FILED
United States Court of Appeals
Tenth Circuit

July 13, 2010

Elisabeth A. Shumaker
Clerk of Court

PUBLISH

UNITED STATES COURT OF APPEALS

TENTH CIRCUIT

UNITED STATES OF AMERICA, Plaintiff-Appellee, v. MICHAEL RAY RENIGAR, Defendant-Appellant.	No. 10-5015

APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OKLAHOMA
(D.C. No. 4:09-CR-00068-JHP-1)

Submitted on the briefs:

Julia L. O'Connell, Federal Public Defender; Barry L. Derryberry, Research & Writing Specialist, Office of the Federal Public Defender, Tulsa, Oklahoma, for Defendant-Appellant.

Thomas Scott Woodward, United States Attorney; Susan K. Morgan, Assistant United States Attorney, Tulsa, Oklahoma, for Plaintiff-Appellee.

Before **BRISCOE,** Chief Judge, **TACHA,** and **O'BRIEN**, Circuit Judges.

BRISCOE, Chief Judge.

Defendant Michael Ray Renigar entered a conditional guilty plea to one count of possessing child pornography in violation of 18 U.S.C. § 2252(a)(4)(B) and (b)(2).

Renigar now appeals the district court's denial of his pretrial motion to suppress evidence and statements. He contends the affidavit underlying the search warrant did not provide probable cause to search his residence. Specifically, he argues that tracing child pornography to an Internet Protocol ("IP") address which was associated with his residential address did not provide an adequate nexus between the evidence of the crimes alleged and the location to be searched—his residence. Exercising jurisdiction pursuant to 28 U.S.C. § 1291, we AFFIRM.[1]

I

On April 9, 2009, Federal Bureau of Investigation ("FBI") Special Agent Joseph Cecchini submitted an application for a search warrant to Magistrate Judge T. Lane Wilson of the United States District Court for the Northern District of Oklahoma. In the application, Cecchini sought permission to search 7148 East 10th Street Apt. #2 in Tulsa, Oklahoma for evidence associated with the possession and/or transmission of child pornography in violation of 18 U.S.C. §§ 2252 and 2252A.

Cecchini attached an affidavit to his application which purported to provide probable cause to search the aforementioned residential address. The affidavit stated that on December 8, 2008, while accessing a publicly available P2P file-sharing network[2]

---

[1] After examining the briefs and appellate record, this panel has determined unanimously that oral argument would not materially assist in the determination of this appeal. See Fed. R. App. P. 34(a)(2); 10th Cir. R. 34.1(G). The case is, therefore, submitted without oral argument.

[2] As we have explained previously, a peer-to-peer, or P2P file-sharing network (continued...)

from an FBI computer located in Calverton, Maryland, FBI Special Agent Stacie Lane connected her computer to the computer of a user named "Reniegar," whose computer was accessing the P2P network from the IP address[3] 68.14.166.230. The affidavit explained that Lane observed that "Reniegar" had made several files on his computer which contained child pornography available for download by the other users of the P2P network, but that Lane was unsuccessful in her attempt to download several of these files.

The affidavit went on to state that on February 17, 18, and 19, 2009, another Special Agent accessed the same P2P network from the FBI's offices in Phoenix, Arizona. The affidavit explained that in much the same manner as Lane, this second Special Agent observed that a user named "Reniegar," accessing the P2P network from the IP address 68.14.166.230, had made several files containing child pornography available for download by other users. The affidavit explained, however, that unlike Lane, this second Special Agent was able to successfully download several of the files available on "Reniegar's" computer.

The affidavit next stated that based upon the information gathered by Lane and the

---

[2](...continued)
allows individual users to download designated files from one another's computers via the internet. See United States v. Shaffer, 472 F.3d 1219, 1221-22 (10th Cir. 2007).

[3] "'An IP address is a unique number identifying the location of an end-user's computer. When an end-user logs onto an internet service provider, they are assigned a unique IP number that will be used for that entire session. Only one computer can use a particular IP address at any specific date and time.'" United States v. Henderson, 595 F.3d 1198, 1199 n.1 (10th Cir. 2010) (quoting United States v. Hamilton, 413 F.3d 1138, 1140 n.2 (10th Cir. 2005)) (internal alterations omitted).

Special Agent in Phoenix, the FBI set out to obtain further information regarding the IP address from which "Reniegar" was accessing the P2P network. The affidavit explained that agents performed a search of the American Registry for Internet Numbers which indicated that the IP address in question is registered to the internet service provider, Cox Communications ("Cox"). The affidavit then stated that FBI agents served an administrative subpoena on Cox who, in turn, advised the FBI that at all relevant times, the IP address in question was assigned to the account of Michael Renigar and that the residential address listed for Renigar's account was 7148 East 10th Street Apt. #2 in Tulsa, Oklahoma. Finally, the affidavit explained that subsequent public records searches performed by the agents identified Michael R. Renigar as a resident of the address Cox had provided.

In addition to detailing the investigative efforts of the FBI, the affidavit also included a section entitled "Background on Computers and Child Pornography." This section detailed the process by which an individual may utilize a computer to access, store, and/or share computer files, including child pornography. It also explained that even if an individual intends to erase all evidence of his or her previous receipt, possession, and/or transmission of designated computer files, a record of the individual's activities may nonetheless be preserved on the computer's hard drive.

After a review of the information contained in Cecchini's affidavit, the magistrate judge issued a warrant to search the aforementioned residential address in Tulsa, Oklahoma for evidence associated with the possession and/or transmission of child

pornography in violation of 18 U.S.C. §§ 2252 and 2252A. The warrant was served on April 13, 2009, at which time FBI agents encountered the defendant, Michael Ray Renigar. Agents seized a computer and several DVDs from Renigar's apartment which contained various depictions of child pornography. At the time of the search warrant's execution, Renigar also gave several incriminating statements in response to questioning by agents.

Subsequently, a grand jury empaneled in the United States District Court for the Northern District of Oklahoma returned a two count indictment charging Renigar with possession of child pornography in violation of 18 U.S.C. § 2252(a)(4)(B) and (b)(2) (Count One) and distribution or attempted distribution of child pornography in violation of 18 U.S.C. § 2252(a)(2) and (b)(1) (Count Two). Renigar then filed a motion to suppress both the physical evidence seized during the execution of the search warrant and the statements he made at the time. Renigar argued that Cecchini's affidavit had failed to provide probable cause for the warrant which, in turn, according to Renigar, caused his entire encounter with the FBI to be in violation of the Fourth Amendment.

A brief hearing was conducted on the matter, at which time the district court orally denied Renigar's motion. Renigar subsequently entered a conditional guilty plea to Count One of the indictment, reserving his right to appeal the district court's denial of his motion to suppress. Count Two of the indictment was dismissed. After accepting his plea, the district court sentenced Renigar to 108 months' imprisonment to be followed by a 10-year term of supervised release.

II

On appeal, Renigar contends that the affidavit which Cecchini offered in support of his application for the search warrant did not provide probable cause to search his residence for evidence associated with the possession and/or transmission of child pornography. Specifically, Renigar alleges "that probable cause was not furnished by [Cecchini's] affidavit because a nexus was not adequately established between the evidence of crime and the location to be searched."[4] Aplt. Br. at 9-10.

When faced with an appeal from the district court's denial of a motion to suppress, "[t]he ultimate question of reasonableness under the Fourth Amendment is a legal conclusion that we review de novo." United States v. Grimmett, 439 F.3d 1263, 1268 (10th Cir. 2006). However, where, as here, "the search . . . was done pursuant to a warrant, we review the issuing judge's finding of probable cause with great deference . . . ." Id. We ask only "whether, under the totality of the circumstances presented in the affidavit, the magistrate judge had a 'substantial basis' for determining that probable cause existed." United States v. Tuter, 240 F.3d 1292, 1295 (10th Cir. 2001) (internal quotation marks and citation omitted). "The test is whether the facts presented in the affidavit would warrant a [person] of reasonable caution to believe that evidence of a crime will be found at the place to be searched." United States v. Artez, 389 F.3d 1106,

[4] In his motion to suppress, Renigar also argued that the affidavit failed to establish probable cause because the information regarding the FBI agents' accessing of child pornography via the P2P network was so old as to be stale. Renigar has, however, abandoned this argument on appeal.

1113 (10th Cir. 2004) (quotation, citation, and emphasis omitted).

In the instant case, we conclude that the information in Cecchini's affidavit would cause a person of reasonable caution to believe that evidence of the possession and/or transmission of child pornography would be found at the residential address in question. Indeed, in light of the information in the affidavit which linked the IP address in question to both child pornography and to the residential address, as well as the affidavit's discussion of computer technology, there was a strong suggestion that the computer which "Reniegar" used to access the P2P network would be found at the apartment and would contain evidence associated with child pornography and/or its transmission.

When addressing this same issue or similar issues, other circuits have reached the same conclusion. For example, in United States v. Perez, 484 F.3d 735, 740 (5th Cir. 2007), the Fifth Circuit concluded that it was "clear that there was a substantial basis to conclude that evidence of criminal activity would be found at [the defendant's address]," based upon an affidavit which "included the information that . . . child pornography . . . had been transmitted over [a certain] IP address . . . and that this IP address was assigned to [the defendant]" who resided at the address listed in the affidavit. Likewise, in United States v. Vosburgh, 602 F.3d 512 (3d Cir. 2010), the Third Circuit concluded that "it was fairly probable that instrumentalities or evidence of [child pornography]—such as computers and computer equipment—would be found in [the defendant's] apartment," id. at 527 (internal quotation marks omitted), based upon an affidavit which "explained that . . . someone using a computer with [a certain] IP address . . . attempted to download

a video that purported to be hardcore child pornography . . . . [and] that on the day in question, the relevant IP address was assigned to a Comcast account registered to [the defendant's] apartment," id. at 526.

In sum, we conclude that the magistrate judge had a "substantial basis" for determining that there was probable cause to search Renigar's apartment. Having reached that conclusion, we need not address Renigar's contention that the good faith exception to the exclusionary rule established in United States v. Leon, 468 U.S. 897 (1984), should not apply.

III

The judgment of the district court is AFFIRMED.