United States Court of Appeals
For the Eighth Circuit

No. 18-3150

United States of America

Plaintiff - Appellee

v.

Alden Dickerman

Defendant - Appellant

Appeal from United States District Court
for the Eastern District of Missouri - St. Louis

Submitted: September 24, 2019
Filed: March 30, 2020

Before KELLY, MELLOY, and STRAS, Circuit Judges.

KELLY, Circuit Judge.

Alden Dickerman pleaded guilty to possession of child pornography after law enforcement executed a warrant at his home and found child pornography on his computer. Dickerman entered a plea agreement, reserving his right to appeal the district court's[1] denial of his motion to suppress. Because we agree with the district court that the good-faith exception to the exclusionary rule applies, we affirm.

I.

The government alleged Dickerman used "Freenet," a decentralized, privacy-focused, peer-to-peer file sharing system, to access child pornography. Freenet is free to use and publicly available to anyone willing to dedicate a portion of their computer's hard drive to the network. Unlike other file sharing systems, Freenet does not give a user immediate access to intact files for downloading. Rather, to allow for anonymous retrieval of files from the network, Freenet breaks down each uploaded file into "blocks." These blocks, or portions of a file, are then distributed over numerous computers that are running Freenet (computers running Freenet are sometimes called "nodes"). No single node stores all of the blocks for a single file, and all blocks are encrypted—meaning that a user whose computer passively stores blocks does not know what the blocks contain.

Someone seeking a particular file on Freenet can use a publicly available "key" to retrieve the file. This "requester" uses the key to ask other Freenet nodes for the blocks he or she needs to make up the desired file. No user is connected to all of the nodes on Freenet. Rather, users are connected to just a subset of all Freenet nodes, called the user's "peers." Thus, a requester sends the blocks request to only his or her peers. When a peer receives the request, the peer's computer provides any of the requested blocks in its possession and then passes, or "relays," the request to *its own* peers on behalf of the original requester. A peer that relays a request is called a "relayer."

[1] The Honorable Henry E. Autrey, United States District Judge for the Eastern District of Missouri, adopting the report and recommendations of the Honorable Nannette A. Baker, Chief Magistrate Judge for the Eastern District of Missouri.

As a result of this decentralized configuration, a computer running Freenet can receive two types of requests: (1) requests from the original requester—the user who located the key and is seeking to obtain all of the blocks for the desired file; and (2) requests from a relayer—another computer on Freenet that simply relays an original request for blocks on to its peers. For purposes of this case, there is an important difference between a requester and a relayer. Requesters know what file they are requesting; relayers do not know what blocks have been requested from their computers or what file those blocks are part of. Relayers do not even know whether their computers have relayed an original request for blocks to their peers.

A key feature of Freenet is that requesters and relayers are indistinguishable to an ordinary user of the network. A user who receives a request does not know whether it came from an original requester or a relayer. Law enforcement, however, can determine which Freenet users request which files by using a statistical algorithm developed and validated by Dr. Brian Levine, an expert in networks and security at the University of Massachusetts Amherst. The algorithm allows law enforcement to distinguish between requests sent from an original requester and requests forwarded by a relayer.

In this case, officers used Dr. Levine's algorithm to determine that a computer associated with Dickerman's Internet Protocol (IP) address had requested child pornography files through Freenet. St. Louis County Detective Michael Slaughter drafted a search warrant application and supporting affidavit to present to a state court judge. In his affidavit, Slaughter wrote that the information was based on his "personal knowledge or information provided by other law enforcement officers." Slaughter outlined his professional background, including that he "received specialized training in the area of computer-based investigations." He identified Special Investigator Wayne Becker as an officer who provided relevant information. He listed Becker's qualifications and experience in "forensic analysis of computers used in criminal activity, including the use of peer-to-peer (P2P) and file sharing networks."

Slaughter described Freenet's basic functionality in his affidavit. He wrote that "someone requesting blocks of a file has taken substantial steps to install *Freenet* and locate" a publicly available key for the desired file. He explained that Freenet's ability "to hide what a user is requesting from the network has attracted persons that wish to collect and/or share child pornography files." Slaughter further averred that he "knows from training and experience that streams of requests for blocks of a particular file from an IP address can be evaluated to determine if the IP address is the likely requester of the file." But Slaughter did not include any details about Dr. Levine, his algorithm, or how officers use the algorithm to determine which Freenet users requested which files.

The affidavit also recounted the investigation into Dickerman's use of Freenet. Slaughter specified how Becker began an undercover operation to identify and collect keys and files shared on Freenet to build a database of keys associated with files that were known or suspected child pornography images. Becker then ran special copies of Freenet modified for law enforcement to track the IP address, key, and timing of requests sent to the law enforcement Freenet nodes. Becker compared this tracked information to the keys in the database he had created. During the investigation, Becker observed an IP address associated with Dickerman's computer "routing and/or requesting suspected child pornography file blocks." Specifically, between 11:08 and 11:10 pm on April 2, 2015, "a computer running Freenet software at IP address 172.12.235.62, requested from Freenet law enforcement nodes 69 parts, or blocks," of a child pornography file. Slaughter described the contents of the "17 jpg images" in the file. He concluded, "The number and timing of the requests was significant enough to indicate that the IP address was the apparent original requester of the file."

The state court judge signed the warrant after reviewing Slaughter's affidavit. Officers then searched Dickerman's home and seized his computer, where they located child pornography. Dickerman was charged in federal court with possession of child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B). He moved to suppress the seized evidence, arguing Slaughter's affidavit was insufficient to establish probable cause and that the issuing judge, by signing the warrant, acted as a "rubber stamp" for law enforcement.

The federal magistrate judge held an evidentiary hearing on the suppression motion, at which Dr. Levine, Slaughter, Becker, and the state court judge testified. The magistrate judge subsequently issued a thorough Report and Recommendation, recommending that Dickerman's motion be denied because Slaughter's affidavit contained sufficient information to establish probable cause. Alternatively, the magistrate judge reasoned, the officers who executed the search relied in good faith on the signed warrant such that the exception to the exclusionary rule applied under United States v. Leon, 468 U.S. 897 (1984).

The district court reviewed the Report and Recommendation, adopted its conclusions "in their entirety," and denied Dickerman's motion to suppress. Dickerman pleaded guilty but reserved his right to appeal the denial of his suppression motion. The district court sentenced him to 60 months in prison and supervised release for life, and ordered $5,500 in restitution. On appeal, Dickerman renews his arguments that the search warrant was issued without probable cause and that the state court judge acted as a "rubber stamp" by signing it.

II.

When reviewing the denial of a motion to suppress, we review the district court's factual findings for clear error and its legal conclusions de novo. United States v. Clay, 646 F.3d 1124, 1127 (8th Cir. 2011). We also review de novo the district court's application of the Leon good-faith exception to the exclusionary rule. Id. We may consider the applicability of the good-faith exception before reviewing the existence of probable cause. Id.

In Leon, the Supreme Court recognized "the exclusionary rule is designed to deter police misconduct rather than to punish the errors of judges and magistrates." Leon, 468 U.S. at 916. And, in "the ordinary case, an officer cannot be expected to question the magistrate's probable-cause determination." Id. at 921. The Court therefore held that the exclusionary rule "should not be applied so as to bar the admission of 'evidence obtained by officers acting in reasonable reliance on a search warrant,'" even if the warrant is later invalidated. Clay, 646 F.3d at 1127 (quoting Leon, 468 U.S. at 900).

"The good-faith inquiry is confined to the objectively ascertainable question [of] whether a reasonably well trained officer would have known that the search was illegal despite the issuing judge's authorization." Id. (cleaned up). "[W]hen assessing the officer's good faith reliance on a search warrant . . . , we can look outside the four corners of the affidavit and consider the totality of the circumstances, including what the officer knew but did not include in the affidavit." United States v. Farlee, 757 F.3d 810, 819 (8th Cir. 2014) (citing Anderson v. Creighton, 483 U.S. 635, 641 (1987)).

There are, however, four situations where Leon's good-faith exception cannot apply. An officer's reliance on a warrant would be unreasonable when:

> (1) the affidavit or testimony supporting the warrant contained a false statement made knowingly and intentionally or with reckless disregard for its truth, thus misleading the issuing judge;
>
> (2) the issuing judge wholly abandoned his judicial role in issuing the warrant;

(3) the affidavit supporting the warrant is so lacking in indicia of probable cause as to render official belief in its existence *entirely unreasonable*; and

(4) the warrant is so facially deficient that no police officer could reasonably presume the warrant to be valid.

United States v. Perry, 531 F.3d 662, 665 (8th Cir. 2008). This case requires us to consider the second and third Leon exceptions.

A.

Dickerman first argues the officers who searched his computer did not act in good-faith reliance on the warrant because Slaughter's affidavit lacked sufficient indicia of probable cause. Dickerman faults Slaughter's affidavit for not fully explaining how law enforcement identified Dickerman's computer as an "original requester" of child pornography rather than simply a passive "relayer" on the Freenet network. As previously noted, this distinction is meaningful because an original requester knows the contents of a sought-after file while a relayer does not. Because the affidavit lacked this explanation, Dickerman argues, it failed to show he had the requisite mens rea to commit the crime charged.

How law enforcement concluded that Dickerman was a requester of the file is important to a finding of probable cause. In his affidavit, Slaughter described generally how Freenet works, explaining the network "breaks a file into small pieces, or blocks," that are distributed across Freenet users' computers. "No one user has the entire intact file." To request a file, a user must obtain a key for the file's individual blocks. A computer running Freenet receives two types of requests from other computers: either "to retrieve from that node's data store, or to forward to another user that may have that part of the file." According to Slaughter, requests for blocks of a particular file "can be evaluated to determine if the IP address is the likely requester of the file."

The affidavit continued, "SI Becker observed IP address 172.12.235.62 routing and/or requesting suspected child pornography blocks." While Slaughter noted that Dickerman's IP address requested "69 parts, or blocks" of a child pornography file, Slaughter did not explain how that number was significant in determining whether Dickerman was an original requester or merely a relayer. Instead, Slaughter simply averred, "[t]he number and timing of the requests was significant enough to indicate that the IP address was the apparent original requester of the file."

Dickerman argues this is a "mere conclusion" that does nothing to establish probable cause. It is true that the affidavit fails to explain how the "number and timing of the requests" led law enforcement to believe Dickerman was the "original requester" of the file. No doubt, it would have been better for Slaughter to specify how officers used Dr. Levine's algorithm to reach this conclusion. Slaughter could have noted the validity and error rate of the algorithm and explained the significance of Dickerman's computer requesting a certain number of blocks of a known child pornography file.[2] As investigative techniques get more sophisticated, affiants should

[2] At the evidentiary hearing, Becker explained how the number and timing of requests enables law enforcement to distinguish between original requesters and passive relayers. He provided an example of a law enforcement computer connected to Freenet, a file composed of 1,000 blocks, and an original requester connected to ten peers on the network. To obtain the file, the requester sends out 1,000 requests roughly evenly distributed among the ten peers, one request for every block. If the law enforcement computer is one of the original requester's ten peers, it would receive approximately 100 requests from the original requester. By contrast, the law enforcement computer would receive only about ten requests from the original requester's other peers, assuming each peer was also connected to ten computers. That is because each of these peer computers are "relaying" to *their* peers a portion of the 100 requests they received from the original requester. And because 100 is significantly larger than ten, law enforcement can determine, with a certain level of accuracy, which computers are original requesters and which are simply relayers.

be mindful to explain their basis for probable cause in a way that is sufficiently comprehensive but still accessible to the judge reviewing the warrant application.

Despite any potential shortcomings in the affidavit, however, the officers' reliance on the warrant in this case was objectively reasonable. Slaughter did not make the conclusion that Dickerman was a requester in isolation: he supported it with other detailed facts about the officers' understanding of Freenet's functionality, their qualifications in computer forensics and experience investigating peer-to-peer networks, and Dickerman's Freenet use. Slaughter also supported his affidavit with information that Freenet "has attracted persons that wish to collect and/or share child pornography files," and that the network is "not a significant source of music, adult pornography, theatrical movies, or other copyright material." Given the numerous details Slaughter included in his affidavit about the investigation into Dickerman's use of Freenet, and about Freenet itself, we cannot say it was "so lacking in indicia of probable cause as to render official belief in its existence *entirely unreasonable*." See Perry, 531 F.3d at 665.

Moreover, as Dickerman acknowledges, the officers executing the search warrant knew more about the circumstances of the alleged offense than what Slaughter included in his affidavit. The officers were aware of additional information about Dr. Levine's algorithm, such as its validity and error rate, as well as the fact that child pornography had been discovered in each of Becker's similar Freenet investigations. Because we may consider "what the officer[s] knew but did not include in the affidavit" to decide whether their reliance on the warrant was objectively reasonable, see Farlee, 757 F.3d at 819, this additional information supports finding good faith, see Clay, 646 F.3d at 1127–28 (considering evidence "available to the officer, but not perhaps the judge," to decide the officer acted in good faith).[3]

B.

Dickerman next contends Leon does not apply because the judge abandoned his judicial role and acted as a "rubber stamp" for law enforcement by signing the search warrant.

The Leon good-faith exception "will not apply to admit evidence if the magistrate who issued the warrants abandoned his or her neutral and detached role in issuing it." Farlee, 757 F.3d at 819 (citing Leon, 468 U.S. at 914). A judge abandons her judicial role when she "does not serve as a neutral and detached actor, but rather as a rubber stamp for the police and an adjunct law enforcement officer." United States v. Ortiz-Cervantes, 868 F.3d 695, 703 (8th Cir. 2017) (cleaned up). For example, this Court has determined an issuing judge abandoned his judicial role by not reading the search warrant and failing to recognize that the application was unsigned and that the warrant did not identify the property to be searched. See United States v. Decker, 956 F.2d 773, 777 (8th Cir. 1992). In addition, the Supreme Court has found violations of the neutrality-and-detachment obligation where the judge possessed a pecuniary interest in issuing the warrant, Connally v. Georgia, 429 U.S.

[3] Another "relevant circumstance to consider when determining whether an officer's actions were objectively reasonable is whether the officer consulted with any attorney prior to seeking the warrant." Clay, 646 F.3d at 1127 (citing United States v. Johnson, 78 F.3d 1258, 1264 (8th Cir. 1996)). Here, Slaughter presented the warrant to a St. Louis County prosecutor before taking it to the state court judge. This strengthens our conclusion that the executing officers relied in good faith on the signed warrant. See id.

245, 251 (1977), and where the judge actively participated in the police investigation, Lo-Ji Sales, Inc. v. New York, 442 U.S. 319, 327–28 (1979).

Dickerman asserts the state court judge acted as a rubber stamp in two ways. First, he argues the judge approved the warrant application without "a sufficient basis to determine probable cause." This argument mirrors his argument that the affidavit "lacked sufficient indicia of probable cause." Yet "the exclusionary rule is designed to deter police misconduct rather than to punish the errors of judges and magistrates." Leon, 468 U.S. at 916. And our good-faith inquiry is focused on whether the officers executing the search warrant were "objectively reasonable" in relying on the judge's signed warrant. Id. at 919–20; see United States v. Scroggins, 361 F.3d 1075, 1083 (8th Cir. 2004). Dickerman's first rubber-stamp theory fails because he has not shown that a reasonably well-trained officer "would have known that the search was illegal despite the issuing judge's authorization." See Clay, 646 F.3d at 1127 (cleaned up); see also Leon, 468 U.S. at 921 ("In the ordinary case, an officer cannot be expected to question the magistrate's probable-cause determination . . . .").

Second, Dickerman argues the state court judge acted as a rubber stamp by signing the warrant without fully understanding Slaughter's affidavit. This argument does not neatly fit within the existing framework for analyzing rubber-stamp claims under Leon. Dickerman does not suggest the judge had a pecuniary interest in issuing the warrant or actively participated in the police investigation. Cf. Lo-Ji Sales, 442 U.S. at 327–28; Connally, 429 U.S. at 251. Nor does Dickerman suggest the judge failed to read the search warrant. Cf. Decker, 956 F.2d at 777. Indeed, as the district court found, the state court judge read Slaughter's entire affidavit and had previously considered 15 to 20 applications for search warrants involving peer-to-peer software before signing the warrant in this case.

Instead, Dickerman focuses his second rubber-stamp argument on the state court judge's testimony at the evidentiary hearing. There, the judge testified that he did not understand how Freenet block requests can be evaluated to determine who is an original requester and who is a relayer, and that some of the technical details in the affidavit were "Greek" to him. Compounding this problem, according to Dickerman, the judge did not request any clarification from law enforcement before signing the warrant.

To decide whether the officers relied in good faith on a search warrant, we confine our inquiry "to the objectively ascertainable question [of] whether a reasonably well trained officer would have known that the search was illegal despite the issuing judge's authorization." Clay, 646 F.3d at 1127 (cleaned up). By primarily relying on the state court judge's post-hoc testimony to argue he did not fully understand the affidavit's contents, Dickerman has not demonstrated that the officers "would have known" of this problem or were objectively unreasonable in their reliance on the signed warrant. See id.

Dickerman suggests the officers should have known the judge acted as a rubber stamp because he failed to ask any questions before signing the warrant. This Court has acknowledged that a judge's silence "might tend to show that he was acting as a mere 'rubber stamp' instead of actively making an independent probable cause determination." United States v. Hallam, 407 F.3d 942, 946 (8th Cir. 2006). Yet we rejected the defendant's rubber-stamp argument in Hallam because, while "the magistrate had no questions and made no statements about the search warrant or affidavit," there was "no indication that the magistrate was biased" nor "any evidence of a pattern of passive, automatic issuance of warrants." Id.

Here, viewing the totality of the circumstances from the officers' perspective, they had no indication that the state court judge had failed to understand the affidavit or otherwise acted as a rubber stamp. See Clay, 646 F.3d at 1127. The judge reviewed the entire affidavit before signing the warrant. Slaughter testified that the judge said nothing to make him “concerned that he didn’t understand the material he was reading.” In addition, Missouri law prohibits state court judges from considering oral testimony when deciding whether to sign a search warrant. See Mo. Rev. Stat. § 542.276, subd. 3 (2010). Slaughter therefore reasonably understood the judge’s lack of questioning to signify that the judge understood his affidavit. Because the officers had no evidence that the judge abandoned his judicial role, they acted in good-faith reliance on the warrant’s validity. See Hallam, 407 F.3d at 946.

Accordingly, the district court properly denied Dickerman’s motion to suppress based on the Leon good-faith exception. In light of this conclusion, we need not reach the underlying question of probable cause. See Clay, 646 F.3d at 1128.

We affirm the judgment of the district court.