

ORIGINAL

IN THE SUPREME COURT OF OHIO  
2013

State of Ohio,

Plaintiff-Appellee,

-vs-

Donald F. Lemasters,

Defendant-Appellant.

Case No. 13 - 1265

On Appeal from the Madison County Court  
of Appeals, Twelfth Appellate District

Court of Appeals Case No. CA 2012-12-028

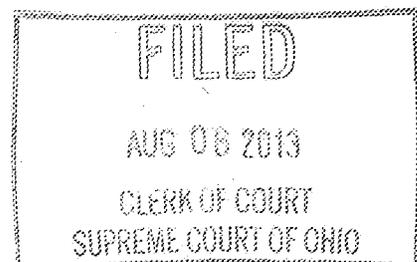
---

MEMORANDUM IN SUPPORT OF JURISDICTION  
OF APPELLANT, DONALD F. LEMASTERS

---

JONATHAN T. TYACK (0066329)  
Tyack, Blackmore, Liston & Nigh Co., LPA  
536 South High Street  
Columbus, OH 43215  
Telephone: 614-221-1341  
Email: jttyack@tblattorneys.com  
COUNSEL FOR DEFENDANT-  
APPELLANT

STEPHEN J. PRONAI (0012063)  
Madison County Prosecuting Attorney  
KIRSTEN J. GROSS (0069997)  
Madison County Assistant Prosecuting  
Attorney  
59 N. Main Street  
London, Ohio 43140  
COUNSEL FOR PLAINTIFF-APPELLEE



**STATEMENT OF WHY THIS CASE INVOLVES A SUBSTANTIAL  
CONSTITUTIONAL QUESTION AND QUESTIONS OF PUBLIC OR GREAT  
GENERAL INTEREST.**

Technology is changing our world in many ways on a daily basis. In fact, technology continues to change rapidly on a daily basis. This case gives this Court an opportunity to apply numerous Constitutional and statutory principles to a technological fact pattern that did not and could not have existed at the time that said Constitutional and statutory rules were first put in place by Congress and the State Legislature.

Appellant's first proposition of law involves a substantial Constitutional question. Specifically, Appellant's first proposition of law raises an issue that will allow this Court to define the parameters of a person's privacy expectations here in the State of Ohio. In today's day and age, private information must be protected more than ever before. Congress has enacted privacy legislation protecting personal information through the Electronic Communications and Privacy Act, 18 U.S.C. § 2701 et. seq. This federal statute is a manifestation of the societal expectation that personal information will be kept private even when provided to third parties.

For centuries, expectations of privacy have been recognized for information provided to attorneys, information provided to doctors, and information provided to priests or other religious leaders. In the twenty first century, however, society recognizes the need for privacy in a number of different arenas. Individuals have a reasonable expectation of privacy in their personal information whether that information is shared with internet service providers (18 U.S.C. § 2701 et. seq.), banks (12 U.S.C. § 3401 et. seq.; 15 U.S.C. § 6801 et. seq.), educational institutions (20 U.S.C. § 1232g), or any other number of commercial third parties.

Since the democratically elected Congress has defined the interest in privacy on behalf of our entire society, it is time for the courts to recognize a reasonable expectation of privacy in

certain information on a Constitutional level such that the improper and warrantless gathering of this information violates the Constitutional protections set forth in the Fourth Amendment to the United States Constitution and Article I, Section 14 of the Ohio Constitution.

Furthermore, this case provides this Court with an opportunity to define privacy interests under both the Fourth Amendment to the United States Constitution, and the Ohio Constitution, in light of the groundbreaking decision by the United States Supreme Court in United States v. Jones, \_\_\_\_\_ U.S. \_\_\_\_\_, 132 S. Ct. 945 (2012). In Jones, a majority of the justices of the United States Supreme Court recognized that a Defendant's reasonable expectation of privacy is no longer synonymous with secrecy. The justices of the United States Supreme Court recognize that individuals can have a reasonable expectation of privacy, even when that information is shared with third parties, or subject to the public domain. This case provides this Supreme Court with an opportunity to interpret the analysis in Jones, and apply it here in the State of Ohio. Therefore, this case involves a substantial constitutional question that is also a question of great general interest in public importance.

#### **STATEMENT OF THE CASE AND FACTS**

The investigation of Appellant began when Detective Marcus Penwell downloaded suspected child pornography from an internet protocol (IP) address that he recognized as in IP address provided by the internet service provider, Time Warner Cable. (Mot. Hrg. Tr. 3/27/12 at pg. 10-12). Detective Penwell then issued an investigative subpoena to Time Warner Cable, purportedly in compliance with Revised Code § 2935.23, in order to obtain the subscriber information so that the actual person using said IP address could be identified. (Mot. Hrg. Tr. 3/27/12 at pg. 12-16, 18, 26). Detective Penwell testified at the time of the motion hearing that he needed to use the investigative subpoena process to obtain the subscriber information from Time

Warner Cable because that information is not otherwise available from any other source. (Mot. Hrg. Tr. 3/27/12 at pg. 26-27). Detective Penwell further acknowledged that he did not seek a search warrant in this case, (Mot. Hrg. Tr. 3/27/12 at pg. 20), nor did he seek the assistance of the Prosecutor's Office. (Mot. Hrg. Tr. 3/27/12 at pg. 19). The investigative subpoena in question was admitted into evidence at the time of the hearing as exhibit one. (Id. at pg. 14).

Detective Penwell further testified that he could not recall whether the Judge asked any specific questions relating to the ongoing investigation. (Id. at pg. 21). Likewise, he was not required to submit any affidavit under oath nor was he required to even submit any kind of written summary to the Judge prior to obtaining the Judge's signature on the investigative subpoena. (Id.) Put simply, Detective Penwell acknowledged that the investigative subpoena process does not carry any of the inherent constitutional safeguards required by a search warrant.

Time Warner Cable responded to the investigative subpoena indicating that the subscriber connected with the internet protocol address in question was Appellant, Donald Lemasters, at his address in Madison County, Ohio. Detective Penwell then contacted the Madison County Sheriff's Office and steps were undertaken to obtain a search warrant for the search of Appellant's home and computers. (Mot. Hrg. Tr. 3/27/12 pg. 15-16). As a result of the search warrant executed by the Madison County Sheriff's Department, on Appellant's home, numerous files of child pornography were recovered. (Id. at pg. 16). It is these child pornography files that form the basis of the indictment against Appellant. (R. 1, 18). No evidence was presented by the State of Ohio to indicate that anyone from Time Warner Cable ever appeared to give testimony under oath, either to a Court or to a Prosecutor. (Mot. Hrg. Tr. 3/27/12 passim). Furthermore, no evidence was presented by the State of Ohio to indicate that any of the information presented by Time Warner was ever made a part of the court record or taken down by a court reporter. (Id.) Contrary

to the provisions of Revised Code § 2935.23, the information was simply sent to Detective Penwell from Time Warner Cable.

Put simply, all of the evidence seized from Appellant as a result of the search warrant of his home and computer arose from the single act of Detective Penwell obtaining Appellant's confidential subscriber information from Time Warner Cable without a search warrant, and otherwise without acting in compliance with Revised Code § 2935.23.

On October 11, 2011, Appellant, Donald Lemasters was indicted with fifteen counts of pandering sexually oriented matter involving a minor in violation of Revised Code § 2907.322(A)(1), nine counts of possession of sexually oriented material involving a minor, in violation of Revised Code § 2907.322(A)(5), and one count of possession of criminal tools, in violation of Revised Code § 2923.24(A). (R. 1). Appellant was arraigned on August 23, 2011, and entered a general plea of not guilty to all charges. (R. 10). After concluding discovery, Appellant filed a motion to suppress alleging that the State of Ohio violated Defendant's rights under the Fourth, Fifth, and Fourteenth Amendment to the United States Constitution, and Appellant's comparable rights under the Ohio Constitution. (R. 17). Appellant then filed a supplemental memorandum in support of his motion to suppress on March 22, 2012. (R. 45). The State of Ohio then subsequently responded to the supplemental motion filed by Appellant. (R. 46). On March 27, 2012, an evidentiary hearing was held relating to Appellant's motion to suppress and the issues raised therein. (Mot. Hrg. Tr. 3/27/12; R. 47). Subsequent to the hearing, on April 3, 2012, the trial court overruled Defendant's motion to suppress in its entirety. (R. 47).

On August 24, 2012, Appellant entered no contest pleas to counts one, two, three, four, five, six, seven, eight, nine, ten, eleven, twelve, thirteen, fifteen, sixteen, seventeen, eighteen, nineteen, twenty, twenty-one, twenty-two, twenty-three, twenty-four, and twenty-five, of the

indictment. Count fourteen of the indictment had previously been dismissed. (Plea Hrg. Tr. 8/24/12; R. 65). The plea was accepted by the court, thus maintaining all rights of Defendant to appeal the issues surrounding his motion to suppress. (Plea Hrg. Tr. at pg. 18; R. 65).

### **ARGUMENT IN SUPPORT OF PROPOSITION OF LAW**

**Proposition of Law No. I: Individuals have a legitimate and reasonable expectation of privacy in their internet subscriber information such that the warrantless seizure of such private information violated the Fourth Amendment to the United States Constitution, and Article I, Section 14 of the Ohio Constitution.**

Under the Fourth Amendment to the United States Constitution, and Section 14, Article 1 of the Ohio Constitution, the Constitutional protections against unreasonable search and seizure begin with the idea that for any search, subject to some well established exceptions, a search warrant is required. The warrant requirement guarantees that searches will not be conducted without a police officer first giving sworn testimony, usually through an affidavit. State v. Wilmoth (1986), 22 Ohio St. 3d 251, 262. Furthermore, the warrant requirement protects the individual right of privacy by making sure that an independent Judge or Magistrate reviews said testimony for probable cause. State v. George (1989), 45 Ohio St. 3d 325, 334. These are important Constitutional protections that may not be circumvented at the discretion of law enforcement.

#### **A. Appellant has a legitimate privacy interest in his subscriber information.**

The United States Congress has determined that an individual has a reasonable expectation of privacy in the records concerning electronic communications, including an individual's IP address. Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2701 et. seq. (hereinafter referenced as "ECPA"). Congress enacted the ECPA "to update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications

technologies.” 132 CONG. REC. S. 144441 (1986). In drafting the ECPA, Congress intended to fairly balance “the interest of privacy and law enforcement.” S. REP. NO. 99-541 (1986). Specifically, 18 U.S.C. § 2703(c)(1) provides that a Governmental entity seeking information like an subscriber information from an Internet Service Provider must comply with specific legal process, by obtaining either a search warrant, a court order, or the subscriber’s consent. 18 U.S.C. § 2703(c)(1). Several other Courts have addressed the question of whether an individual has a reasonable and legitimate expectation of privacy in their personal information, when that personal information is maintained by an internet provider for the purposes of providing internet service. See, State v. Thornton (September 29, 2009), Franklin County App. No. 09 AP-108; 2009 WL 3090409 (and cases cited therein). Only a handful of cases have addressed this issue across the Country. Although these cases have not yet recognized the legitimate expectation of privacy in one’s personal information as protected by the ECPA, none of those cases are binding on this Court.

Because the ECPA makes confidential the information that was sought by law enforcement in this case, and because the ECPA was enacted by Democratically – elected Congress, who collectively speaks for the citizens of this country, then the ECPA creates a rule of law that recognizes a legitimate expectation of privacy that must be recognized by the Courts. Because this privacy interest was established Democratically through Congress, it is per se reasonable and legitimate.

Here, no consent was ever obtained from Appellant, and no proper search warrant was ever obtained for the purposes of obtaining the subscriber information for the IP address in question. Therefore, the question becomes one of determining whether the investigative subpoena purportedly issued under R.C. § 2935.23 of the Ohio Revised Code qualifies as a “Court order”

under the ECPA. Moreover, even if a properly issued investigative subpoena, issued in compliance with R.C. § 2935.23, qualifies as a "Court order" under the ECPA, the fact remains that the mandates of the R.C. § 2935.23 were not followed in this case.

**B. Revised Code § 2935.23 does not allow law enforcement to circumventive the warrant requirement, especially when R.C. § 2935.23 is not followed.**

Revised Code § 2935.23 states as follows:

"After a felony has been committed, and before any arrest has been made, the Prosecuting Attorney of the County, of 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 subpoena 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 of Magistrate taking the testimony. Witness fee shall be paid to such persons as in other cases."

Here, although the investigative subpoena was signed by a Judge (Mot. Hrg. Exhibit 1), this Court should find that it does not properly qualify as a "Court order," R.C. § 2935.23 allows Prosecutors to sign the subpoena as well. Although a Prosecutor did not sign the subpoena in this case, the fact remains that the procedure under R.C. § 2935.23 is simply an evidence gathering tool, not a Court order binding upon Time Warner Cable. There is no court order from any case involving Time Warner Cable, nor was Time Warner Cable ever subject to the Court's jurisdiction in this matter. Therefore, since the investigative subpoena issued to Time Warner Cable does not qualify as a "court order" under the ECPA, the use of this procedure violates Defendant's Constitutional Rights.

Moreover, the investigating detective in this matter did not fully comply with R.C. § 2935.23. It is well established here that although the subpoena was signed by the Judge in Franklin County, and forwarded to Time Warner Cable, no one from Time Warner ever appeared in person

before the Court or the Prosecuting Attorney. Likewise, no representative of Time Warner Cable was ever sworn and placed under oath, nor was any representative of Time Warner Cable ever examined by the Prosecuting Attorney, the Court, or the Magistrate. Furthermore, no examination was ever taken in writing in any form, and no written documentation or record was made with the Court or Magistrate taking the testimony. Consequently, since Detective Penwell did not comply with the mandates of R.C. § 2935.23 then the subpoena issued in this case, (Mot. Hrg. Tr. Exhibit 1), cannot and must not be considered a “court order” under the ECPA.

**C. Under the analysis set forth by the United State Supreme Court in United State v. Jones, Appellant has a reasonable expectation of privacy in his internet subscriber information.**

In United States v. Jones, \_\_\_ U.S. \_\_\_, 123 S. Ct. 945 (2012), the defendant came under suspicion for trafficking in narcotics, and was made a target of an investigation by a joint FBI and Metropolitan Police Department Task Force. In its investigation of the case, law enforcement placed a GPS tracking device on the undercarriage of a vehicle owned by defendant’s wife, while it was parked in a public parking lot. Over the next twenty-eight days, without an appropriate search warrant, the Government used the device to track the vehicle’s movements, and once had to actually replace the device’s battery when the vehicle was parked in a different public lot. The device placed on the vehicle established the vehicle’s location within 50 to 100 feet, and communicated the location by cellular phone to a government computer, relaying thousands of pages of data over the four week period.

Before trial, the defendant filed a motion to suppress, and the district court granted the motion suppressing the data that was obtained while the vehicle was sitting in defendant’s private garage at his residence. However, the trial court in that case ruled that “[a] person traveling in an

automobile on public thoroughfares has no reasonable expectation of privacy in its movements in one place to another.” Jones, supra, at 132 S. Ct. 948.

Ultimately, the United States Court of Appeals for the District of Columbia Circuit reversed the conviction because of the admission of the evidence obtained by the warrantless use of the GPS device, which, the Court of Appeals said, violated the Fourth Amendment. Jones, 132 S. Ct. at 949. (citing United States v. Maynard (2010), 615 F. 3d 544).

Although the majority opinion in Jones discusses and relies upon the fact that the Government trespassed upon defendant’s property, the majority opinion made the effect of the Jones decision very clear when it stated, “[W]e do not make trespass the exclusive test.” Jones, supra, 132 S. Ct. at 953. The court continued by indicating that other types of information would still be subject to an analysis under Katz v. United States (1967), 389 U.S. 347, and the “reasonable expectation of privacy” test established therein. Id.

The majority opinion acknowledges that relying wholeheartedly on a “trespass” theory to determine the existence of a search or a seizure creates “vexing problems”, but the court’s majority refused to address those problems, leaving the question to be answered on another day. However, when reading the majority opinion in the context of the accompanying concurrences by the other justices, it appears clear that the United States Supreme Court is recognizing in Jones, supra, the fact that individuals have a reasonable and legitimate expectation of privacy in information unique to their personal situation, even when that information has been shared with third parties or is subject to the public domain.

As a member of the majority, Justice Sotomayor also issued a concurring opinion. In her concurrence, Justice Sotomayor feels that the majority did not go far enough. In her concurrence, Justice Sotomayor stated, “Of course the Fourth Amendment is not concerned only with

trespassory intrusions on property.” Jones, supra, 132 S. Ct. at 954. (Sotomayor concurring). Justice Sotomayor continued by stating, “Rather, even in the absence of a trespass, ‘a Fourth Amendment’ search occurs when the Government violated a subjective expectation of privacy that society recognizes as reasonable”.” Jones, supra, 132 S. Ct. at 954-955. (Sotomayor concurring). Justice Sotomayor accused the majority of participating in an opinion that “reflects an irreducible constitutional minimum: When the Government physically invades personal property to gather information, a search occurs.” Jones, supra, 132 S. Ct. at 955. (Sotomayor concurring). Justice Sotomayor continues in her concurring opinion by stating the following:

“More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. (citations omitted). This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers, the URLs that they visit, and the e-mail addresses with which they correspond to their internet service providers; and the books, groceries, and medications they purchase to online retailers. Perhaps, as Justice ALITO notes, some people may find the ‘trade off’ to privacy for convenience ‘worthwhile,’ or come to accept this ‘diminution of privacy’ as ‘inevitable’ *post*, at --, and perhaps not. I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Website they had visited in last week, or month, or year. But whatever the societal expectations, they can attain constitutional and protective status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disintegrated to Fourth Amendment protection. (Citations omitted).

Justice Alito then filed a further concurring opinion, with whom Justice Ginsberg, Justice Breyer, and Justice Kagan joined, concurring in the judgment. In his concurring opinion, Justice Alito expressed grave concerns about twenty-first century surveillance techniques, and the technology that allows the Government to obtain and warehouse large amounts of data regarding the activities of private citizens. Just like Justice Sotomayor, Justice Alito’s concurring opinion focuses on the Katz “reasonable expectation of privacy” test to determine whether a search qualifies for Fourth Amendment Protections. Justice Alito further continues by indicating that he

would not rely on some “act of trespass” by the Government to determine a violation of this privacy expectation. Justice Alito further points out that under the prevailing approach, established by Supreme Court Precedent, “an actual trespass is neither necessary nor sufficient to establish a constitutional violation.” Jones, supra, 132 S. Ct. at 960. (Alito concurring) (citing United States v. Karo (1984), 468 U.S. 705, 713).

In his concurrence, Justice Alito discusses how Congress ultimately intervened in cases regarding wiretapping, and he suggests that perhaps Congress may be well suited to define reasonable privacy expectations in cases involving the gathering of digital and technologically advanced data from the devices we use. In the end, Justice Alito concurs with the majority opinion, but he would clearly expand the analysis of the majority to include a determination that the “reasonable expectation of privacy” test set forth in Katz, supra, is the broader test that must be applied in all cases, even when information is shared with third parties. Hence, Justice Alito, and the justices joining his concurring opinion, recognize that individuals have a constitutionally recognized expectation of privacy in their personal information even if it is disclosed to third parties or out in the public domain.

In the end, five Justices of the United States Supreme Court are clearly willing to expand the Katz analysis to situations where information is shared with third parties or otherwise in the public domain. Although it is difficult to say, it is reasonable to suppose that the four unique members of the majority in Jones, supra, may also be willing to expand the Katz test to information shared with third parties, but refused to do so under the limited facts presented in Jones.

Nevertheless, the constitutional issues raised in this case by Appellant are directly on point with the issues discussed and addressed by the United States Supreme Court in Jones, supra. Although Appellant’s subscriber information was clearly shared with the third party, that being

Time Warner Cable, the fact remains that the United States Supreme Court has indicated that the sharing of such information does not necessarily eliminate a person's reasonable expectation of privacy in said information. Under Justice Alito's discussion of Congress' role in the entire process, it appears that the Supreme Court recognizes a reasonable expectation of privacy when that expectation of privacy is either created or reflected by an act of a democratically elected legislature.

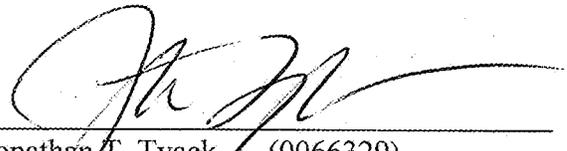
**D. The child pornography files in this case must be suppressed as fruit of the poisonous tree.**

Because the State of Ohio, through Detective Penwell, violated Defendant's Constitutional Rights against unreasonable search and seizure under the Fourth Amendment to the United States Constitution and Section 14, Article 1 of the Ohio Constitution, by obtaining his personal and protected subscriber information from Time Warner Cable through a defective subpoena purportedly issued under R.C. § 2935.23, Defendant's subscriber information must be suppressed. Furthermore, all derivative evidence, including the evidence arising out of the search of Defendant's residence, all of the evidence seized during the search of Defendant's residence, and all of the statements by the Defendant must be suppressed as fruit of the poisonous tree. Wong Sun, et al. v. United States (1963), 371 U.S. 471. Therefore, since essentially all of the evidence presented against Defendant at Trial in this matter was obtained as the fruit of the poisonous tree, and since the Trial Court erred in suppressing all evidence deriving from the unconstitutional gathering of Defendant's private subscriber information, virtually all of the evidence presented at Trial against Defendant must be suppressed.

**CONCLUSION**

For the foregoing reasons, Appellant respectfully requests this Court to accept jurisdiction of this matter, to review the matter accordingly, and to reverse the decision of the Twelfth District Court of Appeals by ordering that all evidence arising out of the warrantless discovery of Appellant's confidential IP address be suppressed.

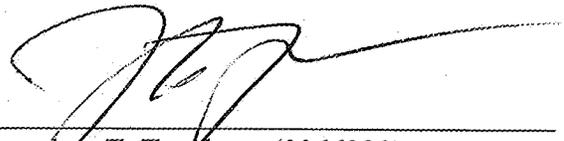
Respectfully submitted,



Jonathan T. Tyack (0066329)  
Tyack, Blackmore, Liston & Nigh Co., L.P.A.  
536 South High Street  
Columbus, Ohio 43215  
(614) 221-1341 Telephone  
(614) 228-0253 Facsimile  
jtyack@tblattorneys.com  
Attorney for Defendant-Appellant

**CERTIFICATE OF SERVICE**

This will certify that a copy of the foregoing has been forwarded to Counsel for Plaintiff-Appellee, Stephen J. Pronai, Prosecuting Attorney & Kirsten J. Gross, Assistant Prosecuting Attorney, 59 N. Main Street, London, Ohio 43140 by regular U.S. Mail, postage prepaid this <sup>8<sup>th</sup></sup> day of August, 2013.



Jonathan T. Tyack (0066329)  
Tyack, Blackmore, Liston & Nigh Co., L.P.A.  
Attorney for Defendant-Appellant

IN THE COURT OF APPEALS  
TWELFTH APPELLATE DISTRICT OF OHIO  
MADISON COUNTY

STATE OF OHIO, :  
 :  
 Plaintiff-Appellee, : CASE NO. CA2012-12-028  
 :  
 - vs - : OPINION  
 : 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. Oafis*, 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 (April 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.

IN THE COURT OF APPEALS  
TWELFTH APPELLATE DISTRICT OF OHIO  
MADISON COUNTY

STATE OF OHIO,

Plaintiff-Appellee,

- vs -

DONALD F. LEMASTERS,

Defendant-Appellant.

:

:

:

:

:

:

CASE NO. CA2012-12-028

JUDGMENT ENTRY

**FILED**  
In The Court of Appeals  
Madison County, Ohio

JUL - 8 2013

*Renee Emboldil*  
Clerk of Courts

The assignment of error properly before this court having been ruled upon, it is the order of this court that the judgment or final order appealed from be, and the same hereby is, affirmed.

It is further ordered that a mandate be sent to the Madison County Court of Common Pleas for execution upon this judgment and that a certified copy of this Judgment Entry shall constitute the mandate pursuant to App.R. 27.

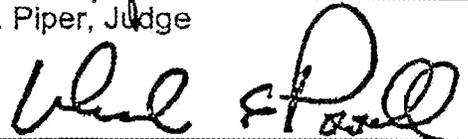
Costs to be taxed in compliance with App.R. 24.



Robert P. Ringland, Presiding Judge



Robin N. Piper, Judge



Mike Powell, Judge

17/398