[Cite as *State v. Thornton* , 2009-Ohio-5125.]

IN THE COURT OF APPEALS OF OHIO

TENTH APPELLATE DISTRICT

State of Ohio,	:	
Plaintiff-Appellee,	:	
		No. 09AP-108
v.	:	(C.P.C. No. 07CR08-5627)
Harold Thornton, II,	:	(REGULAR CALENDAR)
Defendant-Appellant.	:	

D E C I S I O N

Rendered on September 29, 2009

Ron O'Brien, Prosecuting Attorney, and *Laura R. Swisher*, for appellee.

Tyack, Blackmore & Liston Co., L.P.A., and *Thomas M. Tyack*, for appellant.

APPEAL from the Franklin County Court of Common Pleas

KLATT, J.

{¶1} Defendant-appellant, Harold Thornton, II, appeals from a judgment of conviction and sentence entered by the Franklin County Court of Common Pleas. Because the trial court properly denied appellant's motion to suppress, we affirm that judgment.

{¶2} On April 18, 2007, Officer John Priest of the Upper Arlington Police Department ("UAPD") conducted an internet investigation into child pornography using a peer-to-peer computer program called Limewire. Limewire allows users, those who download the program onto their computer, to search for and share files with other users of the program. In essence, Limewire allows a user to have access to other users' computer files and to download those files onto the user's computer.

{¶3} Officer Priest searched the Limewire network for files with titles that included words indicative of child pornography. His search generated a list of files on the Limewire network containing those words. The list also included the internet protocol address ("IP address") of each of the computers that possessed the relevant files. A computer's IP address is similar to a home's mailing address and is unique to the computer's location.

{¶4} Officer Priest recognized one of the IP addresses as being associated with the Columbus, Ohio region and, more specifically, Time Warner's Road Runner internet service.[1] Using the Limewire program, Officer Priest downloaded the file from that IP address and confirmed that it contained child pornography. Officer Priest then prepared a court order to obtain the subscriber information associated with that IP address to find the location of the computer. After a judge of the Franklin County Court of Common Pleas signed the court order, Priest delivered it, via fax, to Time Warner's legal department in Connecticut. Time Warner's response indicated that the IP address was assigned to Terri

[1] Just as phone numbers include an area code that is indicative of a certain location, IP addresses have certain numbers that correlate to certain areas and providers. In this case, the IP address began with the numbers "24.95" which Officer Priest explained was specific to Time Warner's Columbus Road Runner network.

Perry, who lived at 568 South Terrace Avenue, in Columbus, Ohio. Appellant Perry are married.

{¶5} With that information, Officer Priest requested and obtained a search warrant for Perry's home. On May 7, 2007, the UAPD executed the search warrant at Perry's home. A number of people, including appellant, were in the house at the time. Appellant spoke with Officer Priest and informed him that the Road Runner internet service was exclusive to the computer in the upstairs bedroom that he shared with Perry.[2] He also told Priest that he was the primary user of that computer and that he used the Limewire program. In a subsequent interview with the police, appellant admitted to installing the Limewire program on the computer.

{¶6} Pursuant to the search warrant, police seized Perry's computer from the house. A search of the computer's hard drive revealed seven files that contained child pornography. As a result, a Franklin County Grand Jury indicted appellant with 14 counts of pandering sexually oriented matter involving a minor in violation of R.C. 2907.322. Counts 1 through 7 of the indictment alleged that appellant, with knowledge of the character of the material or performance involved, created, recorded, photographed, filmed, developed, reproduced, or published material that showed a minor participating or engaging in sexual activity, and/or advertised, sold, distributed, transported, disseminated, exhibited, or displayed any such material (hereinafter referred to as the "creation counts"). Counts 8 through 14 alleged that appellant, with knowledge of the character of the material or performance involved, solicited, received, purchased, exchanged, possessed or controlled material that showed a minor participating or

engaging in sexual activity (hereinafter referred to as the "possession counts"). Appellant entered not guilty pleas to the charges and proceeded to trial.

[2] Two other computers were found in the home. One was not connected to the internet, and the other was connected to the internet but through another internet service provider, not Time Warner.

{¶7} Appellant filed a motion to suppress the evidence obtained by the UAPD. His motion claimed that the UAPD: (1) conducted an illegal search of Perry's computer, and (2) illegally obtained subscriber information from Time Warner. After a hearing, the trial court denied appellant's motion. The matter was then tried to the court, who found appellant guilty of the possession counts but not guilty of the creation counts. The trial court sentenced appellant accordingly.

{¶8} Appellant appeals and assigns the following error:

> I. THE TRIAL COURT ERRED IN OVERRULING THE MOTION TO SUPPRESS AS THE ACTIONS OF THE UPPER ARLINGTON POLICE DEPARTMENT VIOLATED THE DEFENDANT'S RIGHTS UNDER THE FOURTH AND FOURTEENTH AMENDMENTS OF THE CONSTITUTION OF THE UNITED STATES AND THE CONSTITUTION OF THE STATE OF OHIO.

{¶9} Appellant contends the trial court erred when it overruled his motion to suppress. Appellate review of a motion to suppress presents a mixed question of law and fact. *State v. Groce,* 10th Dist. No. 06AP-1094, 2007-Ohio-2874, ¶6. When considering a motion to suppress, the trial court assumes the role of trier of fact, and is therefore, in the best position to resolve factual questions and evaluate the credibility of witnesses. *State v. Mills* (1992), 62 Ohio St.3d 357, 366. Consequently, an appellate court must accept the trial court's findings of fact if they are supported by competent, credible evidence. *State v. Brooks* (1996), 75 Ohio St.3d 148, 154. Accepting these facts as true, the appellate court must then independently determine, without deference to the conclusion of the trial court, whether the facts satisfy the applicable legal standard. *State v. Burnside,* 100 Ohio St.3d 152, 2003-Ohio-5372, ¶8; *Columbus v. Dials,* 10th Dist. No. 04AP-1099, 2005-Ohio-6305, ¶17-18.

{¶10} Appellant first contends that the UAPD's initial search of Perry's computer was an illegal general, exploratory search. We disagree.

{¶11} 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. *State v. Keith*, 10th Dist. No. 08AP-28, 2008-Ohio-6122, ¶16, quoting *United States v. Jacobsen* (1984), 466 U.S. 112, 113, 104 S.Ct. 1652, 1656. 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), 2d Dist. No. 94-CA-21, citing *Katz v. United States* (1967), 389 U.S. 347, 351, 88 S.Ct. 507, 511; *Keith*.

{¶12} Appellant knowingly exposed to the public the files found on Perry's computer and the IP address associated with that computer through the use of the Limewire program on the computer. Therefore, he had no reasonable expectation of privacy in that evidence. *United States v. Ganoe* (C.A.9, 2008), 538 F.3d 1117, 1127 (no legitimate expectation of privacy in files defendant made available to public using Limewire software); *United States v. Borowy* (D.Nev. 2008), 577 F.Supp.2d 1133, 1136 (same); *United States v. Forrester* (C.A.9, 2008), 512 F.3d 500, 510 (no reasonable expectation of privacy in IP address); *United States v. Li* (Mar. 20, 2008), S.D. Cal. No. 07 CR 2915 JM, at 5, slip opinion (same). In that situation, Fourth Amendment protections are not implicated because a search does not occur. See *Keith*, citing *State v. Sheppard* (2001), 144 Ohio App.3d 135, 141.

{¶13} Appellant next addresses the process used by the UAPD to obtain Perry's subscriber information from Time Warner. Subscriber information, such as name,

address, and phone number, is information that the customer provides to the internet service provider in order to receive internet service. Appellant first argues that Time Warner improperly disclosed Perry's subscriber information to the UAPD. The Electronic Communications Privacy Act, 18 U.S.C. 2701 et. seq. ("ECPA") regulates the disclosure of electronic communications and subscriber information. Specifically, 18 U.S.C. 2703(c)(1) provides instances when a governmental entity may require an internet service provider such as Time Warner to disclose a customer's subscriber information. Appellant contends Time Warner violated this portion of the statute by disclosing Perry's subscriber information without her consent. See 18 U.S.C. 2703(c)(1)(C).

{¶14} Assuming without deciding that appellant has standing to raise this argument,[3] federal courts addressing this matter have consistently held that the remedy for a violation of the ECPA is a civil action for damages, not suppression. 18 U.S.C. 2708; *United States v. Perrine* (C.A.10, 2008), 518 F.3d 1196, 1202; *United States v. Beckett* (S.D.Fla. 2008), 544 F.Supp.2d 1346,1350; *United States v. Sherr* (D. Md. 2005), 400 F.Supp.2d 843, 848; *United States v. Kennedy* (D.Kan. 2000), 81 F.Supp.2d 1103, 1110. Therefore, even if Time Warner's disclosure violated the ECPA,[4] that statutory violation would not provide appellant with a basis to suppress the subscriber information. Moreover, a customer does not have a reasonable expectation of privacy in subscriber information given to an internet service provider. *Perrine* at 1204; *Sherr* at 848.

{¶15} Finally, appellant contends that the court order requiring Time Warner's disclosure of his wife's subscriber information was not a valid subpoena. Appellant

[3] Time Warner disclosed information relating to Perry, its subscriber, not appellant.

[4] We note that 18 U.S.C. 2703(c)(1)(A) and (B) allows for disclosure pursuant to a warrant or court order.

makes this argument because Time Warner's letter in response to the court order noted that it was responding to a subpoena. Appellant argues that the order was not a valid subpoena because it did not comply with Crim.R. 17 and because it was delivered to an out-of-state entity. Regardless of whether the court order was a valid subpoena, appellant does not argue that the court order was invalid. See 18 U.S.C. 2703(c)(1)(B). Even if the court order was invalid, and even if Time Warner's response to such an order would violate the ECPA, appellant's remedy would be a civil action against Time Warner, not suppression of evidence. 18 U.S.C. 2707; 18 U.S.C. 2708.

{¶16} For all these reasons, the trial court did not err by denying appellant's motion to suppress. Accordingly, appellant's assignment of error is overruled and we affirm the judgment of the Franklin County Court of Common Pleas.

Judgment affirmed.

FRENCH, P.J., and CONNOR, J., concur.