question of law. *Id.* In determining whether the evidence is legally sufficient to support a conviction, " '[t]he relevant inquiry is whether, after viewing the evidence in a light most favorable to the prosecution, any rational trier of fact could have found the essential elements of the crime proven beyond a reasonable doubt.' " *State v. Robinson,* 124 Ohio St.3d 76, 2009-Ohio-5937, ¶ 34, quoting *State v. Jenks,* 61 Ohio St.3d 259 (1991), paragraph two of the syllabus. A verdict will not be disturbed unless, after viewing the evidence in a light most favorable to the prosecution, it is apparent that reasonable minds could not reach the conclusion reached by the trier of fact. *State v. Treesh,* 90 Ohio St.3d 460, 484 (2001).

{¶ 28} In a sufficiency inquiry, appellate courts do not assess whether the state's evidence is to be believed, but whether, if believed, the evidence admitted at trial supports the conviction. *State v. Yarbourgh,* 95 Ohio St.3d 227, 2002-Ohio-2126, ¶ 79 (evaluation of witness credibility not proper on review for sufficiency of evidence); *State v. Bankston,* 10th Dist. No. 08AP-668, 2009-Ohio-754, ¶ 4 (noting that "in a sufficiency of the evidence review, an appellate court does not engage in a determination of witness credibility; rather, it essentially assumes the state's witnesses testified truthfully and determines if that testimony satisfies each element of the crime").

{¶ 29} In contrast, the weight of the evidence concerns the inclination of the greater amount of credible evidence offered to support one side of the issue rather than the other. *Thompkins* at 387. Although there may be sufficient evidence to support a judgment, a court may nevertheless conclude that a judgment is against the manifest weight of the evidence. *Id.*

{¶ 30} When presented with a challenge to the manifest weight of the evidence, an appellate court may not merely substitute its view for that of the trier of fact, but must review the entire record, weigh the evidence and all reasonable inferences, consider the credibility of witnesses and determine whether in resolving conflicts in the evidence the trier of fact clearly lost its way and created such a manifest miscarriage of justice that the conviction must be reversed and a new trial ordered. *Id.* An appellate court should reserve reversal of a conviction as being against the manifest weight of the evidence for only the most " 'exceptional case in which the evidence weighs heavily against the

conviction.' " *Thompkins* at 387, quoting *State v. Martin*, 20 Ohio App.3d 172, 175 (1st Dist.1983).

{¶ 31} In addressing a manifest weight of the evidence argument, an appellate court may consider the credibility of the witnesses. *State v. Cattledge*, 10th Dist. No. 10AP-105, 2010-Ohio-4953, ¶ 6. However, in conducting such review, the court is guided by the presumption that the jury or the trial court in a bench trial " 'is best able to view the witnesses and observe their demeanor, gestures and voice inflections, and use these observations in weighing the credibility of the proffered testimony.' " *Id.*, quoting *Seasons Coal Co. v. Cleveland*, 10 Ohio St.3d 77, 80 (1984). Thus, a reviewing court must defer to the factual findings of the jury or judge in a bench trial regarding the credibility of the witnesses. *State v. DeHass*, 10 Ohio St.2d 230 (1967), paragraph one of the syllabus.

{¶ 32} The evidence presented at the bench trial (which, as noted, included by stipulation the evidence presented at the suppression hearing), is as follows. Officer Priest testified both as a factual witness and as an expert in computer forensics. Officer Priest provided an overview of the peer-to-peer file-sharing process in the context of child pornography cases. To that end, he averred that the Shareaza program permits a user to enter search terms as a means of locating files available for download from a file-sharing network. According to Officer Priest, a user searching for child pornography typically enters search terms such as "pedo," "pthc" or "kdv." (Apr. 4, 2013 Tr., 87.)[3] When a user locates a file containing the requested search terms, the user may initiate a download of the file by right-clicking or double-clicking the file; a user may also simultaneously download a number of files by highlighting the requested files and right-clicking or double-clicking the highlighted files. The time involved in the downloading process varies depending upon the size of the requested file, the availability of the file for download, and the number of individuals requesting download of the shared file.

{¶ 33} The downloading process creates a duplicate of the file on the user's computer. In essence, "a new copy of [the downloaded file] exists in the world on [the user's] computer that wasn't there before." (Apr. 4, 2013 Tr., 66.) The location of the

[3] Officer Priest testified that "pedo" is an abbreviation of "pedophile," and "pthc" is an abbreviation for "preteen hardcore." Although he was uncertain of the exact meaning of "kdv," he averred that "it typically is child pornography of a young boy nature." (Apr. 4 2013 Tr., 87.)

downloaded file on the user's computer depends upon how the user sets up "preferences" for downloading. (Apr. 4, 2013 Tr., 66.) The "default" setting in the Shareaza program automatically places downloaded files into a shared location. (Apr. 4, 2013 Tr., 66, 118.) Users may affirmatively override the default setting to prevent files from downloading into a shared location.

{¶ 34} During the downloading process, the files are available for play in the Shareaza browser through use of a "preview button." (Apr. 4, 2013 Tr., 118.) The "preview button" makes an exact copy of a file that is being downloaded at a specific point in time and permits access to the incomplete file in a temporary download location for the purpose of viewing the contents of the file. Once the incomplete file is accessed, the user then determines whether to continue the downloading process or delete the partially downloaded file.

{¶ 35} As to the facts specific to the present case, Officer Priest testified that, on June 22, 2010, he determined that a user at a particular IP address (which was subsequently determined to be registered to appellant), using the Shareaza program had downloaded a number of files with titles commonly associated with child pornography.[4] Pursuant to the default setting in the Shareaza program utilized by appellant, these files were downloaded into a shared location "that [was] being advertised out on the Internet to anybody and everybody running the same protocol * * * Shareaza, making these files available for anybody that wanted a copy of them." (Apr. 4, 2013 Tr., 27.) Utilizing the "Roundup" software, Officer Priest, in a "Single Source download," downloaded one of the files from appellant's computer to his investigative computer. (Apr. 4, 2013 Tr., 29.) Officer Priest described a "Single Source download" as one that downloads a file from another computer in a manner that assures the person downloading the file that no other individuals are contributing to the download and that it all derives from the suspect IP address. After viewing the downloaded file, Officer Priest confirmed that it contained child pornography.

[4] Officer Priest testified as to the precise titles of a number of these files. Because the precise titles are, to say the least, vulgar, we choose not to replicate them here. We note, however, that many of the titles contain some combination of the terms "pthc" and "pedo"; in addition, many contain references to underage participants.

{¶ 36} After the laptop and external hard drive were retrieved from appellant's home, Officer Priest, using specialized software, conducted two separate forensic examinations of the files and other artifacts contained on those two devices and thereafter prepared reports of his findings. This forensic analysis revealed that the Shareaza program on appellant's laptop utilized the default setting, which automatically placed downloaded files into a shared location. The recovered artifacts from the Shareaza program on the laptop included search terms indicative of child pornography, including "gay pedo," "gay-kdv," "gay boy," "gay young," and "pedo boy." (Apr. 4, 2013 Tr., 115.) For testing purposes, Officer Priest entered the "gay pedo" and "gay-kdv" search terms in the Shareaza program; he retrieved files with titles indicative of child pornography in approximately 90 percent of the testing. According to Officer Priest's forensic reports, a total of 41 videos containing child pornography were discovered on the laptop and external hard drive.

{¶ 37} Officer Priest identified the files that ultimately formed the basis of the indictment in case No. 12CR-2800 as "bros.avi" (Counts 1 and 5), "deep.mpg" (Counts 2 and 6), "friends4.mpg" (Counts 3 and 7), and "friends6.mpg" (Counts 4 and 8). All four files were recovered from a deleted status on the external hard drive. Officer Priest determined that the "bros.avi" file had been viewed for a period of seven to ten seconds prior to being deleted; however, he could not determine whether the other three files had been viewed prior to being deleted.

{¶ 38} Officer Priest identified the files that ultimately formed the basis of the indictment in case No. 12CR-1564 as "p-101 boy orgy pthc pedo kdv" ("p-101 boy orgy") (Counts 1 and 5), "pedo gay three preteen boys on couch" ("three preteen boys") (Counts 2 and 6), "5 yo sucks * * *" ("5 yo sucks") (Counts 3 and 7), and "$rpcoudh.avi" (Counts 4 and 8).[5] The "p-101 boy orgy" file was the file downloaded by Officer Priest from appellant's IP address on June 22, 2010. According to Officer Priest, "[a] complete copy [of the file] had to exist in a shared location at that IP address at the time of the [June 22, 2010] investigation." (Apr. 4, 2013 Tr. 76.) The "three preteen boys" and "5 yo sucks" files were recovered from the shadow volume of the Windows operating system on

[5] The full titles of three of the files are offensive. For this reason, we have used abbreviated versions of those titles.

appellant's laptop. Officer Priest described the shadow volume as "a process in which Windows maintains a copy of files to make the recovery of accidentally deleted or lost files easy. * * * The shadow is an automated process. It takes it at undisclosed intervals when there's been changes to the system. In order for something to be in the shadow, it had to exist on the machine at that specific time in a user-obtainable area." (Apr. 5, 2013 Tr., 47-48.) He further averred that files in "[t]he shadow copy, although not immediately visible, [are] still in an active directory. They are not deleted; they are not overwritten; they are fully accessible through restore, backup, or other utilities." (Apr. 5, 2013 Tr., 112.) The "$rpcoudh.avi" file was recovered from the shadow volume in the laptop's recycle bin. According to Officer Priest, deleted files reside temporarily in the recycle bin; the recycle bin is maintained by the Windows operating system to allow users to recover accidentally deleted files.

{¶ 39} Although Officer Priest acknowledged that his forensic analysis did not establish the precise method by which the files were downloaded to the laptop, he was able to determine that appellant downloaded the files individually and not as part of a group download. He further averred that, although he could not determine exactly how the files found on the external hard drive had been transferred to that location, he could determine that it was through "user-attributed action." (Apr. 5, 2013 Tr., 73.) He also acknowledged that the "p-101 boy orgy" file did not exist in any form on either the laptop or the external hard drive at the time he conducted his forensic examination.

{¶ 40} Officer Priest conceded that terms utilized in a Shareaza program search could retrieve files with titles not necessarily indicative of file contents and that file titles may include terms indicative of child pornography that actually contain only adult pornography. However, he also testified that files with titles indicative of child pornography more often than not contain child pornography rather than adult pornography. He conceded that he could not definitively determine when searches were run or if any of the files at issue were directly related to the search terms found in the Shareaza program. In addition, he acknowledged that the downloading of a file to the shared location, the existence of a file in the shadow volume or recycle bin or the transfer of a file to an external hard drive, does not necessarily mean that the user viewed the file.

He also conceded that the "preview button" had not been utilized with regard to any of the files at issue.

{¶ 41} Although Officer Priest acknowledged the possibility that a user could inadvertently download child pornography while searching for adult pornography, he did not think that had happened in the present case, as his investigation revealed a pattern of child pornography downloads from appellant's IP address over a two-year period.

{¶ 42} The state also presented the testimony of Detective Junk and Detective Penwell, both of whom interviewed appellant during the September 7, 2010 search of appellant's residence. The audiotape of that interview was played at trial. During the interview, appellant averred that he was a widower and lived alone with his school age daughter. He acknowledged that he owned both a laptop and an external hard drive and had internet access through AT&T. When apprised that the officers were investigating allegations of child pornography on his computer, appellant acknowledged that he sometimes viewed gay adult pornography, but that child pornography was "not my thing." (Apr. 5, 2013 Tr., 156; State's exhibit No. 5.) He also admitted that he had downloaded the Shareaza program onto his laptop and accessed it by utilizing search terms such as "young" because he was drawn to "younger men." (Apr. 5, 2013 Tr., 167, 190; State's exhibit No. 5.) As a result, he sometimes came across images he clearly identified as involving teenagers; however, he immediately deleted those images.

{¶ 43} When asked if he had any reason to believe that those types of images would be found on his laptop or external hard drive, appellant initially replied, "I certainly hope there's nothing on that machine." (Apr. 5, 2013 Tr., 172; State's exhibit No. 5.) Later in the interview he stated, "I know there's probably something on that machine" because "you run into stuff." (Apr. 5, 2013 Tr., 173-74.) He further stated that he worked as a forensics "IT person" and realized that "every time you do anything, there's a trail" and that you can "never wipe anything completely clean." (Apr. 5, 2013 Tr., 177-78.) Regarding the use of search terms in the Shareaza program, appellant averred that, although he did not know what the abbreviation "pthc" meant, he acknowledged that "kdv" often brought up videos containing child pornography. (Apr. 5, 2013 Tr., 183-84.) Although he conceded that files in the shared location on his laptop could be accessed by others, he stated he did not intentionally share files with others. When informed that law

enforcement connected with his computer and downloaded child pornography through the Shareaza program, appellant averred, "I never thought of that. * * * Shame on me." (Apr. 5, 2013 Tr., 188.)

{¶ 44} C. Matthew Curtin of Interhack, a computer forensics consulting firm, testified as an expert witness on behalf of appellant. Mr. Curtin averred that he analyzed several items related to the case, including Officer Priest's computer forensics reports, additional documentation provided by Officer Priest, and the report of an image of the external hard drive that formed the basis of the 2012 indictment. Mr. Curtin prepared his own computer forensic reports based upon his analysis of the foregoing information.

{¶ 45} Mr. Curtin testified that the Shareaza program prohibits a user from viewing the content of a file prior to downloading it. A user may only view the content of a file after it has been downloaded into the shared location, and viewing a file requires some type of affirmative action by the user. He acknowledged, however, that a user necessarily observes the title of a file before initiating a download of the file. He further averred that when using search terms in a peer-to-peer filing sharing system, only the names of files are searched; the content of the files are not searched. He acknowledged that once the Shareaza program downloads a file into the shared location, that file is available for download by others. He further testified that a user need not view a file before downloading, transferring, backing it up or deleting it.

{¶ 46} As to the specifics of the instant case, Mr. Curtin testified that, because each of the four files that became the subject of the 2012 indictment had been deleted from the external hard drive, appellant would have had to utilize special software to recover them from their deleted status and gain access to them. As to the files pertinent to the 2013 indictment, Mr. Curtin averred that the fact that the files existed on appellant's laptop in the shared location, the shadow volume or the recycle bin did not necessarily mean that appellant had accessed or viewed those files. He acknowledged, however, that for a file to be located in the shadow volume or the recycle bin of a computer necessarily meant that the file existed on the computer at one time in the same condition it later existed in the shadow volume or the recycle bin. He also acknowledged that there was no definitive way to determine whether appellant actually viewed the files he downloaded prior to deleting them.

{¶ 47} Mr. Curtin ultimately opined that the forensic computer data was consistent with appellant's explanation that he inadvertently downloaded all the files containing child pornography onto his laptop and immediately deleted them upon discovering the nature of the file contents. He acknowledged on cross-examination, however, that the forensic computer data was also consistent with purposeful downloads of files containing child pornography followed by deletion of those files.

{¶ 48} In its judgment entry in case No. 12CR-2800, the trial court averred that it found appellant guilty of Counts 6, 7, and 8, all felonies of the fourth degree pursuant to R.C. 2907.322(A)(5), and specifically that appellant "knowingly 'possessed or controlled' material with knowledge of the character of the material or performance as child pornography." As noted, Counts 6, 7, and 8 corresponded to the "deep.mpg," "friends4.mpg," and "friends6.mpg" files, respectively. In its judgment entry in case No. 12CR-1564, the trial court averred that it found appellant guilty of Count 1, a felony of the second degree pursuant to R.C. 2907.322(A)(1), and specifically that appellant "knowingly 'publish[ed]' material with knowledge of the character of the matter as child pornography," and guilty of Counts 5, 6, and 7, felonies of the fourth degree pursuant to R.C. 2907.322(A)(5), and specifically that appellant "knowingly 'possessed or controlled' material with knowledge of its character as child pornography." As noted, Counts 1 and 5 corresponded to the "p-101 boy orgy" file; Counts 6 and 7 corresponded to the "three preteen boys" and "5 yo sucks" files, respectively.

{¶ 49} As pertinent here, R.C. 2907.322(A) provides:

> No person, with knowledge of the character of the material or performance involved, shall do any of the following:
>
> (1) * * * [P]ublish any material that shows a minor participating or engaging in sexual activity, masturbation, or bestiality;
>
> * * *
>
> (5) Knowingly * * * possess, or control any material that shows a minor participating or engaging in sexual activity, masturbation, or bestiality.

{¶ 50} There is no dispute that the video files found on appellant's laptop and external hard drive depicted minors participating or engaging in sexual activity, masturbation or bestiality. Appellant contends the evidence presented by the state is insufficient to prove beyond a reasonable doubt that he had "knowledge of the character of the material" underlying his convictions. Appellant further contends that his convictions are against the manifest weight of the evidence, as they are based upon the impermissible stacking of inferences leading to speculative findings unsupported by the testimonial and forensic evidence.

{¶ 51} "A person acts knowingly, regardless of his purpose, when he is aware that his conduct will probably cause a certain result or will probably be of a certain nature. A person has knowledge of circumstances when he is aware that such circumstances probably exist." R.C. 2901.22(B). "Whether a person acts knowingly can only be determined, absent a defendant's admission, from all the surrounding facts and circumstances, including the doing of the act itself." *State v. Conant,* 5th Dist. No. 13CA55, 2014-Ohio-1739, ¶ 27, citing *State v. Huff,* 145 Ohio App.3d 555, 563 (1st Dist.2001). Accordingly, " '[t]he test for whether a defendant acted knowingly is a subjective one, but it is decided on objective criteria.' " *Id.,* citing *State v. McDaniel,* 2d Dist. No. 16221 (May 1, 1998).

{¶ 52} Here, the state relied on circumstantial evidence to prove its case. " 'Circumstantial evidence and direct evidence inherently possess the same probative value.' " *Id.,* quoting *Jenks* at paragraph one of the syllabus. "Furthermore, '[s]ince circumstantial evidence and direct evidence are indistinguishable so far as the [fact finder's] fact-finding function is concerned, all that is required of the [fact finder] is that [it] weigh all of the evidence, direct and circumstantial, against the standard of proof beyond a reasonable doubt.' " *Id.,* quoting *Jenks* at 272.

{¶ 53} Construing the evidence in a light most favorable to the state, a rational trier of fact could conclude that appellant knew that the video files found on his computers contained child pornography. Appellant admitted that he downloaded the Shareaza program to view pornography and that the Shareaza program allowed him to enter search terms as a means of locating pornography files available for download. The forensic examination of appellant's computers revealed that he entered search terms including

"pedo" and "kdv." Officer Priest testified that these search terms are commonly used in attempts to locate child pornography. When interviewed during the search of his residence, appellant acknowledged that the search term "kdv" often brought up videos containing child pornography. Appellant's use of these search terms constitutes evidence of appellant's knowledge of the content of the files found on his computers and undermines his claim that his possession of the files was accidental.

{¶ 54} Contrary to appellant's assertion, whether the specific search terms utilized by appellant led to the downloading of the particular files at issue is irrelevant. The fact remains that appellant input search terms indicative of child pornography, and child pornography was discovered on appellant's computers. Indeed, with respect to case No. 12CR-1564, the titles of three of the files at issue contain the search terms entered by appellant, proving that he knew the character of their contents.

{¶ 55} Appellant's statements made during his interview with police also suggest that he knew his computer files contained child pornography. As noted, when asked that question, he first stated, he "hope[d]" not. He later admitted "there's probably something" on the computers. He also stated that he realized computer activity leaves "a trail" and that computer activity could never be completely erased. Appellant further contends that the state's failure to establish that he ever viewed the video files amounts to a failure to establish that he was aware that they contained child pornography. Appellant cites no authority in support of this argument, and we note that neither R.C. 2907.322(A)(1) nor (5) require that the offender actually view the material.

{¶ 56} Moreover, contrary to appellant's assertion, the fact that the files were recovered from the deleted status, the shadow volume or in the recycle bin of appellant's computers does not mean that the state failed to prove that he was unaware of the contents of those files. Officer Priest testified that individuals often download child pornography, delete the files out of guilt or fear of being discovered, and re-download them at a later date. In addition, both Officer Priest and Mr. Curtin averred that files recovered from the deleted status, the shadow volume or the recycle bin had to have at one point existed in a user obtainable area.

{¶ 57} Appellant's assertion that he accidentally downloaded the files without knowing that they contained child pornography is undermined by Officer Priest's

testimony. Although Officer Priest acknowledged that a user could inadvertently download child pornography while searching for adult pornography, he believed that such was not the case here, as his investigation revealed a pattern of child pornography downloads from appellant's IP address over a two-year period. He further averred that his forensic analysis of appellant's computers revealed 41 videos containing child pornography. It is difficult to believe that appellant could accidentally download that many videos. In addition, Mr. Curtin conceded that his forensic computer examination was consistent with purposeful downloads of files containing child pornography followed by deletion of those files.

{¶ 58} With regard to his conviction on Count 1 in case No. 12CR-1564 (the "publishing" count), appellant maintains that someone else may have used his IP address to make the "p-101 boy orgy" file available for download through Shareaza. However, nothing in the record before us indicates that anyone other than appellant downloaded this file. No one else was shown to have had access to appellant's IP address, especially at the time this file was downloaded.

{¶ 59} As to appellant's contention that his convictions are against the manifest weight of the evidence because they are based upon the impermissible stacking of inferences, we note that where "the state relies on circumstantial evidence to prove an essential element of an offense, it is not necessary for 'such evidence to be irreconcilable with any reasonable theory of innocence in order to support a conviction.' " *Conant* at ¶ 31, quoting *Jenks* at paragraph one of the syllabus. "While inferences cannot be based on inferences, a number of conclusions can result from the same set of facts." *Id.*, citing *State v. Lott*, 51 Ohio St.3d 160, 168 (1990). "Moreover, a series of facts and circumstances can be employed by a [fact finder] as the basis for its ultimate conclusions in a case." *Id.*, citing *Lott* at 168.

{¶ 60} Ultimately, "the reviewing court must determine whether the appellant or the appellee provided the more believable evidence, but must not completely substitute its judgment for that of the original trier of fact 'unless it is patently apparent that the factfinder lost its way.' " *State v. Pallai*, 7th Dist. No. 07 MA 198, 2008-Ohio-6635, ¶ 31, quoting *State v. Woullard*, 158 Ohio App.3d 31, 2004-Ohio-3395, ¶ 81 (2d Dist.2004). In other words, "[w]hen there exist two fairly reasonable views of the evidence or two

conflicting versions of events, neither of which is unbelievable, it is not our province to choose which one we believe." *State v. Dyke*, 7th Dist. No. 99 CA 149, 2002-Ohio-1152, citing *State v. Gore*, 131 Ohio App.3d 197, 201 (7th Dist.1999). The weight to be given the evidence and the credibility of the witnesses are issues for the trier of fact. *DeHass* at paragraph one of the syllabus.

{¶ 61} The court as the trier of fact was free to accept or reject any and all of the evidence offered by the parties and assess the witnesses' credibility. " '[W]hile the [fact finder] may take note of the inconsistencies and resolve or discount them accordingly, * * * such inconsistencies do not render [a] defendant's conviction against the manifest weight or sufficiency of the evidence.' " *State v. Craig*, 10th Dist. No. 99AP-739 (Mar. 23, 2000), quoting *State v. Nivens*, 10th Dist. No. 95APA09-1236 (May 28, 1996). Indeed, the fact finder may believe all, part or none of a witness's testimony. *State v. Raver*, 10th Dist. No. 02AP-604, 2003-Ohio-958, ¶ 21, citing *State v. Antill*, 176 Ohio St. 61, 67 (1964). Although the evidence in the present case may have been circumstantial, we reiterate that circumstantial evidence has the same probative value as direct evidence. *Jenks*.

{¶ 62} Upon careful review of the entire record in this matter, we find appellant's convictions are based upon sufficient evidence and are not against the manifest weight of the evidence. Accordingly, appellant's second and third assignments of error are overruled.

{¶ 63} Having overruled all three of appellant's assignments of error, we affirm the judgments of the Franklin County Court of Common Pleas.

Judgments affirmed.

SADLER, P.J., and DORRIAN, J., concur.

———————————————