[Cite as *State v. Lemasters*, 2013-Ohio-2969.]

IN THE COURT OF APPEALS

TWELFTH APPELLATE DISTRICT OF OHIO

MADISON COUNTY

STATE OF OHIO,	:	
Plaintiff-Appellee,	:	CASE NO. CA2012-12-028
	:	O P I N I O N
- vs -		7/8/2013
	:	
DONALD F. LEMASTERS,	:	
Defendant-Appellant.	:	

CRIMINAL APPEAL FROM MADISON COUNTY COURT OF COMMON PLEAS
Case No. CRI20110122

Stephen J. Pronai, Madison County Prosecuting Attorney, Kirsten J. Gross, 59 North Main Street, London, Ohio 43140, for plaintiff-appellee

Tyack, Blackmore, Liston & Nigh Co., L.P.A., Jonathan T. Tyack, 536 South High Street, Columbus, Ohio 43215, for defendant-appellant

PIPER, J.

{¶ 1} Defendant-appellant, Donald Lemasters, appeals a decision of the Madison County Court of Common Pleas, denying his motion to suppress.

{¶ 2} Detective Marcus Penwell of the multi-jurisdictional Internet Crimes Against Children Task Force investigates social networking sites where adults solicit children for sexual activity. He also monitors file-sharing programs for distribution of child pornography

files. During an investigation, Detective Penwell connected with an internet protocol (IP) address belonging to a computer that contained child pornography files. Through the use of "Shareaza," a file sharing program, Detective Penwell was able to access and download child pornography from the computer, which had an IP address belonging to a Time Warner Cable internet customer.

{¶ 3} Detective Penwell obtained an investigative subpoena issued by a court and contacted Time Warner Cable in order to determine the user of the IP address. Detective Penwell discovered that the IP address belonged to Lemasters, and contacted the Madison County Sheriff's Office to involve them in the investigation. Police then obtained and executed a search warrant for Lemasters' home. Police seized over 170,000 images of child pornography from Lemasters' home, including images of infant and toddler rape. The images were found on Lemasters' computer and also on various DVDs that Lemasters made from the child pornography he downloaded from his computer.

{¶ 4} Lemasters was charged with 15 counts of pandering sexually-oriented matter involving a minor, nine counts of possession of sexually-oriented material involving a minor, and one count of possession of criminal tools. Lemasters filed a motion to suppress evidence of the images seized from his house. At the hearing, Detective Penwell appeared and testified. The trial court denied Lemasters' motion to suppress, and Lemasters pled no contest to the charges against him. The trial court found Lemasters guilty and sentenced him to an aggregate sentence of eight years. Lemasters now challenges the trial court's decision denying his motion to suppress, raising the following assignment of error.

{¶ 5} THE TRIAL COURT ERRED IN OVERRULING APPELLANT'S MOTION TO SUPPRESS ALL EVIDENCE ARISING OUT OF OR RESULTING FROM THE INVESTIGATIVE SUBPOENA SENT TO TIME WARNER CABLE BY DETECTIVE PENWELL FOR THE PURPOSES OF DETERMINING APPELLANT'S IDENTITY.

{¶ 6} Lemasters argues in his assignment of error that the trial court erred in denying his motion to suppress.

{¶ 7} Appellate review of a ruling on a motion to suppress presents a mixed question of law and fact. *State v. Cochran*, 12th Dist. No. CA2006-10-023, 2007-Ohio-3353. Acting as the trier of fact, the trial court is in the best position to resolve factual questions and evaluate witness credibility. *Id.* Therefore, when reviewing a trial court's decision regarding a motion to suppress, a reviewing court is bound to accept the trial court's findings of fact if they are supported by competent, credible evidence. *State v. Oatis*, 12th Dist. No. CA2005-03-074, 2005-Ohio-6038. "An appellate court, however, independently reviews the trial court's legal conclusions based on those facts and determines, without deference to the trial court's decision, whether as a matter of law, the facts satisfy the appropriate legal standard." *Cochran* at ¶ 12.

{¶ 8} The Fourth Amendment to the United States Constitution protects people from illegal searches and seizures. In order to employ Fourth Amendment protections, a defendant must have a "constitutionally protected reasonable expectation of privacy." *Katz v. United States*, 389 U.S. 347, 360, 88 S.Ct. 507 (1967). The United States Supreme Court has directed reviewing courts to consider a two-part test in order to determine whether the Fourth Amendment is implicated. "First, has the individual manifested a subjective expectation of privacy in the object of the challenged search? Second, is society willing to recognize that expectation as reasonable?" *California v. Ciraolo*, 476 U.S. 207, 211, 106 S.Ct. 1809 (1986), citing *Katz* at 360.

{¶ 9} As stated by the court in *Katz*, "what a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." 389 U.S. at 351. Instead, "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith v. Maryland*, 442 U.S. 735, 743, 99 S.Ct. 2577

(1979). As this court has specifically held, 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. *State v. Hamrick*, 12th Dist. No. CA2011-01-002, 2011-Ohio-5357, ¶ 19, jurisdiction declined 131 Ohio St.3d 1513, 2011-Ohio-5357.

{¶ 10} In *Hamrick,* the appellant was using a file-sharing program to share child pornography over the internet. In the exact same manner as what occurred in the case at bar, Detective Penwell became aware of an IP address that was linked to child pornography. Detective Penwell moved for an investigative subpoena, which he delivered to Time Warner Cable. Time Warner then identified Hamrick as the subscriber in question. A search warrant was later obtained and executed, and police seized 339 images and 28 videos of child pornography. Hamrick was indicted on several counts of illegal use of a minor in nudity-oriented material and pandering obscenity involving a minor. Hamrick moved to suppress the images seized from his home, arguing that his Fourth Amendment rights were violated where the police did not gain a search warrant before obtaining information from Time Warner. The trial court overruled Hamrick's motion to suppress, and Hamrick appealed to this court.

{¶ 11} In our decision, we found that Hamrick's "constitutional rights were not violated when law enforcement obtained his subscriber information from Time Warner because he ha[d] not demonstrated an objectively reasonable expectation of privacy in this information." 2011-Ohio-5357 at ¶ 18. In so holding, we reasoned that "when 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. Appellant cannot now claim to have a Fourth Amendment privacy interest in this information." *Id*. at ¶ 19. Despite Lemasters' suggestion that we stray from our decision in *Hamrick*, we decline to do so and find the reasoning set forth in *Hamrick* also applicable to the case at bar.

{¶ 12} Lemasters claims that our reasoning in *Hamrick* should be adjusted in light of recent case law holding that use of a GPS to track a suspect's movements constitutes a search and implicates the Fourth Amendment. *United States v. Jones*, __U.S.__, 132 S.Ct. 945 (2012). In *Jones*, the United States Supreme Court held very specifically that "the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search.'" *Id*. at 949. In so holding, the court reasoned that by placing a GPS on the suspect's car, "the Government physically occupied private property for the purpose of obtaining information." *Id*. The court went on to state that "we have no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted." *Id*.

{¶ 13} Despite Lemasters' arguments to the contrary, the *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.

{¶ 14} 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 files 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 Detective Penwell 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.

{¶ 15} Since the release of the Supreme Court's decision in *Jones*, several courts have been asked to decide whether accessing file-sharing programs and IP address information constitutes a search that implicates the Fourth Amendment. In finding that no expectation of privacy exists in such cases, the courts have not analyzed the issue as being controlled by *Jones*.

{¶ 16} For example, the United States District Court for the Eastern District of Missouri declined to extend *Jones* in the same manner that Lemasters asserts. *United States v. Nolan*, E.D.Mo. No. 1:11CR 82 CEJ, 2012 WL 1192183 (Mar. 6, 2012). In *Nolan*, the court stated that the appellant's reliance on *Jones* was "misdirected." *Id*. at *10. In so stating, the court reasoned that while *Jones* states that a search warrant is required before a police officer can "legally attach a GPS device to a suspect's vehicle," accessing one's files and internet information through peer-to-peer sharing is not a search because the files are not "private." *Id*. The court concluded, "when Mr. Nolan placed the images in his shared folder, he was offering them to the world. * * * Mr. Nolan's privacy was not invaded by [the police] because Mr. Nolan offered them to [the police] and to anyone else on the world wide network." *Id*.

{¶ 17} Similarly, the United States District Court for the Eastern District of New York has also found an appellant's attempt to apply *Jones* to facts similar to the case at bar "misplaced." *United States v. Brooks*, E.D.N.Y. No. 12-CR-166 (RRM), 2012 WL 6562947, *5 (Dec.17, 2012). In *Brooks*, the appellant had multiple images of child pornography on his computer, and used a file-sharing program to access and share the images. The

investigating officer downloaded the files from Brooks' computer, and then procured Brooks' identity through the use of his IP address.

{¶ 18} The *Brooks* court disregarded the appellant's reliance on *Jones*, and stated,

> In contrast to *Jones,* there is no evidence here that the undercover agent made any physical intrusion on a constitutionally protected area. The agent did not install any device or software on Brooks' computer to enable monitoring or tracking, did not physically enter Brooks' home, and did not physically access his computer. * * * As such, the undercover agent did not physically intrude on any of Brooks' constitutionally protected areas. Therefore, because this situation involves "merely the transmission of electronic signals without trespass," the *Katz* reasonable-expectation-of-privacy governs this analysis, which, as discussed above, does not implicate Brooks' Fourth Amendment rights.

Id.

{¶ 19} Additionally, the Sixth Circuit recently considered whether an appellant had a reasonable expectation of privacy in files he shared using a file-sharing program. *United States v. Conner*, 6th Cir. No. 12-3210, 2013 WL 1490109 (Apr. 11, 2013). In *Conner*, the appellant was convicted of multiple counts related to his possession of child pornography. Conner used the file sharing service "LimeWire" to share files containing child pornography with other interested users. Once again, Detective Penwell used the file-sharing program to access child pornography files on Conner's computer, after having moved for an investigatory subpoena from the court and receiving Conner's IP address information from his internet service provider.

{¶ 20} Conner argued to the Sixth Circuit that he had a reasonable expectation of privacy in his files, and that Detective Penwell should have secured a warrant before using the file sharing program to access child pornography files on his computer. The Sixth Circuit, in affirming the district court's denial of Conner's motion to suppress, stated that "public exposure of information in this manner defeats an objectively reasonable expectation of privacy under the Fourth Amendment." 2013 WL 1490109 at *4. However, the court never

discussed Detective Penwell's use of the file-sharing program or obtaining IP address information as the trespassory invasion or "physical intrusion" contemplated by *Jones*.

{¶ 21} Similarly, the United States District Court for the Western District of Pennsylvania recognized that "internet subscribers who use [internet service providers] to connect to the internet from their homes do not have a reasonable expectation of privacy in their subscriber information or IP addresses because they have conveyed this information to third parties in order to connect to the internet." *United States v. Stanley*, W.D. Penn. No. 11-272, 2012 WL 5512987 (Nov.14, 2012). Despite *Jones*, the court did not analyze the police investigation of the appellant's IP address as a trespassory search invoking the appellant's Fourth Amendment rights.

{¶ 22} Well-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. Lemaster's Fourth Amendment rights were not implicated by Detective Penwell's use of the file-sharing system, or in his obtaining Lemasters' information from Time Warner based upon Lemaster's IP address.

{¶ 23} Lemasters also argues that Detective Penwell violated the federal Electronic Communications Privacy Act, 18 U.S.C. 2701 et seq. (ECPA), by obtaining information from Time Warner. According to the ECPA,

> 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 issued using the procedures described in the Federal Rules of Criminal Procedure (or, 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;

According to 18 U.S.C. 2703(d),

> A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and 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. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

{¶ 24} The facts are clear that Detective Penwell did not obtain a warrant before obtaining Lemasters' information from Time Warner. Instead, Detective Penwell was granted an investigative subpoena from a judge, which authorized him to require Time Warner to share the information regarding Lemasters' IP address. However, Lemasters argues that the investigative subpoena is 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.

{¶ 25} According to R.C. 2935.23,

> After a felony has been committed, and before any arrest has been made, the prosecuting attorney of the county, or any judge or magistrate, may cause subpoenas to issue, returnable before any court or magistrate, for any person to give information concerning such felony. The subpoenas shall require the witness to appear forthwith. Before such witness is required to give any information, he must be informed of the purpose of the inquiry, and that he is required to tell the truth concerning the same. He shall then be sworn and be examined under oath by the prosecuting attorney, or the court or magistrate, subject to the constitutional rights of the witness. Such examination shall be taken in writing in any form, and shall be filed with the court or magistrate taking the testimony.

{¶ 26} Detective Penwell testified that he obtained the investigative subpoena by

submitting relevant facts to the judge, including that he was investigating suspected child pornography and that he had downloaded child pornography images from the IP address in question. However, no representatives from Time Warner appeared as a witness, and the judge issued the investigative subpoena without taking any testimony regarding the issue. While it may be true that the investigative subpoena was issued without witness testimony, the remedy Lemasters seeks is unavailable to him.

{¶ 27} As this court also stated in *Hamrick*, the ECPA does not provide suppression of evidence as a remedy should information be obtained in a manner not consistent with state law. We recognized in *Hamrick* that while the ECPA specifically allows for civil damages and criminal punishment for violations of the ECPA, the statute states nothing about the suppression of information in a court proceeding. Instead, congress "clearly intended for suppression not to be an option for a defendant whose electronic communications have been intercepted in violation of the ECPA." 2011-Ohio-5357 at ¶ 17; *see also United States v. Ferguson*, 508 F.Supp.2d 7, 10 (D.C.2007) (finding that the ECPA "does not provide for a suppression remedy").

{¶ 28} The ECPA specifically states, "the remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter." 18 U.S.C. 2708. While 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.

{¶ 29} Having found that Lemasters' did not have a reasonable expectation of privacy, that Detective Penwell'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. As such,

Lemasters' single assignment of error is overruled.

{¶ 30} Judgment affirmed.

RINGLAND, P.J., and M. POWELL, J., concur.