

NOT RECOMMENDED FOR FULL-TEXT PUBLICATION

File Name: 19a0491n.06

Case No. 18-6082

**UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT**

FILED
Sep 24, 2019
DEBORAH S. HUNT, Clerk

UNITED STATES OF AMERICA,)
)
Plaintiff-Appellee,)
)
v.)
)
MARCUS WILLIAMS,)
)
Defendant-Appellant.)

ON APPEAL FROM THE
UNITED STATES DISTRICT
COURT FOR THE WESTERN
DISTRICT OF TENNESSEE

OPINION

BEFORE: MOORE, McKEAGUE, and GRIFFIN, Circuit Judges.

McKEAGUE, Circuit Judge. Marcus Williams traded child pornography online. When federal agents found out, they applied for a search warrant for his home and car. The search yielded a laptop and cell phones full of child pornography. After the government charged Williams with possessing and distributing child pornography, Williams moved to suppress all evidence from the search because the information used to obtain the search warrant was allegedly stale. The district court denied the motion, and a jury convicted Williams on all charges. Williams appeals, arguing both that the district court erred in denying his suppression motion and that the evidence was insufficient to support the jury’s verdict. We disagree and **AFFIRM**.

I.

During an October 2015 child exploitation investigation, federal agents in Virginia discovered that someone with the username “marcus williams trueone12345” was trading child

pornography over Kik (a mobile instant message application) with another user. Kik produced the internet protocol address associated with the username in early 2016 in response to an administrative subpoena. With Comcast's help, federal agents then tied that online address to a home address in Memphis, Tennessee belonging to Williams's uncle. All this information was passed on to Memphis-based Special Agent Aaron Thompson, along with data from the "marcus williams trueone12345" Kik account. The account data included child pornography and October 2015 messages discussing the exchange of child pornography through the email address "marcus.williams41@yahoo.com."

So Thompson investigated Williams. In June 2016, Thompson staked out the uncle's house. He saw Williams park his car there and go inside. Then in July, Thompson received data from the Yahoo email account pursuant to a search warrant. This account data confirmed two things: one, whoever was using the "marcus.williams41" email address was trading child pornography; and two, that person was, as late as July 5, 2016, logging in from Williams's uncle's home and directing "clients" to contact him through Kik or another email address. Thompson double-checked that Williams was still parking his car there in August and late September—he was—then applied for a search warrant on September 29, 2016. Thompson recounted everything from the October 2015 Virginia investigation onward in his affidavit, and stated that based on his experience he expected to find a potentially years-long archive of child pornography on a personal computer or cell phone in the home or Williams's car.

And that's exactly what Thompson found when he searched the home on October 5, 2016 after a magistrate judge approved the warrant—a laptop storing over 3,000 pornographic videos of children. Williams's three cell phones also had videos. When Thompson confronted Williams, Williams confirmed that the Yahoo and Kik accounts were his and that he had been living with his

uncle for a year. But Williams maintained that he was not responsible for the child pornography on his accounts and devices.

On March 8, 2017, the government charged Williams with two counts of distributing child pornography over the internet, 18 U.S.C. § 2252(a)(2), and one count of possession of child pornography, 18 U.S.C. § 2252(a)(4)(B). (The first distribution charge related to a February 26, 2016 email Williams sent containing child pornography; the second, a similar October 3, 2016 email.) Williams moved to suppress the evidence obtained from the search on the ground that Thompson relied on “stale” information in his affidavit. According to Williams, the search warrant lacked probable cause because Thompson could not “connect the dots” between online messages sent in October 2015, an internet protocol address discovered five months later, and the September 29, 2016 search warrant application. The district court denied the motion, reasoning that the affidavit was not stale when considering the character of the crime, the nature of the criminal, the items to be seized, and the places to be searched. Williams proceeded to trial, where the government called Thompson and two other agents to testify; Williams chose not to present a defense. The jury convicted Williams on all three counts, and the district court sentenced him to 188 months’ imprisonment. Williams timely appeals, challenging the district court’s denial of his suppression motion and the sufficiency of the evidence used to convict him.

II.

First, the suppression motion. We use a mixed standard when reviewing a district court’s denial of a motion to suppress. We review its factual findings for clear error and its legal findings de novo. *United States v. Gross*, 662 F.3d 393, 398 (6th Cir. 2011). And we take the evidence “in the light most favorable to the government” where, as here, it’s the defendant’s motion the district

court denied. *United States v. Carter*, 378 F.3d 584, 587 (6th Cir. 2004) (en banc) (quotation omitted).

Whether Thompson’s affidavit provided probable cause for the issuance of a search warrant is a legal question. *United States v. Frazier*, 423 F.3d 526, 531 (6th Cir. 2005). In answering that question, we consider only the information Thompson provided the issuing magistrate. *United States v. Pinson*, 321 F.3d 558, 565 (6th Cir. 2003). Still, we pay “great deference” to a magistrate’s judgment, which “should not be set aside unless arbitrarily exercised.” *United States v. Leake*, 998 F.2d 1359, 1363 (6th Cir. 1993) (quotation omitted). If the magistrate had a “substantial basis for . . . conclud[ing]’ that a search would uncover evidence of wrongdoing,” *Illinois v. Gates*, 462 U.S. 213, 236 (1983) (quotation omitted), we must uphold the search warrant. *Leake*, 998 F.2d at 1363.

Williams argues that Thompson’s information was too old to support the magistrate judge’s probable cause determination. Outdated or “stale” information, by itself, cannot establish probable cause. See *United States v. Spikes*, 158 F.3d 913, 923 (6th Cir. 1998). But just because information is old doesn’t mean it’s stale—each case is different, and the circumstances of the case control rather than temporal lines in the sand. See *Sgro v. United States*, 287 U.S. 206, 210–11 (1932); *United States v. Burney*, 778 F.3d 536, 540 (6th Cir. 2015). Whether information is stale depends on “the character of the crime (chance encounter in the night or regenerating conspiracy?), the criminal (nomadic or entrenched?), the thing to be seized (perishable and easily transferable or of enduring utility to its holder?), [and] the place to be searched (mere criminal forum of convenience or secure operational base?),” among other things. *Spikes*, 158 F.3d at 923 (quotation omitted). “[E]ven if a significant period has elapsed since a defendant’s last reported criminal activity, it is

still possible that, depending upon the nature of the crime, a magistrate may properly infer that evidence of wrongdoing is still to be found on the premises.” *Id.*

Williams’s main contention is that Thompson applied for a search warrant more than seven months after agents discovered his Kik and Yahoo accounts, meaning Thompson impermissibly “sat on” the connection between those accounts and his uncle’s home for about six months. We rejected a similar contention in *United States v. Frechette*, 583 F.3d 374 (6th Cir. 2009). In that case, a sixteen-month-old online subscription to a child pornography website provided the basis for a search warrant for the defendant’s home. *Id.* at 377–78. Although information that old is “usually” too stale for a drug case, we held that it is fresh enough for a child pornography case. *Id.* at 379. That’s because all four *Spikes* factors point toward freshness in a typical child pornography case: “child pornography is not a fleeting crime” but rather “carried out in the secrecy of the home and over a long period” (the first, second, and fourth factors); and “images of child pornography can have an infinite life span” when traded digitally (the third factor). *Id.* at 378–79.

This case is far easier than *Frechette*. Thompson’s affidavit established—through Williams’s eponymous accounts, an internet protocol address, and stakeouts—that Williams was operating out of his uncle’s home from October 2015 to September 2016. And the affidavit listed the pornographic videos of children that Williams sent and received from October 2015 to at least May 2016, providing incriminating filenames and descriptions. In other words, Williams, having “entrenched” himself in a “secure operational base,” traded illegal videos of unlimited life span over the course of several months. The magistrate judge thus had a substantial basis for concluding that a search of the uncle’s home and Williams’s car would yield evidence of wrongdoing despite the six-month delay between Williams’s messages and the search warrant application. *See United States v. Hampton*, 504 F. App’x 402, 404 (6th Cir. 2012) (per curiam) (ten-month delay in

obtaining a search warrant did not render an affidavit stale in a child pornography case); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010) (more than seven-month delay); *United States v. Lapsins*, 570 F.3d 758, 767 (6th Cir. 2009) (nine-month delay); *United States v. Paull*, 551 F.3d 516, 522–23 (6th Cir. 2009) (thirteen-month delay).

Williams also argues he “abandoned” his email account four months before the search warrant application or was not otherwise responsible for it. But we must view the evidence in the government’s favor. *See Carter*, 378 F.3d at 587. The affidavit indicates that as late as July 2016, Williams was still accessing his Yahoo account and directing “clients” to his other accounts. Email forwarding is not abandonment. Even if it were, the magistrate judge still had a substantial basis for concluding Williams’s devices contained child pornography because digital media can be stored indefinitely, let alone for four months. *Cf. Frechette*, 583 F.3d at 376–79 (defendant’s child pornography subscription that lapsed after one month provided probable cause for a search warrant issued over a year later).

So there was nothing stale about Thompson’s affidavit, and the magistrate judge appropriately found probable cause existed for the issuance of a search warrant. We accordingly affirm the district court’s denial of Williams’s motion to suppress.

III.

That leaves Williams’s challenge to the jury’s verdict. When reviewing the jury’s verdict, “the relevant question is whether, after viewing the evidence in the light most favorable to the prosecution, *any* rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt.” *Jackson v. Virginia*, 443 U.S. 307, 319 (1979). “We draw all available inferences and resolve all issues of credibility in favor of the jury’s verdict, and it is not necessary

for us to exclude every reasonable hypothesis but guilt.” *United States v. Avery*, 128 F.3d 966, 971 (6th Cir. 1997).

The evidence was sufficient to convict Williams on his distribution and possession charges. Thompson testified that Williams admitted the Yahoo and Kik accounts were his. Child pornography was sent and received through those accounts. Williams’s laptop and cell phones were brimming with child pornography. That’s plenty. *See, e.g., United States v. Oufnac*, 449 F. App’x 472, 475–78 (6th Cir. 2011); *United States v. Mellies*, 329 F. App’x 592, 607 (6th Cir. 2009).

Williams suggests the government had to both show his accounts and laptop weren’t “attacked” or accessed by others and explain why the pornographic videos of children on his laptop were sloppily organized. Not so. With his admissions and the number of videos found on his personal devices, the evidence of Williams’s guilt was overwhelming even if others could have accessed those devices. *See Oufnac*, 440 F. App’x at 476–77. Nor does knowing possession and distribution require a defendant to fastidiously archive his child pornography collection. “Knowingly” means with “knowledge of the facts that constitute the offense,” *Bryan v. United States*, 524 U.S. 184, 193 (1998), not “expertly.”

There was sufficient evidence for the jury to convict Williams, so we affirm the judgment.

IV.

For these reasons, we **AFFIRM** the denial of Williams’s motion to suppress and the judgment entered against him.