RECOMMENDED FOR FULL-TEXT PUBLICATION
Pursuant to Sixth Circuit Rule 206

File Name: 08a0156p.06

UNITED STATES COURT OF APPEALS

FOR THE SIXTH CIRCUIT

UNITED STATES OF AMERICA,
Plaintiff-Appellee,

v.

BRENT TERRY,
Defendant-Appellant.

No. 07-3757

Appeal from the United States District Court
for the Southern District of Ohio at Cincinnati.
No. 06-00091—Sandra S. Beckwith, Chief District Judge.

Argued: March 17, 2008

Decided and Filed: April 15, 2008

Before: BOGGS, Chief Judge; ROGERS, Circuit Judge; and SHADUR, District Judge.[*]

COUNSEL

ARGUED: Richard W. Smith-Monahan, OFFICE OF THE FEDERAL PUBLIC DEFENDER, Cincinnati, Ohio, for Appellant. Christopher K. Barnes, ASSISTANT UNITED STATES ATTORNEY, Cincinnati, Ohio, for Appellee. **ON BRIEF:** Richard W. Smith-Monahan, OFFICE OF THE FEDERAL PUBLIC DEFENDER, Cincinnati, Ohio, for Appellant. Jeb T. Terrien, ASSISTANT UNITED STATES ATTORNEY, Cincinnati, Ohio, for Appellee.

OPINION

BOGGS, Chief Judge. Brent Terry entered a conditional guilty plea to one count of possession of images of minors engaged in sexually explicit conduct, in violation of 18 U.S.C. § 2252(a)(4)(B), reserving his right to appeal the district court's denial of his motion to suppress. Terry argues that the search warrant permitting federal agents to search his home was not grounded upon probable cause, and that the search therefore violated the Fourth Amendment. For the following reasons, we affirm the judgment of the district court.

---

[*]The Honorable Milton I. Shadur, United States District Judge for the Northern District of Illinois, sitting by designation.

I

The facts of this case are undisputed. In the early morning hours of October 14, 2004, Internet service provider AOL (formerly known as America Online) intercepted two e-mail messages containing a known child pornography image. These messages were sent from the e-mail address "skippie4u@aol.com" to an unknown recipient (or recipients) at 2:35 a.m. and again at 2:36 a.m. The following day, AOL forwarded the image, along with the screen name, e-mail address, and zip code of the user, to the National Center for Missing and Exploited Children (NCMEC), which in turn forwarded the information to Immigration and Customs Enforcement (ICE) officers. Upon issuance of a summons, AOL provided ICE more information on the "skippie4u" screen name, which revealed that "skippie4u" was one of three screen names assigned to a master AOL account registered to Roy Terry, who lived at 10 Township Avenue in Cincinnati, Ohio. Defendant Brent Terry (Roy's son) was the registered user of the "skippie4u" screen name. ICE confirmed through the Postal Service that both Roy and Brent Terry received mail at 10 Township Avenue.

Based on this information, ICE obtained a search warrant for the Township Avenue address and executed it on March 21, 2005. The record does not reveal what, if anything, was searched and/or seized from the Township Avenue residence. It appears, however, that ICE was most interested in Brent Terry, not his father, because the e-mail account used to send the image was registered specifically to the younger Terry. During the search, ICE reported that Roy Terry

> was interviewed at which time he stated that he has an Internet account through America Online (AOL), which is utilized, by himself, Brenda TERRY and Brent TERRY. Roy TERRY stated that Brent TERRY lives at 16 Walnut St. Cincinnati, OH and has access to the aforementioned AOL account from that address. Roy TERRY also stated that Brent TERRY has a computer that he uses at that address to access the account. Furthermore, Roy TERRY informed [ICE] that Brent TERRY utilizes the screen name Skippie 4U when accessing the aforementioned AOL account from his address 16 Walnut St. Cincinnati, OH.

Application and Affidavit for Search Warrant at 8 (capitalization in original). Roy also told ICE that Brent had lived at the Walnut Street address, which he rented from Roy, for approximately one and a half years. Thus, he was living in the Walnut Street residence at the time his e-mail account was used to send the illegal image.

ICE then obtained the search warrant for 16 Walnut Street that is the subject of this appeal. That warrant was executed on the same day, and agents recovered a laptop computer, three hard drives, and various external media from the residence, which were found to contain a total of 123 images and eight videos of minors engaged in sexually explicit conduct. Terry later moved to suppress this evidence, which motion the district court denied. Thereafter Terry entered a conditional guilty plea pursuant to Federal Rule of Criminal Procedure 11(a)(2) and appealed the denial of his suppression motion to this court.

II

"When reviewing the denial of a motion to suppress, we review the district court's findings of fact for clear error and its conclusions of law *de novo*." *United States v. Foster*, 376 F.3d 577, 583 (6th Cir. 2004) (quoting *United States v. Hurst*, 228 F.3d 751, 756 (6th Cir. 2000)). However, when judging the sufficiency of an affidavit to establish probable cause in support of a search warrant, the Supreme Court has "repeatedly said that after-the-fact scrutiny . . . should not take the form of de novo review. . . . Rather, reviewing courts are to accord the magistrate's determination 'great deference.'" *United States v. Allen*, 211 F.3d 970, 973 (6th Cir. 2000) (en banc) (quoting *Illinois v. Gates*, 462 U.S. 213, 236 (1983)). This means that "so long as the magistrate had a

'substantial basis for . . . conclud[ing]' that a search would uncover evidence of wrongdoing, the Fourth Amendment requires no more." *Ibid.* (quoting *Gates*, 462 U.S. at 236). Accordingly, "[t]his circuit has long held that an issuing magistrate's discretion should only be reversed if it was arbitrarily exercised." *Ibid.*

In deciding whether to issue a search warrant, the Fourth Amendment requires "the issuing magistrate . . . simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Gates*, 462 U.S. at 238; *see also United States v. Smith*, 510 F.3d 641, 652 (6th Cir. 2007) (referring to this as a 'totality of the circumstances' approach). A "fair probability" is not interpreted as connoting any particular mathematical degree of probability. *See Maryland v. Pringle*, 540 U.S. 366, 371 (2003) ("The probable-cause standard is incapable of precise definition or quantification into percentages because it deals with probabilities and depends on the totality of the circumstances. . . . Finely tuned standards such as proof beyond a reasonable doubt or by a preponderance of the evidence . . . have no place in the probable-cause decision.") (internal quotation omitted).

Terry asserts that that there was an insufficient nexus to connect the intercepted child pornography image to his home computer, arguing that the AOL e-mail account used to send the illicit image could have been accessed from any computer with an Internet connection. We certainly agree that to establish probable cause to support a search warrant, there must be some nexus between the illegal activity suspected and the property to be searched. *See United States v. McPhearson*, 469 F.3d 518 (6th Cir. 2006) (mere fact that man arrested for non-drug offense had drugs on his person did not establish the requisite nexus to search his home for drugs); *United States v. Carpenter*, 360 F.3d 591, 594 (6th Cir. 2004) (en banc) (fact that marijuana was found growing near a residence, by itself, "f[e]ll short of establishing the required nexus between the . . . residence and evidence of marijuana manufacturing"). We do not agree, however, that such a nexus was lacking in this case.

The government's affidavit established that (1) the AOL e-mail account belonging to the "skippie4u" screen name sent two e-mail messages at approximately 2:30 a.m. containing a known child pornography image; (2) Brent Terry was the registered user of the "skippie4u" screen name; (3) Brent Terry lived at 16 Walnut Street at the time the e-mail messages were sent; and (4) Brent Terry had a computer at that address through which he accessed the "skippie4u" e-mail account used to send the messages. It requires no great leap of logic to conclude that the computer in Terry's home was probably used to send the intercepted messages. Given that the probable cause standard deals with "the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act," *Gates*, 462 U.S. at 231 (quoting *Brinegar v. United States*, 338 U.S. 160, 175 (1949)), the district court did not err in concluding that "as a matter of plain common sense, if . . . a pornographic image has originated or emanated from a particular individual's email account, it logically follows that the image is likely to be found on that individual's computer or on storage media associated with the computer." Dist. Ct. Order at 7. There are other possibilities, of course—a hacker illicitly using Terry's e-mail account, for example—but probable cause does not require "near certainty," only a "fair probability." *See United States v. Martin*, 289 F.3d 392, 400 (6th Cir. 2002) ("Although innocent explanations for some or all of these facts may exist, this possibility does not render the . . . determination of probable cause invalid.").[1]

In a similar case, this court upheld probable cause to search a home where the defendant had purchased subscriptions to known child pornography websites, but where it was unknown precisely which computer he had used to access those sites. *See United States v. Wagers*, 452 F.3d 534 (6th

[1]Though not central to our analysis on this point, the fact that the images were sent at approximately 2:30 in the morning further reduces the likelihood that a computer other than the one in Terry's home was used.

Cir. 2006). In *Wagers*, the defendant used a business-based checking card to subscribe to two websites that made available both legal and illegal pornography. He argued that since "his subscriptions were connected only to his business office, not to his home," there was "nothing . . . [to] connect[] the residence to the alleged child pornography offenses." *Id.* at 539. We rejected this "feeble" argument, observing that the affidavit "aver[red] that an [Internet Protocol (IP)] address assigned by Insight [Communications] . . . was used to purchase both memberships" and that the defendant "used Insight at his home but not his office . . . ." *Ibid.* Logically, we concluded that the defendant's "home would be well within the ambit of a properly issued search warrant." *Ibid.* We further noted that "[e]ven if the home were only one of two locations—home and office—served by Insight, there would be sufficient evidence to support probable cause." *Ibid.*

Terry attempts to distinguish *Wagers* on the ground that, unlike in *Wagers*, there was no IP information either to tie his computer to the e-mail messages, or even to limit the possible number of computers that could have been used to send the message. But the *Wagers* opinion did not hold that IP information was an indispensable prerequisite to obtaining a search warrant in a case involving Internet-based child pornography, only that such information contributed to the totality of the probable-cause determination. Indeed, *Wagers* favorably cited several cases that arguably involved even less evidence of probable cause than is presented here. *See id.* at 540, 543 (citing *United States v. Gourde*, 440 F.3d 1065 (9th Cir. 2006) (en banc); *United States v. Martin*, 426 F.3d 68 (2d Cir. 2005); and *United States v. Froman*, 355 F.3d 882 (5th Cir. 2004)). All of the cited cases involved defendants who subscribed to websites that were advertised as child pornography sites but contained both legal and illegal material, and in which the government's affidavit supporting a search warrant never stated whether the individuals had actually downloaded any of the *illicit* materials. Nevertheless, the courts universally found that the probable cause threshold had been satisfied because the defendants had purchased *access* to child pornography. In this case, although there was no evidence that Terry belonged to such a website, there was evidence that Terry had actually *possessed* (as opposed to merely having had access to) child pornography. While any IP or other information that could have more specifically tied Terry's home computer to the e-mail messages would certainly have been welcome, we are satisfied that the use of Terry's personal e-mail account in the wee hours of the morning, combined with information that Terry used his home computer to access that account, established at least a "fair probability" that the computer used to send the messages was, in fact, the one in Terry's home. Ergo, there was at least a fair probability that the illicit image (or similar images) would be found there.[2]

We are somewhat troubled by the fact that the *content* of the incriminating e-mail messages was apparently not preserved.[3] It is thus impossible to know the context in which the image was sent; Terry argues that he may have merely been replying to some unsolicited child pornography spam to request that no further such images be sent to him. Although this is theoretically possible,[4] it is not enough for Terry simply to speculate about hypothetical "false-positive" scenarios. He presented no evidence at the suppression hearing about the actual occurrence of such "spam-

---

[2]We do not believe that the passage of five months between the sending of the intercepted e-mail messages and the execution of the warrant changes the probable cause calculus much, if at all. Images typically persist in some form on a computer hard drive even after the images have been deleted and, as ICE stated in its affidavit, such evidence can often be recovered by forensic examiners. *See United States v. Lacy*, 119 F.3d 742, 746 (9th Cir. 1997) (holding that the nature of the crime "provided good reason to believe the computerized visual depictions downloaded by Lacy would be present in his apartment when the search was conducted ten months later") (internal quotation omitted).

[3]The record does not reveal whether this failure was the fault of AOL, the NCMEC, or ICE.

[4]Whether an image that is received via an e-mail message is also included in an outgoing reply would depend on various factors, including the e-mail client settings, whether the image was included within the body of the incoming message or as an attachment, the operation of any filtering software, etc.

rejection" transmission of child porn, either in his case or in society generally. Since a probable cause finding does not require a preponderance of the evidence, in order to undermine the magistrate's finding, the likelihood of an innocent explanation must (at the very least) be *greater* than the likelihood of a guilty one. For example, this court has indicated that—given studies demonstrating that a sizable percentage of United States currency in circulation is tainted with a detectable level of cocaine residue—a canine alert to currency, standing alone, will likely not establish probable cause in a forfeiture action. *United States v. $5,000.00 in U.S. Currency*, 40 F.3d 846, 849-50 (6th Cir. 1994).[5] In the context of automobiles, however, the rate of false positives is significantly lower, and an alert from a trained, reliable canine will alone establish probable cause to search the vehicle. *United States v. Diaz*, 25 F.3d 392, 393-94, 396 (6th Cir. 1994). Although we recognize that the government ultimately has the burden of demonstrating probable cause, absent *any* evidence that innocent persons frequently receive and reply to unsolicited child pornography spam (and in a way that would produce the computer traces in this case), this court cannot say that the magistrate judge arbitrarily exercised his discretion in issuing a search warrant for Terry's home.

III

For the foregoing reasons, we AFFIRM the judgment of the district court.

[5]More recent case law has called this assumption into question. *See United States v. Funds in Amount of Thirty Thousand Six Hundred Seventy Dollars*, 403 F.3d 448, 459 (7th Cir. 2005) (skeptically approaching the "currency contamination theory" and citing newer research indicating that "it is likely that trained cocaine detection dogs will alert to currency only if it has been exposed to large amounts of illicit cocaine within the very recent past").