

ORIGINAL

IN THE SUPREME COURT OF OHIO

STATE OF OHIO,	:	CASE NO. 13-1265
	:	
APPELLEE,	:	On Appeal from the Madison
	:	County Court of Appeals,
v.	:	Twelfth Appellate District
	:	
DONALD F. LEMASTERS,	:	Court of Appeals
APPELLANT.	:	Case No. CA2012-12-028

---

APPELLEE'S MEMORANDUM IN OPPOSITION TO JURISDICTION

---

JONATHAN T. TYACK (0066329)  
 536 South High Street  
 Columbus, OH 43215  
 Telephone: 614-221-1341  
 Email: [jttyack@tblattorneys.com](mailto:jttyack@tblattorneys.com)  
 COUNSEL FOR DEFENDANT-APPELLANT

STEPHEN J. PRONAI  
 Madison County Prosecuting Attorney  
 KIRSTEN J. GROSS (0069997)  
 Madison County Assistant Prosecuting Attorney  
 59 North Main Street  
 London, OH 43140  
 Telephone: 740-852-2259  
 Email: [kgross@co.madison.oh.us](mailto:kgross@co.madison.oh.us)  
 COUNSEL FOR PLAINTIFF-APPELLEE

RECEIVED  
 SEP 09 2013  
 CLERK OF COURT  
 SUPREME COURT OF OHIO

FILED  
 SEP 09 2013  
 CLERK OF COURT  
 SUPREME COURT OF OHIO

**TABLE OF CONTENTS**

**STATEMENT OF WHY THIS CASE DOES NOT INVOLVE A SUBSTANTIAL CONSTITUTIONAL QUESTION OR RAISE A QUESTION OF PUBLIC OR GREAT GENERAL INTEREST** .....1

**ARGUMENT IN OPPOSITION OF APPELLANT’S PROPOSITIONS OF LAW** .....1

**Proposed Proposition of Law I:** Individuals have a legitimate and reasonable expectation of privacy in their internet subscriber information such that a warrantless seizure of such private information violated the Fourth Amendment to the United States Constitution, and Article I, Section 14 of the Ohio Constitution.....1

**A. Appellant has a legitimate privacy interest in his subscriber information.....2**

**B. Revised Code §2935.23 does not allow law enforcement to circumvent the warrant requirement, especially when R.C. §2935.23 is not followed.....2**

**C. Under the analysis set forth by the United States Supreme Court in United States v. Jones, Appellant has a reasonable expectation of privacy in his internet subscriber information.....5**

**D. The child pornography files in this case must be suppressed as fruit of the poisonous street.....9**

**CONCLUSION** .....10

**CERTIFICATE OF SERVICE** .....10

## MEMORANDUM OPPOSING JURISDICTION

### STATEMENT OF WHY THIS CASE DOES NOT INVOLVE A SUBSTANTIAL CONSTITUTIONAL QUESTION OR RAISE A QUESTION OF PUBLIC OR GREAT GENERAL INTEREST

This case does not involve a constitutional question. The issue raised in this case is whether an alleged violation of the Electronic Communications Privacy Act of 1986 is tantamount to a violation of the Fourth Amendment to the United States Constitution. To find that a violation of the Fourth Amendment has occurred, the party claiming the violation must demonstrate that he had a reasonable expectation of privacy in the information that was obtained and some wrong-doing on behalf of the government. The argument that follows explains that neither occurred in this case. Appellant is attempting to create a constitutional question where one does not exist. Accordingly, jurisdiction must be denied.

Furthermore, this case does not raise a question of public or great general interest. Appellant characterizes the decision in *U.S. v. Jones* as groundbreaking and an opportunity for this Court to interpret the analysis of the United States Supreme Court in the *Jones* decision, however, the only opportunity that arises out of the *Jones* case is the opportunity to reaffirm the longstanding litany of Fourth Amendment case law with respect to physical intrusion and warrantless searches which have nothing to do with the case before this court. *State v. Lemasters* does not present any new information to the Court and therefore to revisit the issue would not fall within the jurisdictional requirement of presenting a question of public or great general interest. For those reasons, jurisdiction should also be denied.

### ARGUMENT IN OPPOSITION OF APPELLANT'S PROPOSITIONS OF LAW

**I. Proposed Proposition of Law: 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.**

The Fourth Amendment to the United States Constitution prohibits unreasonable searches and seizures. A search occurs when an expectation of privacy that society is prepared to consider reasonable is infringed upon. *State v. Keith*, 2008-Ohio-6122 (10th Dist.), quoting *United States v. Jacobsen* (1984), 466 U.S. 112, 113. A criminal defendant may invoke the protections of the Fourth Amendment “only if he can show that he had a legitimate expectation of privacy in the place searched or the item seized.” *United States v. Ziegler*, 474 F.3d 1184, 1189 (9th Cir. 2007) (quoting *Smith v. Maryland*, 442 U.S. 735, 740 (1979)). An individual cannot be said to have a reasonable expectation of privacy in that which he knowingly exposes to the public. *State v. Lopez* (Sept. 28, 1994), 2nd Dist. No. 94-CA-21, citing *Katz v. United States* (1967), 389 U.S. 347, 351.

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

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

The Electronic Communications Privacy Act (ECPA) authorizes the government to require disclosure of stored communications and transaction records by third-party service providers. Under 18 U.S.C. §2703(c)(2), “a provider of electronic communication service or remote computing service shall disclose to a government entity the ... name; ... address; ... telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address ... of a subscriber to or customer of such service....” 18 U.S.C. §2703(c)(2). Section 2708 of the ECPA specifically states that “[t]he 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. It has been widely held across

various jurisdictions, federal jurisdictions, and in the Tenth District Court of Ohio that violations of the ECPA do not warrant exclusion of evidence. *US v. Perrine*, 518 F.3d 1196, 1202 (10th Cir. 2008); *State of Ohio v. Thornton*, 2009-Ohio-5125 (Ohio App. 10th Dist), 2009 WL 3090409 (Ohio App. 10th Dist). *See also United States v. Steiger*, 318 F.3d 1039, 1049 (11th Cir. 2003); *United States v. Smith*, 155 F.3d 1051, 1056 (9th Cir. 1998); *Bansal v. Russ*, 513 F. Supp.2d 264, 282-83 (E.D. Pa. 2007); *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).

Appellant was using a file-sharing program called Shareaza to view and exchange child pornography. Shareaza is a file-sharing program that any user could use to search for files currently being shared on the network and locate Appellant's files. Making these files available to any user is consistent with a lack of expectation of privacy. Appellant had no reasonable expectation of privacy in the information that was being shared with the public through Shareaza. *United States v. Gano* (C.A. 9 Dist., 2008), 538 F.3d 1117, 1127. Furthermore, the Tenth Circuit has held that access to peer-to-peer software, "to the extent such access could expose ... information to outsiders, ... vitiates any expectation of privacy [the defendant] might have had in his computer and its contents." *Perrine, supra* at 1205. Appellant is unable to demonstrate a reasonable expectation of privacy in the information that is the subject of this case and therefore is unable to demonstrate any violation of his Fourth Amendment rights.

On October 17, 2011, Ohio's Twelfth District Court of Appeals issued a decision in a case directly on point with Appellant's case holding that the remedy of suppression is not available under the ECPA. *State v. Hamrick*, Madison App. No. CA2011-01-002 at ¶17. In that case, as in this case, the State argues that the State obtained a valid court order through its investigative subpoena, thereby complying with the ECPA. The State also argued in *Hamrick*, as

it does in this case, that there is no reasonable expectation of privacy, and therefore no Fourth Amendment violation, in the identifying information that Time Warner/Roadrunner provided to law enforcement that demonstrated that Appellant was the subscriber of the IP address presented to them.

The Twelfth District held that “[E]ven if law enforcement obtained appellant’s subscriber information pursuant to an invalid court order, suppression is not a remedy contemplated under the ECPA.” *Id.* In its holding, the court continued to state that, “[T]he statute specifically allows for civil damages and criminal punishment for violations of the ECPA, see 18 U.S.C. §§ 2707, 2701(b), but speaks 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.” *Id.* (quoting *United States v. Kennedy* (D.Kan.2000), 81 F.Supp.2d 1103 at 1110). The Twelfth District correctly noted that, “[T]he ECPA specifically states: ‘[t]he remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter.’” *Id.*; Section 2708, Title 18, U.S. Code.

The Twelfth District Court of Appeals also held in *Hamrick*, that there is no objectively reasonable expectation of privacy in subscriber information provided to a third party. *Id.* at ¶18. “[W]hat a person knowingly exposes to the public, even in his home or office, is not a subject of a Fourth Amendment protection.” *Katz v. United States* (1967), 389 U.S. 347, 351, 88 S.Ct. 507. The Court reasoned that when a person enters into an agreement with a third-party provider such as Time Warner/Roadrunner for internet service, he knowingly reveals his subscriber information associated with his IP address, including his name, address, and telephone number and cannot later claim to have a Fourth Amendment privacy interest in the information. *Id.* at

¶19. See *Smith v. Maryland* (1979), 442 U.S. 735, 743-744, 99 S.Ct. 2577 (“a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties”); *United States v. Cray* (S.D. Ga. 2009), 673 F.Supp.2d 1368, 1375; *Freedman v. Am. Online, Inc.* (D.Conn.2005), 412 F.Supp.2d 174, 181 (“courts have universally found that, for purposes of the Fourth Amendment, a subscriber does not maintain a reasonable expectation of privacy with respect to this subscriber information”); *State v. Thornton*, 2009-Ohio-5125 at ¶12.

The Hamrick case was appealed to the Ohio Supreme Court and jurisdiction was denied on February 22, 2012. See *State of Ohio v. Hamrick*, Case No. 11-2002. The issues raised in the Hamrick motion to suppress and subsequent appeals to the Ohio Twelfth District Court of Appeals and the Ohio Supreme Court were identical to the issues raised in Appellant’s original motion to suppress, subsequent appeal, and incorporated to the State’s response herein. Based on the foregoing, all of the issues outlined above have been ruled upon and suppression is not available as a remedy.

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

Subsequent to the original motion to suppress filed by Appellant’s original attorney, the United States Supreme Court decided *United States v. Jones* (January 23, 2012) 132 S.Ct. 945, 2012 WL 171117. In his supplemental motion to suppress, Appellant cites to this case as a means to reopen the issue of whether a Fourth Amendment reasonable expectation of privacy exists in the information that Time Warner/Roadrunner turned over to law enforcement in an effort to present suppression as a viable remedy.

The narrowed down issue is whether a user of an IP address has a reasonable expectation of privacy in the subscriber information attached to the IP address under the Fourth Amendment.

In *State v. Thornton*, the Tenth District Court of Appeals addressed this very issue. The facts in *Thornton* were not perfectly analogous as they involved multiple users of the same computer. However, the case has many similarities to the case at bar. An Upper Arlington Police Officer used a peer-to-peer computer program (a file sharing program) and determined that suspected child pornography was on a suspect's computer; he used the file sharing network to download a suspected child pornography file from the suspect IP address and confirmed that it contained child pornography. The officer then prepared a court order to obtain subscriber information associated with the IP address which was signed by a Franklin County Court Common Pleas Judge. The court order was faxed to Time Warner/Roadrunner's legal department and Time Warner/Roadrunner provided the user information attached to the IP address. Thornton was not the subscriber connected to the IP address. However, further investigation revealed that Thornton and the subscriber used the same computer. A motion to suppress was filed prior to a trial to the court in part asking that the court suppress the evidence because defendant's Fourth Amendment rights had been violated. The trial court overruled said motion and proceeded to find, after trial, Thornton guilty on certain possession offenses and not guilty on certain pandering offenses. The matter was then appealed citing to violations of the ECPA. The court emphasized that federal courts have consistently held that the remedy for violation of the ECPA is a civil action for damages not suppression. Of particular note to the case at bar, the court went on to state, "Moreover, a customer does not have a reasonable expectation of privacy in subscriber information given to an internet service provider." *United States v. Perrine* (2008), 518 F.3d 1196, 1204; *United States v. Sherr* (2005), 400 F.Supp.2d 843 at 848. Indeed, the Tenth District Court of Appeals in *Perrine* addressed this very issue. *Perrine* also appears to

make a broader Fourth Amendment challenge to the government's acquisition of his subscriber information from Yahoo! and Cox. The district court held:

"the identifying information at issue here-defendant's name, address, etc.-was information that he voluntarily transmitted to the third-party internet providers, Cox and Yahoo!. Indeed, defendant also admitted at the hearing that he had enabled peer-to-peer file sharing on this computer, thereby giving anyone with internet access the ability to gain entrance to his computer. Under such a scenario, a defendant holds no reasonable expectation of privacy that the Fourth Amendment will protect." *Perrine* at 1202.

Every federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation. *See, e.g., Guest v. Leis*, 255 F.3d 325, 336 (6th Cir.2001). *Id.* at 10.

Similarly, the United States District Court, District of Maryland found in *United States v. Sherr*, that:

"[T]he defendant's constitutional rights were not violated when AOL divulged his subscriber information to the government. The defendant avers that he had a reasonable and legitimate expectation of privacy in the subscriber information that he provided to AOL. Def.'s Mem. in Supp. of Mot. to Suppress Illegal Search and Seizure 1-2; Def.'s Reply Mem. 2-4; Def's Supp. Mot. and Mem. to Suppress Search Warrant 1. The courts that have already addressed this issue, however, uniformly have found that individuals have no Fourth Amendment privacy interest in subscriber information given to an ISP." *See, e.g., United States v. Hambrick*, 55 F.Supp.2d 504 (W.D.Va. 1999), *aff'd*.

These cases clearly stand for the proposition that there is no reasonable expectation of privacy under the Fourth Amendment and subscriber information relating to an IP address. Because no such expectation of privacy exists, the evidence obtained as a result of this information should not be suppressed as the information was not obtained in violation of the Fourth Amendment.

The *Jones* case has no bearing on this long-standing case law. In *Jones*, the issue before the United States Supreme Court was whether the government's placement of a global

positioning system (GPS) on an automobile as a method to track and record its movements constitutes a search under the Fourth Amendment. The Court, not surprisingly, held that it was a search. *Jones* at 949. The facts of the *Jones* case show that the government obtained a search warrant authorizing the placement of a GPS device on the automobile of a private vehicle within 10 days of the date of issue of the warrant in the District of Columbia. The GPS device was placed on the vehicle in question on the eleventh day and not in the District of Columbia, but in Maryland. *Id.* at 948. The government conceded noncompliance with the search warrant, but argued that the search warrant was not needed, as the tracking device was attached to the vehicle in a public parking lot where the vehicle owner would enjoy no reasonable expectation of privacy. *Id.* The Supreme Court rejected that argument and very clearly stated, “[T]he Government physically occupied private property for the purpose of obtaining information. 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.* at 949. The *Jones* case is a case of physical intrusion, a trespass, by the government to obtain information about a defendant. It is not a reasonable expectation of privacy case as presented by Appellant.

The United States Supreme Court majority holding that the *Jones* case represents a trespass to gain information, and therefore constitutes a search under the Fourth Amendment to the United States Constitution, includes Justice Scalia, Chief Justice Roberts, Justice Kennedy, Justice Thomas, and Justice Sotomayor. Justice Sotomayor also submits a concurring opinion in which she suggests that, “it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.” *Id.* at 957. This is the statement that the Appellant latches onto in his argument that the subscriber information that he voluntarily provided to Time Warner/Roadrunner is entitled to some sort of

privacy protection under the Fourth Amendment in direct contravention to existing case law. Yet even Justice Sotomayor acknowledges that, “resolution of these difficult questions in this case is unnecessary, however, because the Government’s physical intrusion on the Jones’ Jeep supplies a narrower basis for decision.” *Id.*

The holding in *Jones* is simple and uncontroverted. It is a trespass case, not a reasonable expectation of privacy case, and has no bearing on Appellant’s suppression motion. In this case, the State complied with the requirements of the ECPA to obtain Appellant’s information. Even if there was a violation of the ECPA, the remedy is civil between Appellant and Time Warner/Roadrunner, his internet service provider. The information obtained was voluntarily provided to Time Warner/Roadrunner and no reasonable expectation of privacy attaches to it. Law enforcement in this case acted reasonably based on the information it had before it to obtain an investigative subpoena.

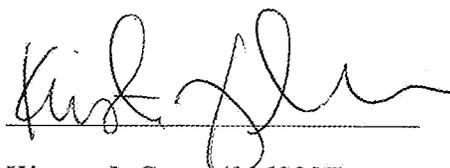
**D. The child pornography files in this case must be suppressed as fruit of the poisonous tree.**

Appellant’s argument does not present any facts related to a reasonable expectation of privacy. Because there is no credible Fourth Amendment argument in this case, as detailed in the State’s argument above, suppression is not an available remedy.

**CONCLUSION**

Mr. Lemasters has failed to demonstrate that this case raises a substantial constitutional question or that this case is of public or great general interest. Accordingly, the State respectfully requests that this Court deny jurisdiction.

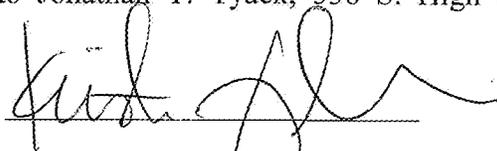
Respectfully submitted,



Kirsten J. Gross (0069997)  
Assistant Prosecuting Attorney  
Madison County Ohio  
59 N. Main Street  
London, OH 43140  
740.852.2259 Telephone  
740.845.1694 Facsimile  
kgross@co.madison.oh.us

**CERTIFICATE OF SERVICE**

The undersigned hereby certifies that a copy of the foregoing was deposited in the U.S. Mail on the 6<sup>th</sup> day of September, 2013, addressed to Jonathan T. Tyack, 536 S. High Street, Columbus, Ohio 43215.



Kirsten J. Gross (0069997)  
Assistant Prosecuting Attorney  
Madison County Ohio  
59 N. Main Street  
London, OH 43140