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

File Name: 06a0209p.06

UNITED STATES COURT OF APPEALS

FOR THE SIXTH CIRCUIT

UNITED STATES OF AMERICA,
Plaintiff-Appellee,

v.

LYMAN WAGERS,
Defendant-Appellant.

No. 05-5296

Appeal from the United States District Court
for the Eastern District of Kentucky at Lexington.
No. 04-00066—Karl S. Forester, District Judge.

Argued: January 24, 2006

Decided and Filed: June 27, 2006

Before: BOGGS, Chief Judge; BATCHELDER, Circuit Judge; and WEBER, District Judge.*

COUNSEL

ARGUED: H. Louis Sirkin, SIRKIN, PINALES & SCHWARTZ, Cincinnati, Ohio, for Appellant. John Patrick Grant, ASSISTANT UNITED STATES ATTORNEY, Lexington, Kentucky, for Appellee. **ON BRIEF:** H. Louis Sirkin, Jennifer M. Kinsley, SIRKIN, PINALES & SCHWARTZ, Cincinnati, Ohio, for Appellant. John Patrick Grant, ASSISTANT UNITED STATES ATTORNEY, Lexington, Kentucky, for Appellee.

OPINION

BOGGS, Chief Judge. Lyman Wagers pleaded guilty to receiving and possessing child pornography. On February 11, 2005 he was sentenced to 180 months in prison. The sentence conformed to the 15-year mandatory minimum for second offenders under 18 U.S.C. § 2252(b)(1). Arguing that the three search warrants leading to evidence incriminating him were not supported by probable cause, he appeals the trial court's denial of his motion to suppress evidence seized pursuant to the warrants. *See United States v. Wagers*, 339 F. Supp. 2d 934, 940 & n.1 (E.D. Ky. 2004). We affirm.

*The Honorable Herman J. Weber, United States District Judge for the Southern District of Ohio, sitting by designation.

I

This is Wagers's second conviction on child pornography charges. He was convicted in 1997 of one count of possession of child pornography and sentenced in the United States District Court for the Eastern District of Kentucky to 366 days in prison, plus three years of supervised release. In the case now before us, Wagers, a 57-year-old erstwhile lawyer and C.P.A., pleaded guilty to one count of conspiracy to receive child pornography, nineteen counts of receiving child pornography, and one count of possession of child pornography. The terms of his guilty plea allowed him to appeal the conviction on the grounds that the search warrants used in the investigation were not supported by probable cause.

A Homeland Security sting operation led to Wagers's arrest. From March to August 2003, federal agents purchased subscriptions to and visited websites available at redlagoon.com, video2000.com, and darkfeeling.com. While visiting these sites, the agents found images of child pornography. They obtained records from the billing services of these sites. These records revealed that Wagers had purchased subscriptions to redlagoon.com on June 30, 2002; to video2000.com on March 22, 2003 and again on June 3, 2003; and to darkfeeling.com on April 15, 2003. Though the lengths of Wagers's subscriptions are not clear from the record, based on the prices he paid for his subscriptions, as compared to the prices the agents paid for one-month subscriptions, it appears that each of Wagers's subscriptions was for between one and two months of membership. This inference has been offered by Wagers and is not contested by the government. The agents who examined the websites did so by purchasing one-month subscriptions on March 26, 2003, August 1, 2003, and July 21, 2003, respectively.

On April 5, 2004, federal agents executed a search warrant at the home of Lyman Wagers ("Mimosa Lane" or "home"). After finding child pornography on Wagers's home computer, agents swore out another affidavit for his office. On April 7, 2004, agents obtained a separate warrant for his office ("Harrodsburg Rd." or "office"). The same day, he was arrested for possession of child pornography. The following day, agents obtained a third search warrant, directed to America Online, the company supporting Wagers's email account ("AOL" or "email"). Wagers's guilty plea and conviction are based on images found on his home computer, at least some of which, he concedes, were transmitted via his American Online account.

The home and office affidavits were both more than thirty pages long and quite detailed. The AOL affidavit is seven pages and less detailed, but it states that agents had connected Wagers's AOL email address to his home address and to the purchase of subscription memberships to all of the websites containing offending material. It further states that the affiant's "experience and training" lead him to believe that Wagers uses his AOL account to "order, arrange for the payment of, and arrange for the receipt of child pornography . . . ." *Id*. at 162. The warrants and their supporting affidavits alleged that Wagers had bought subscriptions to websites that were found at a later date to display child pornography. They did not specifically allege that Wagers had viewed the sites or that he had accessed unlawful content on them.

A federal grand jury indicted Wagers on May 6, 2004. He moved to suppress the evidence seized at his home and office. The district court denied the motion without a hearing. Wagers pleaded guilty to all counts, conditioning the plea on his right to appeal the ruling on the motion to suppress.

The district court sentenced Wagers to 180 months in prison on February 11, 2005. The guidelines range was 97 to 121 months, but the sentence conformed to the 15-year mandatory minimum for second offenders required by 18 U.S.C. § 2252(b)(1).

Wagers timely appealed his conviction, challenging the district court's denial of his motion to suppress.

II

This court reviews a district court's factual findings supporting its denial of a motion to suppress for clear error. It reviews *de novo* the district court's determination as to the reasonableness of the search as a question of law. *United States v. Carpenter*, 360 F.3d 591, 594 (6th Cir. 2004) (en banc); *United States v. Harris*, 255 F.3d 288, 291-92 (6th Cir. 2001). The "appellate court must consider the evidence in the light most favorable to the government" when reviewing a denial of a motion to suppress. *United States v. Herndon*, 393 F.3d 665, 667 (6th Cir. 2005) (quoting *United States v. Erwin*, 155 F.3d 818, 822 (6th Cir. 1998) (en banc)). "Probable cause exists where there is a fair probability, given the totality of the circumstances, that contraband or evidence of a crime will be found in a particular place." *United States v. Helton*, 314 F.3d 812, 819 (6th Cir. 2003) (quoting *United States v. Davidson*, 936 F.2d 856, 859 (6th Cir. 1991)).

III

Wagers's first major argument is that the affidavits were not supported by probable cause for three reasons:

1) the affidavits supporting the search warrants did not allege that he had owned website memberships at a time when illegal images were mounted on the sites or that he had accessed the sites during the times when illegal images were available;

2) the affidavits do not adequately connect the illicit activity to his home, office, or AOL account; and

3) the affidavit for the home warrant improperly relied on the fact of Wagers's prior conviction.

In this section, we address each component of this argument in turn. In section IV of this opinion we address the second major argument of Wagers's appeal.

Wagers notes that the agents' subscriptions post-dated the expiration of all but possibly one of his own subscriptions. He argues that the affidavits supporting the search warrants merely infer that there were unlawful images on those sites at the time of his earlier subscriptions.

To assess how much of an inference was made in issuing the search warrants, it is useful to observe that roughly five months elapsed between the end of Wagers's subscription to redlagoon.com and the commencement of the agents' subscription. Approximately one month passed before their subscriptions to darkfeeling.com. And it is possible that only a few days elapsed between the end of Wagers's second subscription to video2000.com and the government's. Indeed, if Wagers's subscription was for two months (which, according to his own brief's uncontested calculation of "between one and two months," is possible), there would be a short overlap between the end of his second subscription and the government's subscription. Whether or not there was an actual overlap between subscriptions, an inference based on the difference of a few days–in the case of video2000.com–or of roughly 30 days–in the case of darkfeeling.com–is not very hard to make, even setting aside the perhaps more tenuous inference based on research on redlagoon.com that was five months after Wagers's known use.

Wagers claims in his brief (Appellant's Brief, 12) that these three websites contained both legal and illegal images. The government claims this assertion is false. (Appellee's Brief, 12) Wagers does not offer clear support for his statement in the record. Neither, for that matter, does

the United States. The government points only to two printouts in the Joint Appendix submitted to this court, of the homepages of darkfeeling.com and redlagoon.com, both of which announce that *all* models featured on the sites are "14 or younger." (JA 195-96) These homepage reproductions are highly suggestive but not conclusive. Advertisers have been known to mislead before. Wagers rebuts, moreover, that the affidavits never state that the sites offer exclusively illegal content. Appellant's Reply Brief, 7. Neither party's view is definitive. But the district court was correct in concluding that this question is not dispositive. Probable cause to search for illicit pornography in Wagers's home, office, and email account existed even without a statement that these three websites contained only illegal images. *See* 339 F. Supp. 2d at 940 & n.1 The district court's conclusion is especially strong in light of the temporal analysis: based on the proximity in time between their subscriptions and his, the agents were justified in averring the essential similarity of the websites at the time Wagers had subscribed to them to the sites as they appeared during the sting operation's subscriptions.

Wagers argues that the affidavits do not connect the alleged crime to the places searched. For a search warrant to be valid, the place to be searched must be connected to the crime alleged. *E.g.*, *United States v. Laughton*, 409 F.3d 744 (6th Cir. 2005). Wagers does not dispute that he lived at 3813 Mimosa Lane, for which the first warrant issued. However, he does contend that "there is nothing in the affidavit connecting the residence to the alleged child pornography offenses." Appellant's Brief, 14. He offers two feeble pieces of support for this argument. First, he notes that he did not get Internet access at this residence until October 9, 2002, months after his subscription to redlagoon.com expired. However, his subscriptions to the other two websites post-date this Internet access.

Second, he notes that his subscriptions to video2000.com and darkfeeling.com were made on a checking card with a billing address of 1608 Harrodsburg Rd. in Lexington. Therefore, he argues, his subscriptions were connected only to his business office, not to his home, even though his home was the subject of the first warrant. However, the affidavit sworn by Homeland Security Special Agent Sean Lichner in support of the April 5, 2005 search warrant of the Mimosa Lane home notes specifically that the investigation into the subscription records of the three websites revealed that a subscriber's email address "Spike20004U@aol.com" was connected to 1608 Harrodsburg Rd. and 3813 Mimosa Lane, both in Lexington, Kentucky. The affidavit also avers that two credit card numbers and a phone number associated with the Mimosa Lane address were obtained from the websites' billing service provider, and that these data were soon connected to the name Lyman Wagers.

In addition, the affidavit avers that the investigation revealed that Wagers used Insight Communications as his home Internet service.[1] *Id*. at 99. It further avers that an IP address assigned by Insight to Wagers was used to purchase both memberships at video2000.com and the membership at darkfeeling.com. *Ibid*. Because this IP address was assigned by Insight, and because it appears from the wording of the affidavit that Wagers used Insight at his home but not his office, his home would be well within the ambit of a properly issued search warrant. Even if the home were only one of two locations–home and office–served by Insight, there would be sufficient evidence to support probable cause. Given the specificity of the investigation's results and the content of the affidavit, the warrant was valid.

Wagers cites *United States v. Savoca*, 761 F.2d 292, 297 (6th Cir. 1983), for the proposition that the "existence of probable cause to believe a suspect is guilty of a crime does not create probable cause to search that individual's residence without independent evidence establishing a

[1]The affidavit notes that Wagers uses Insight as the Internet provider for his home. It also notes that Insight had his office address for billing purposes. However, it appears from the wording of the affidavit that Wagers did not use Insight at his office, but only at his home.

nexus between the place and the crime." Appellant's Brief, 15. *Savoca* did not involve a home, but a motel room, a location subject to a lesser expectation of privacy. Second, and more importantly, we criticized the affidavit in that case as "only tenuously connect[ing] the place to be searched with two persons for whom arrest warrants were outstanding," for "fail[ing] to describe the relationship of the persons to the premises," and because it "did not state, for example, whether the location to be searched was a permanent residence, a transient lodging, or a third party's residence which the two named persons were merely visiting." The affidavit stated only that "both suspects 'were seen' in the motel room on two occasions." *Id*. at 297 and n.8. The affidavit in our case is much more specific.

It is true that, in *United States v. Helton*, 314 F. 3d 812, 821 (6th Cir. 2003), this court held that, even where police investigations revealed that a defendant was closely connected to possession of narcotics, a search warrant for his home was invalid without any evidence linking that residence to the drug trade. However, that case is easily distinguished. First, part of the affidavit was based on an anonymous tipster, which the court reasonably found to have been insufficiently reliable to form the basis of probable cause. *Id*. at 821-22. Second, part of the affidavit was based on a confidential informant's allegation, much of which pointed to a home other than the defendant's. *Id*. at 821. No such affirmative evidence, pointing to places other than Wagers's home or business, appears here. Third, the remainder of the affidavit was based on the placing of three phone calls per month from the defendant's home telephone to the number of a known drug trafficker. The evidence in our case connecting the defendant, his computer, his IP address, and his home to the offense is considerably stronger, particularly where the criminal activity (viewing child pornography) is much more tied to a place of privacy, seclusion, and high-speed Internet connectivity (e.g. a home or office) than the storing of drugs (which can take place in a car, a ditch, a hole in the ground, etc.).

Our opinion today is consistent with the views of our sister circuits. The Second and Fifth Circuits, for example, have noted that evidence that a person has visited or subscribed to websites containing child pornography supports the conclusion that he has likely downloaded, kept, and otherwise possessed the material. *United States v. Martin*, 418 F.3d 148, 157 (2d Cir. 2005); *United States v. Froman*, 355 F.3d 882, 890-91 (5th Cir. 2004).

As to the third warrant in his case, the one served on AOL, Wagers notes that the affidavit sworn in support of this warrant observes mostly that he subscribed to and visited websites. The only reference to email in the affidavit is the affiant's stated "belie[f] that Wagers uses the spike20004U@aol.com email account to order, arrange for the payment of, and arrange for the receipt of child pornography." (JA 162, quoted at Appellant's Brief, 17) Wagers also used an IP address furnished by AOL to sign up for at least one of his subscriptions. An offender without relatively sophisticated knowledge of transmittal or downloading technology might reasonably be expected to use email to send and receive pornographic images or at least web links to them. Probable cause does require a sufficient nexus between the location to be searched and the evidence sought. *United States v. McLevain*, 310 F.3d 434, 439 (6th Cir. 2002). This court, in *United States v. Schultz*, 14 F.3d 1093 (6th Cir. 1994), declined to find such a nexus–and held that the avowed training and experience of law enforcement-affiants failed to subsitute for it–where police suspected a defendant of drug offenses and therefore sought to search his safety deposit box. However, the nexus between an AOL email account and Internet-accessed child pornography, especially where some of that access has been through AOL IP addresses, is much more obvious than the connection between drug trafficking and safety deposit boxes.

Wagers's final argument on the warrant's sufficiency is that the affidavit for the home warrant "relies heavily upon the fact that Wagers had a previous child pornography conviction." (Appellant's Brief, 15) Though the affidavit supporting that warrant does take note of his prior offense over less than two full pages, the document is 32 pages long, plus four pages of attachments, and the discussion of his prior offense is not the preponderant support for the application for the

warrant. Implying that a prior conviction cannot properly raise an inference of later criminal activity, even for an identical or nearly identical offense, Wagers argues that an "individual's criminal history . . . is not the appropriate focus for a search warrant affidavit." Appellant's Brief, 16. Wagers's only citation of law for this proposition is *Mays v. City of Dayton*, 134 F.3d 809, 814 (6th Cir. 1998), stating that "[s]earch warrants are directed not at persons, but at specific locations where there is probable cause to believe the instrumentalities or evidence of crimes will be found." This case does not help Wagers's larger implied argument here, to the effect that search warrants based in part on prior convictions are presumptively invalid. The test for probable cause, as the Supreme Court affirmed very recently in *United States v. Grubbs*, 126 S. Ct. 1494 (2006), is whether "'there is a fair probability that contraband or evidence of a crime will be found in a particular place.'" *Grubbs* at 1499 (quoting *Illinois v. Gates*, 462 U.S. 213, 238 (1983)). The application of this test is not fettered by the presumption of innocence embodied in the test for conviction. Instead, a "person of reasonable caution" would take into account predelictions revealed by past crimes or convictions as part of the inquiry into probable cause. *See, e.g.*, *United States v. Blanton*, 520 F.2d 907, 912 (6th Cir. 1975) (finding probable cause to search defendant's car where the arresting officer was reliably informed that the car trunk contained a machine gun and money, where the officer knew that the defendant had extensive use of the car, and where the officer personally knew the defendant well enough to know of his "past criminal record"). Wagers's prior conviction for possession of child pornography followed the seizure of illegal images on both his home and his office computers. When, in our case, the Homeland Security agents uncovered evidence of Wagers's connection to the websites carrying child pornography, his prior conviction was relevant, though not dispositive. Given the requirements of seclusion and a high-speed Internet connection, a home and office search warrant is supported by probable cause under these circumstances. For this reason, and for the several reasons already adduced *supra*, the district court did not abuse its discretion in denying a motion to suppress evidence gathered pursuant to a search warrant for Wagers's home and office.

IV

Wagers's secondary point is that the Internet is an "ever-changing global method of communication" that "heighten[s]" the "importance of the probable cause requirement." (Appellant's Brief, 8) Some websites contain both lawful images and unlawful images. He argues that the Internet presents too many opportunities for search warrants to be issued where innocent activity and criminal activity may be easily confused or accidentally mixed (*e.g.*, by visiting websites containing legal and illegal images). His argument here seems to be that the Internet is a new and different entity, and that such an entity should be analyzed cautiously by law enforcement and courts. A lurking point, though Wagers never states it explicitly (most likely because he was caught red-handed with at least six hundred graphic and disturbing images of children having–or being forced to have–sex), is that the Internet may present too many opportunities for a search warrant to be issued where innocent activity (viewing lawful pornography) and criminal activity (viewing unlawful pornography) may be easily confused or accidentally mixed, as by visiting websites that may contain lawful and unlawful pornography. His contention implies rejection of the common law's capacity to handle significant innovation and novelty.[2]

The tools available to us are adequate to the task of helping us understand the risks posed to Fourth Amendment rights by the type of law enforcement we see in the appeal before us. As it applies to the facts of Wagers's case, the Internet does not present a murky new innovation without adequate analogs in the pre-"wired" world. In essence, Wagers's Internet argument is just a

[2]This capacity has, at times, been considered perfect. *See* Joseph H. Beale, *A Treatise on the Conflict of Laws* § 3.2, 4.12 (1935) (describing the common law as a seamless web of interlocking principles which, properly applied, can fully accommodate intelligent analysis of a case arising from commerce with any technological invention, including, illustratively, the streetcars of mid-nineteenth century Boston, which Chief Justice Lemuel Shaw deftly analyzed using existing common law analysis in *Commonwealth v. Temple*, 80 Mass. (14 Gray) 69, 74 (1859)).

variation of the "simply in the wrong place at the wrong time" refrain. This type of argument is not infrequently put forward in other contexts, for example by persons attacking search warrants based, in part, on their presence in a shady part of town, near the scene of a murder, or any number of locales or factors that could also have an innocent explanation. Indeed, it is a commonplace part of judging attacks on convictions as well as warrants (with their lower standard of proof), that the law can properly judge evidence that could be consistent with innocence as well as guilt, and that our system can make a valid determination as to which obtains in a particular fact pattern. It is well established in this court that "the probable cause requirement does not require that every contrary hypothesis be excluded." *United States v. Alfano*, 838 F.2d 158, 162 (6th Cir. 1988). No new standard of evidence is necessary for dealing with cases involving the Internet. All that is required is a consistent application of our existing approaches to possibly ambiguous evidence.

To press his argument that the Internet poses novel risks to constitutional law enforcement, Wagers relies heavily on the Ninth Circuit's recent decision in *United States v. Gourde*, 382 F.3d 1003 (9th Cir. 2004). In that case, the defendant was arrested following the execution of a search warrant based on an affidavit that alleged that he subscribed to a website that contained both lawful and child pornography but silent on the question whether he had actually used the site and/or accessed its content. *Id*. at 1007. The Ninth Circuit panel invalidated the search warrant as supported by insufficient information to furnish probable cause. The court demanded particularized information that the defendant had viewed illegal images. *Id*. at 1013.

His reliance on *Gourde* is flawed for three compelling reasons. First, Gourde appears to have had no prior convictions for child pornography. Wagers does. Following questioning pursuant to his 1997 arrest, the FBI learned that Wagers had transmitted "many more than [four]" images via his AOL "internet connection" (though it is unclear whether this transmittal refers to "email" or just his means of "surfing") in the years preceding that arrest.[3] Second, the affidavit supporting the search warrant in *Gourde* expressly noted that the website visited in that case, Lolitgurls.com, featured images of "adult pornography, child pornography, and child erotica." (Affidavit of David J. Moriguchi, filed January 29, 2003, page 3) The affidavits supporting the search warrants in our case note only that the websites visited by Wagers featured illegal images. They are silent on whether these sites also included legal pornography. Third, the *Gourde* ruling was substantially overturned en banc. *United States v. Gourde*, 440 F.3d 1065 (9th Cir. 2006) (en banc). The en banc court held that probable cause did exist in the case.

V

Because the district court properly denied Wagers's motion to suppress evidence, we **AFFIRM** his conviction.

[3]For precision and completeness, it bears noting that the defendant admitted to having "transmitted many more than that number," where "that number" equaled "four."