In the

United States Court of Appeals

For the Seventh Circuit

No. 19-2230

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

MICHAEL REES,

Defendant-Appellant.

Appeal from the United States District Court for the
Central District of Illinois.
No. 18-cr-10033 — **Michael M. Mihm**, *Judge*.

ARGUED FEBRUARY 12, 2020 — DECIDED APRIL 30, 2020

Before BAUER, KANNE, and BARRETT, *Circuit Judges*.

KANNE, *Circuit Judge*. An investigation into online sharing of child pornography led law-enforcement officers to Michael Rees's residences and vehicle, where they executed search warrants and found child pornography. Charged with federal crimes, Rees moved to suppress the evidence found in the searches. A district court denied his motion, and Rees then pled guilty to the charges but reserved his right to appeal the suppression decision. Appealing that decision, Rees argues

that the evidence was inadmissible because the warrants were invalid and the officers could not reasonably rely on them to conduct the searches.

We affirm for two reasons. First, the warrant-issuing judge had a substantial basis for concluding that there was a fair probability evidence of child-pornography crimes would be uncovered in the searches. And second, even if the warrants were invalid, the officers executed them in objective good faith.

I. BACKGROUND

In 2017 and 2018, FBI Child Exploitation Task Force Officer William Lynn was investigating the sharing of child pornography through online, peer-to-peer networks. Over the course of six months, his investigation led him to believe child pornography would be found in the college apartment, house, and pickup truck of 40-year-old Michael Rees.

Seeking warrants to search these places, Officer Lynn gave a magistrate a seventeen-page probable-cause affidavit, which described the officer's training and experience, law-enforcement methods for tracking child pornography on peer-to-peer networks, and the specific investigation that steered him toward Rees's residences and vehicle.

Based on Officer Lynn's affidavit alone, the magistrate issued the requested warrants. When officers executed them, they found thousands of still images and almost 200 videos of child pornography on Rees's computer. A grand jury charged Rees with four counts of receiving, and one count of possessing, child pornography, 18 U.S.C. § 2252A(a)(2)(A), (5)(B).

Initially pleading not guilty, Rees moved to suppress the evidence found in the searches. He argued that the warrants

were invalid for want of probable cause and the officers could not rely on them in good faith. Unconvinced after a hearing, the district court denied Rees's motion. Rees then pled guilty to all five charges while reserving his right to appeal the suppression decision. The district court accepted Rees's guilty plea, entered a judgment of conviction, and sentenced Rees to 97 months' imprisonment—a sentence Rees does not contest.

On appeal, Rees maintains that the warrants were unsupported by probable cause and could not be relied upon in good faith.

II. ANALYSIS

Rees's appeal challenges only the admissibility of evidence obtained from warrant-authorized searches. Our review of warrant-authorized searches involves a complex standard. *See United States v. McIntire*, 516 F.3d 576, 578 (7th Cir. 2008).[1] But it is simplified in this case because the district court did not make credibility determinations or findings of historical fact based on evidence received during the

[1] The precise standard, which we articulated in *McIntire*, is the following:

> A district court's findings of historical fact are reviewed for clear error, whether or not a warrant issued. *Ornelas v. United States*, 517 U.S. 690, 699 (1996). A district judge's legal conclusions are reviewed without deference. And on the mixed question whether the facts add up to "probable cause" under the right legal standard, we give no weight to the district judge's decision—for the right inquiry is whether the judge who issued the warrant (rarely the same as the judge who ruled on the motion to suppress) acted on the basis of probable cause. On *that* issue we must afford "great deference" to the issuing judge's conclusion.

McIntire, 516 F.3d at 578.

suppression hearing. *See id.*; *United States v. Koerth*, 312 F.3d 862, 865 (7th Cir. 2002). Indeed, the district court confirmed at the suppression hearing that it would be receiving no evidence, only argument. As a result, we face just two questions, each involving a single standard.

The first question is, did the warrant-issuing judge act on the basis of probable cause? *See United States v. Aleshire*, 787 F.3d 1178, 1178–79 (7th Cir. 2015). On this question, we uphold the magistrate's finding of probable cause so long as that judge "had a 'substantial basis for … conclud[ing]' that a search would uncover evidence of wrongdoing." *Illinois v. Gates*, 462 U.S. 213, 236 (1983) (alteration in original) (quoting *Jones v. United States*, 362 U.S. 257, 271 (1960)).

The second question is, if the warrants were invalid, was the evidence obtained from the searches nevertheless admissible because the officers relied on the warrants in objective good faith? *See United States v. Leon*, 468 U.S. 897, 922 (1984). On this question, our review is *de novo*—again, because the district court drew only a legal conclusion, without finding facts or determining credibility. *See United States v. Mitten*, 592 F.3d 767, 770–71 (7th Cir. 2010).

A. Probable Cause

The Fourth Amendment guarantees that "no Warrants shall issue, but upon probable cause." U.S. Const. amend. IV. Rees contends that the warrants here were not issued upon a proper probable-cause decision, for three reasons: first, when ruling on the motion to suppress, the district court inappropriately relied on a demonstrative aid that supplied new inculpatory information; second, Officer Lynn's affidavit

exposed fatal gaps in his investigation; and third, key information in the affidavit was stale.

We first dispense with Rees's demonstrative-aid argument. During the suppression hearing, the government presented the district court with a two-and-one-third-page document condensing the information in Officer Lynn's seventeen-page affidavit. Rees argues that this "complex demonstrative aid" did not merely summarize the affidavit but added inculpatory information to it. He surmises that the district court relied on that new information when denying Rees's motion to suppress, and that without the additional information, the magistrate (the warrant-issuing judge) could not have based the warrants on a finding of probable cause.

This argument reaches outside the scope of our review. Our task is to determine whether the magistrate had a substantial basis to conclude that probable cause existed. To do this, we look only at the information the magistrate had. *See Rainsberger v. Benner*, 913 F.3d 640, 650 (7th Cir. 2019); *United States v. Harris*, 464 F.3d 733, 739 (7th Cir. 2006). The magistrate here had only Officer Lynn's affidavit. So, our review does not encompass the later-made demonstrative aid or the district court's alleged misuse of it.

We emphasize an important qualification: the demonstrative aid was not evidence of falsities in the affidavit. *Cf., e.g.*, *United States v. Roth*, 391 F.2d 507, 509 (7th Cir. 1967) (suppression hearing included testimony exposing a fatal flaw in the affidavit). This is germane because—while a district court may *not* consider new inculpatory information supporting a finding of probable cause—the court *may* (and at times must) consider new information attacking the veracity of the warrant affidavit or on issues outside whether probable cause

existed. *See Rainsberger*, 913 F.3d at 650 n.5; *Harris*, 464 F.3d at 738–39. But Rees does not contend that the district court received exculpatory evidence. He argues only that the demonstrative aid included inculpatory information outside the affidavit's four corners and that the added information should not have contributed to the district court's decision that the warrants were valid.

Whether the demonstrative aid included new inculpatory information, and whether the district court improperly relied on it when concluding the warrants were proper, are both beside the probable-cause inquiry we face today. Our review concerns only whether the affidavit, alone—the sole basis on which the magistrate issued the warrants—was enough for the magistrate to decide that probable cause existed. In other words, the affidavit's four corners bound our review. *See United States v. Bell*, 585 F.3d 1045, 1049 (7th Cir. 2009) ("When, as here, the affidavit is the only evidence provided to the judge in support of the search warrant, the validity of the warrant rests solely on the strength of the affidavit.").[2]

We turn now to the question at hand: whether the warrant-issuing judge had a substantial basis for its probable-cause determination. The magistrate's task was "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. Probable cause does

[2] To be clear, had the district court received evidence undermining the veracity of information in the affidavit, our review would involve another layer of analysis. *See McIntire*, 516 F.3d at 578. But that is not the situation before us.

not require a showing of criminal activity, as it rides on "the degree of suspicion that attaches to particular types of non-criminal acts." *Id.* at 243 n.13. It also depends on the totality of the circumstances—"the whole picture"—not each fact in isolation. *District of Columbia v. Wesby*, 138 S. Ct. 577, 588 (2018) (quoting *United States v. Cortez*, 449 U.S. 411, 417 (1981)).

Ultimately, the magistrate had to decide whether Officer Lynn's affidavit provided enough information to warrant a prudent person to believe that criminal conduct has occurred and that evidence of it would be found in Rees's residences and truck. *See Gates*, 462 U.S. at 238; *Whitlock v. Brown*, 596 F.3d 406, 411 (7th Cir. 2010). Rees argues that gaps and staleness in Officer Lynn's affidavit required a negative answer. We disagree. To explain why, we will recapitulate portions of Officer Lynn's affidavit, though we will not provide the same depth and detail. We will then address Rees's arguments.

1. Officer Lynn's Affidavit

Officer Lynn first gave background information about peer-to-peer file-sharing networks and his law-enforcement experience with them. He recounted some of his and other officers' knowledge about how digital media, including child pornography, is often stored and distributed through personal computers. Notably, he explained that digital media can often be recovered from devices even after those devices have been in storage for months or even years; and—due to the nature of digital devices and the operating systems involved in peer-to-peer sharing—evidence of downloaded files can be recovered after a user deletes the files from a computer.

Getting more specific, Officer Lynn described two peer-to-peer networks that were integral to his investigation:

eDonkey and BitTorrent. The two networks are distinct and rely on different software, but both are used to share and download digital files.

Officer Lynn explained that the eMule software, which operates on the eDonkey network, tracks and gives credit to individual users for their sharing activity; and it does so by assigning each network user a unique identifier, or "user hash." That user hash allows officers to see which user is offering to share particular files.

BitTorrent works a bit differently. It enables users to share sets of files that may be stored across multiple computers. The sets of files are the "payload" of a "torrent file," which has a unique "infohash" identifier. This infohash works as a form of "digital fingerprinting," singularly identifying the torrent file and its corresponding payload. When a user wants to download a payload, the user connects his or her device to computers that have the payload's pieces. The devices connect via the internet and "ports," which range in number from zero to 65,535. Whereas ordinary internet browsing typically occurs on low-numbered ports, like port 80, BitTorrent sharing typically occurs on less-common, high-numbered ports, which decrease the likelihood that the sharing will interfere with the computers' other functions.

In addition to describing these networks, Officer Lynn devoted a section of his affidavit to how officers use a law-enforcement database to track peer-to-peer network activity involving child pornography. He explained that officers log on to peer-to-peer networks, and when they find files containing child pornography, the officers record—in the database—various information about the transfer of those files. That information includes the IP addresses of computers involved in the

transfer, the date and time the files were shared, the file names and infohashes, and identifying information about the users engaged in the transaction. Multiple law-enforcement agencies use this common database to record, store, and share investigative information about peer-to-peer dissemination of child pornography.

Officer Lynn also noted that another resource, a law-enforcement reference library, stores child-pornography files for use in child-pornography investigations. By matching the infohash of a shared torrent file to the infohash of a file or set of files in the library, Officer Lynn understood that the shared torrent payload and the corresponding files in the library have the same content.

Against this technical background, Officer Lynn charted the investigation that homed in on Rees's residences and truck.

In October 2017, Officer Lynn logged on to the BitTorrent network and connected his computer to a "suspect" device. He began investigating this particular device because it was associated with a BitTorrent file that had a payload containing child pornography or child erotica. In a series of connections, Officer Lynn's computer—which was running investigative software—reported that the suspect device had all pieces of a payload for another torrent file. That torrent file's infohash matched one in the law-enforcement reference library, which informed Officer Lynn that the payload included 32 images of a child engaging in sexually explicit conduct.

Officer Lynn recorded the suspect device's IP address and learned through an administrative subpoena that the address was assigned to a 32-unit apartment complex near Illinois

State University. To differentiate between individual apartment units' internet activity going forward, officers installed a tracking system on the complex's internal network, which assigned a different internal IP address to each apartment unit.

Next, Officer Lynn drew upon investigatory information recorded in the law-enforcement database. He noticed that, before the internal-network tracker was installed at the apartment complex, an officer had logged eDonkey activity taking place at the complex's IP address. The same user hash for that activity had also been logged in the database for eDonkey activity at another IP address, which was assigned to Michael Rees for a single-family home in Pekin, Illinois. Rees's driver's license likewise listed the Pekin address as his residence. The eDonkey activity logged for Rees's home IP address took place during the university's mid-year break, on January 8, 2018. Rees's home IP address was also logged in the law-enforcement database for BitTorrent activity on the same day, January 8.

Officer Lynn soon learned that Rees had leased one of the 32 apartments near the university for the 2017–18 academic year. As a result, the officers narrowed their internal-network tracking to monitor internet usage of only Apartment 8, the apartment Rees had leased with three other residents.

During the spring semester, in March 2018, Officer Lynn observed a recent database entry for BitTorrent activity at the apartment complex's IP address. The database indicated that the activity occurred through port 22,863. The internal-network tracker showed that the same numbered port was used at the same time by someone at Apartment 8.

Finally, state records revealed that Rees had a white pickup truck, which, Officer Lynn explained, was seen parked near both Rees's apartment and his Pekin home.

Officer Lynn submitted that, based on the information he retailed in the affidavit, probable cause existed to believe that evidence of crimes concerning child pornography would be found in Rees's apartment, house, and truck.

2. Gaps and Staleness

Rees points to a number of holes in the investigation described in Officer Lynn's affidavit. He also argues that Officer Lynn's findings grew stale before the search warrants issued.

Specifically, Rees points out that anyone at the apartment complex could have downloaded the October 2017 payload that Officer Lynn's computer reported was located on the suspect device. He adds that Officer Lynn did not actually open the files downloaded in October 2017; the officer instead compared the payload's infohash to that of files in a reference library. Rees also asserts that the affidavit did not clarify that the law-enforcement database includes only information about files that officers have recognized contain child pornography. He reasons that Officer Lynn first described a "peer-to-peer database" and then referred to the "ICAC Cops database" when charting his investigation; the affidavit did not explicitly state that the two terms refer to the same database—the one Officer Lynn described as storing information on the sharing of child pornography. Rees additionally reminds us that child erotica, which may have prompted Officer Lynn's initial inquest into the suspect device's activities, is not contraband. He continues that Officer Lynn did not personally view the files shared in the peer-to-peer activity that officers

tied to Rees's apartment and house, specifically. And he lastly urges that the criminal activity Officer Lynn observed in October was stale by the time he applied for the affidavits six months later.

These are strong reasons why Officer Lynn had not proven, in the affidavit, that Rees received and possessed child pornography in his apartment, house, and truck. But probable cause is a low bar that can be cleared without a *prima facie* showing of criminal activity. *See Gates*, 462 U.S. at 235, 243 n.13. Again, what matters is the degree of suspicion that arises from particular types of noncriminal acts, taken altogether. *Id.* at 243 n.13.

Here, the affidavit did not establish an airtight case against Rees. But it supplied plenty of information for a prudent person to believe child pornography would be found in Rees's homes and truck. Although Officer Lynn's investigation began with a suspicion that a certain device was associated with child pornography or child erotica (which is not contraband), the next step in his investigation gave strong indication that the suspect device contained images of child pornography, not just child erotica. By connecting his computer to the suspect device in October, and by comparing the infohash of the files downloaded by the suspect device to the infohash of child-pornography files in the reference library, Officer Lynn had good reason to believe the suspect device's user had downloaded child pornography.

Next, Officer Lynn located the suspect device at the 32-unit apartment complex. He did this by tracking down the geographic location of the IP address that the suspect device used to download the contraband files. Further funneling the investigation to more precisely locate the device, Officer Lynn

saw that the law-enforcement database indicated the same eDonkey user had engaged in child-pornography sharing both at the apartment complex and at Rees's house, where (the law-enforcement database informed him) BitTorrent activity concerning child pornography also took place. Officer Lynn later learned that Rees resided at both locations.

Finally, suspicion mounted around Apartment 8 when Officer Lynn learned, based on database entries, that someone at the complex had shared child pornography using port 22,863. And the internal-network tracker showed that, at the same time, someone was using the same uncommon, high-numbered port via the internal IP address of Apartment 8: Rees's apartment. Finally, Rees's truck was seen at both residences.

Despite the imperfections Rees identifies, all the information in the affidavit is enough for a reasonable person to believe that evidence of child-pornography crimes would be found in Rees's apartment, house, and truck.

Rees's argument about staleness does not change this conclusion. He argues that the affidavit's information about the October 2017 downloads was stale by the time Officer Lynn sought the warrants in late March 2018. Because that key information was stale, he says, the affidavit did not support a finding of probable cause. We disagree for two reasons.

First, the information about the October 2017 downloads was supported by more recent peer-to-peer activity logged in the law-enforcement database, which suggested that the same kind of criminal activity continued into March 2018. *See United States v. Pless*, 982 F.2d 1118, 1126 (7th Cir. 1992) ("Passage of time is less critical when the affidavit refers to facts

that indicate ongoing continuous criminal activity."). Officer Lynn indicated—when describing the law-enforcement database—that officers used the database to "log information regarding child pornography trading on the peer-to-peer network." He explained that the information recorded in the database stemmed from the sharing of files identified by law-enforcement officers as "child pornography file[s]," which meant that the database provided "a historical record of computers that have offered the child pornography file for download." So, the later logged entries of peer-to-peer activity connected to Rees's home and apartment could reinforce a belief that the originally detected criminal activity was ongoing.

Second, even if more recent information did not refresh Officer Lynn's initial observations of criminal conduct, that information from October 2017 did not go stale over six months. We have not identified a precise expiration time for an affidavit's information. That's because probable cause is a "fluid concept," *Gates*, 462 U.S. at 232, and the recency of information given to the issuing judge is just one factor in the totality-of-the-circumstances probable-cause inquiry, *United States v. Carroll*, 750 F.3d 700, 703 (7th Cir. 2014). But we have recognized that evidence contained in computer equipment does not rapidly dissipate or degrade, that child-pornography collections tend to be kept for long periods of time, and that digital information is often retrievable from hard drives even after a user "deletes" it. *See id.* at 704–05; *United States v. Seiver*, 692 F.3d 774, 776 (7th Cir. 2012). So, information regarding digital child-pornography files may stave off staleness for years. *See, e.g.*, *Carroll*, 750 F.3d at 706 (five years); *United States v. Newsom*, 402 F.3d 780, 783 (7th Cir. 2005) (one year); *see also Carroll*, 750 F.3d at 704–05 (listing cases from other circuits).

Officer Lynn confirmed that the devices and operating systems involved in peer-to-peer sharing allow officers to recover information about network activity even after a user deletes specific files or has kept a device in storage for months or years. He also revealed how peer-to-peer networks allow users to access the same or similar child-pornography files without keeping them on their own computers: the users can relocate files on the network and download them again and again. In this way, peer-to-peer networks may, in some cases, extend the time before which certain evidence of child-pornography crimes goes stale—because the evidence may be stored across a greater number of electronic devices. *See Seiver*, 692 F.3d at 778 (stressing that inquiries into staleness and child-pornography collectors must be grounded "in a realistic understanding of modern computer technology and the usual behavior of its users").

Of course, at some point "after a *very* long time" the likelihood that certain digital information will be recoverable from a specific device "drops to a level at which probable cause to search the suspect's home for the computer can no longer be established." *Id.* at 777. But Rees has not shown that this is an "exceptional case," *id.* at 778, in which a delay between the electronic transfer of an image and Officer Lynn's requests to search for evidence of child-pornography crimes "destroy[ed] probable cause to believe that a search of the computer will turn up the evidence sought," *id.* at 777. Accordingly, staleness did not prevent the magistrate from appropriately finding probable cause.

All-in-all, the affidavit supplied a substantial basis for the magistrate to conclude that the requested searches had a fair probability of uncovering evidence of child-pornography

crimes. This is enough to affirm the district court's denial of Rees's motion to suppress. But there is another reason Rees is not entitled to relief.

B. Good Faith

Even if the search warrants lacked a basis in probable cause, the exclusionary rule does not operate against the evidence if the good-faith exception applies—that is, if the officers who executed the warrants relied, in objective good faith, on the magistrate's probable-cause decision. *See Leon*, 468 U.S. at 922–24.

Officer Lynn's choice to obtain the warrants in the first place invokes a presumption that he acted in good faith. *See United States v. Lickers*, 928 F.3d 609, 618 (7th Cir. 2019). To overcome this presumption, Rees must show the existence of a situation in which the good-faith exception does not apply, *see id.*; *United States v. Glover*, 755 F.3d 811, 818–19 (7th Cir. 2014); four such situations are well established: (1) the affiant misled the magistrate with information the affiant knew was false or would have known was false but for the affiant's reckless disregard for the truth; (2) the magistrate wholly abandoned the judicial role and instead acted as an adjunct law-enforcement officer; (3) the affidavit was bare boned, "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable"; and (4) the warrant was so facially deficient in particularizing its scope that the officers could not reasonably presume it was valid, *Leon*, 468 U.S. at 923 (quoting *Brown v. Illinois*, 422 U.S. 590, 611 (1975) (Powell, J., concurring in part)).

Rees does not argue that the warrants lacked adequate particularity, rendering them facially deficient. Instead, he

argues some conglomerate of the other three. Hard-pressed to say the detailed, seventeen-page affidavit was bare boned, Rees contends that Officer Lynn omitted clarifying information, which left the magistrate confused and misled into believing probable cause existed. Echoing his arguments for why probable cause was lacking, he says that the affidavit failed to highlight the fact that Officer Lynn neither opened the files downloaded in October 2017 nor confirmed that the peer-to-peer activity recorded thereafter involved child pornography.

Although this information could have been clearer, Officer Lynn supplied it to the magistrate. And, for reasons we've already explained, this information did not prevent the magistrate from properly finding probable cause. Even if it did, though, the indicia of probable cause were not so lacking that official belief in its existence was unreasonable. And Rees has not shown that the alleged failure to spotlight certain information resulted from reckless disregard for the truth.[3] So, Rees has not overcome the presumption of good faith with his first arguments.

Finally, resuscitating his focus on the demonstrative aid, Rees says the affidavit was too technical and confusing for the magistrate to have functioned as anything but a rubber stamp for law enforcement. After all, he reasons, the district court

[3] Rees has neither argued nor established that he is entitled to a *Franks* hearing, which requires a "substantial preliminary showing" that (1) the affidavit had a material falsity or omission that would alter the probable-cause determination, and (2) the falsity or omission was made "knowingly and intentionally, or with reckless disregard for the truth." *Franks v. Delaware*, 438 U.S. 154, 155–56 (1978); *see Glover*, 755 F.3d at 820.

relied on the government's demonstrative aid to navigate the affidavit's content.

Even if the district court used the demonstrative aid—something we do not decide—that alone would not establish that the magistrate was unable to understand Officer Lynn's affidavit and carry out his judicial role. The affidavit provided detailed, comprehensible descriptions of both the relevant technology and the investigative steps officers took. So, Rees has not shown that the affidavit was so befuddling that the magistrate must have abandoned his neutral, detached role.

III. CONCLUSION

Because the magistrate had a substantial basis for concluding probable cause existed to search Rees's residences and truck, and because the officers executing the searches could rely on the warrants in objective good faith, we AFFIRM the denial of Rees's motion to suppress.