NOT RECOMMENDED FOR FULL-TEXT PUBLICATION
File Name: 19a0529n.06

No. 18-6333

UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

FILED
Oct 16, 2019
DEBORAH S. HUNT, Clerk

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff-Appellee,	)	
	)	
v.	)	ON APPEAL FROM THE
	)	UNITED STATES DISTRICT
KENDALL R. CARTER,	)	COURT FOR THE MIDDLE
	)	DISTRICT OF TENNESSEE
Defendant-Appellant.	)	

Before: SUTTON, KETHLEDGE, and STRANCH, Circuit Judges.

KETHLEDGE, Circuit Judge. Kendall Carter appeals the district court's denial of his motion for a *Franks* hearing and his motion to suppress evidence of child pornography and interstate extortion. We reject his arguments and affirm.

During the summer of 2014, Carter—then a 20 year-old living in his parents' basement in Milton, Tennessee—befriended a handful of 13 to 16 year-old girls on an instant messaging app called Kik. After he had done so, Carter used multiple online personas to coerce the girls into sending him nude photos. Then Carter threatened to post the photos online unless the girls sent him even more sexually explicit images.

In October 2014, one of the girls, a 13 year-old in North Dakota, reported that someone was sexually exploiting her on Kik. Investigators looked at her chat logs and found two usernames in chat sessions where she had been coerced into sending sexually explicit photos and videos. They sent Kik an administrative subpoena for information about those usernames and about two

chat sessions that took place on September 14, 2014. Kik's reply showed that the usernames had been created several months earlier and had been active on an iPhone and iPad. Kik did not have IP addresses—which are numerical labels that can identify a user's physical location in a computer network—dating back to September 14. (The company retained IP information for just 30 days.) But Kik had that information for hundreds of more recent sessions, when both usernames accessed Kik from the same IP address in Milton, Tennessee. That IP address, a local internet-service provider confirmed, was associated with a residential address in Milton and with a specific subscriber named Kendall Carter.

The investigators in North Dakota handed the case off to Detective Patty Higgins, a sheriff's deputy with the Rutherford County (Tennessee) Sheriff's Office. Higgins applied for a search warrant and signed an affidavit that stated, among other things, that investigators had linked the Kik usernames in the September 14 chat sessions to an IP address, and linked the IP address to Carter. The warrant itself sought evidence of sexual exploitation of minors, including an iPhone and an iPad "used to facilitate the aforementioned criminal activity[.]" R. 46-1 at Page ID 404.

Higgins and another officer went to Carter's house, where Carter's father invited them in. After a short conversation with Carter's parents, the officers said they needed to see the iPhone and iPad that belonged to the Carters' son Kendall. The Carters asked to see a warrant, so the officers showed it to them. Kendall Carter then gave the officers his iPhone, iPad, and passwords to both devices.

Investigators later searched Carter's iPhone and iPad, where they found hundreds of images of child pornography. They also found Kik chat sessions in which Carter had coerced multiple girls into sending him sexually explicit images and videos.

Federal prosecutors charged Carter with a total of 15 counts of production and attempted production of child pornography, *see* 18 U.S.C. § 2251(a), possession of child pornography, *see id.* § 2252A(a)(5)(B), and use of interstate communications to commit extortion, *see id.* § 875(d). Carter later moved for a *Franks* hearing concerning what he alleged were false statements in Higgins's affidavit. He also moved to suppress the evidence seized during the search of his house. The district court denied both motions.

Carter thereafter conditionally pleaded guilty to two counts of production of child pornography, two counts of extortion, and one count of possession of child pornography, preserving the right to appeal the denial of his motion to suppress. Before his sentencing hearing, however, Carter filed another motion to suppress, alleging that the investigators' use of an administrative subpoena to collect his IP address violated the Fourth Amendment as interpreted in *Carpenter v. United States*, 138 S. Ct. 2206 (2018). The district court again denied the motion, and sentenced Carter to 30 years in prison.

Carter now appeals the district court's denial of his motion for a *Franks* hearing and his motions to suppress. For these denials, we review legal questions de novo and factual findings for clear error. *United States v. Poulsen*, 655 F.3d 492, 503 (6th Cir. 2011).

To obtain a *Franks* hearing, a defendant must make a substantial preliminary showing of two things: first, that the affidavit includes a false statement that was made "knowingly and intentionally, or with reckless disregard for the truth"; second, that the allegedly false statement is "necessary to the finding of probable cause." *See United States v. Mastromatteo*, 538 F.3d 535, 545 (6th Cir. 2008). In the context of child pornography, an affidavit that connects a defendant, an offending username, and the defendant's residence is enough to establish probable cause for a search. *See United States v. Elbe*, 774 F.3d 885, 890 (6th Cir. 2014). Carter says that Higgins's

affidavit falsely linked the September 14 chat sessions with his IP address, because Kik in fact did not have IP information for those sessions. The rest of the affidavit, however, shows that someone used two usernames to coerce a child to send sexually explicit images, and that those usernames accessed Kik from an IP address associated with Carter's residence. That connection—between Carter, his residence, and the offending usernames—is enough to show that there was a "fair probability" that evidence of a crime would be found at Carter's house. *See id*. at 888. The affidavit's allegedly false statement was therefore immaterial to the issue of probable cause. Hence the district court properly denied Carter's motion for a *Franks* hearing. *See Mastromatteo*, 538 F.3d at 545.

The same is true as to the motions to suppress. Carter argues that the search warrant itself was invalid in several respects. First, he contends that the warrant left the officers free to take any iPhones and iPads they wanted, which he says violates the Fourth Amendment requirement that a warrant describe "with particularity" the things law enforcement may seize. *United States v. Willoughby*, 742 F.3d 229, 233 (6th Cir. 2014). But a warrant that constrains a search to evidence of a specific crime satisfies the particularity requirement. *United States v. Castro*, 881 F.3d 961, 965 (6th Cir. 2018). And here the warrant restricted the search to an iPhone and an iPad "used to facilitate the aforementioned criminal activity[.]" R. 46-1 at Page ID 404. Rather than leaving the officers without direction, the warrant told them enough to "guide and control [their] judgment in selecting what to take[.]" *Willoughby*, 742 F.3d at 233.

Second, Carter says that the warrant was overbroad, because it might have allowed officers to seize "clearly innocuous" items. But the remedy for an overbroad warrant is to suppress the evidence taken specifically under the overbroad search term. *United States v. Richards*, 659 F.3d 527, 537 (6th Cir. 2011). Carter points to none here, so his argument fails.

Third, Carter contends that the warrant was invalid because, he says, Tennessee law required Higgins to obtain a district attorney's approval before she applied for it. But the Tennessee Supreme Court has since held otherwise. *See State v. Miller*, 575 S.W.3d 807, 813 (Tenn. 2019). Nor do we suppress evidence based on violations of state law. *See United States v. Beals*, 698 F.3d 248, 263 (6th Cir. 2012). Hence Carter's contention fails.

Carter also argues that the search was improperly executed for several reasons. First, he says that officers violated the "knock-and-announce" rule. *See* 18 U.S.C. § 3109. But that rule applies only when officers enter by force; here, they were invited in. *Id.* Second, he says the officers violated the Fourth Amendment because they did not show the search warrant until asked. But here nothing required the officers to present the warrant any sooner than they did. *See Baranski v. Fifteen Unknown Agents of the Bureau of Alcohol, Tobacco & Firearms*, 452 F.3d 433, 442–43 (6th Cir. 2006) (en banc). Third, Carter says that his federal prosecution effectively precluded him from challenging the search on state-law grounds. But he has not identified any aspect of the search that violated state (or federal) law.

Finally, Carter argues that the investigators violated the Fourth Amendment when they obtained his IP address by an administrative subpoena rather than by a search warrant after a showing of probable cause. His argument relies upon the Supreme Court's decision in *United States v. Carpenter*, 138 S. Ct. 2206 (2018), which concerned cell-site locational data, not IP addresses. But we have no need to consider whether to extend *Carpenter*'s holding to IP addresses here. For our court has already held that the good-faith exception to the exclusionary rule applies to searches that complied with the Stored Communications Act and then-binding case law. *See United States v. Carpenter*, 926 F.3d 313, 318 (6th Cir. 2019).

The district court's judgment is affirmed.