5-17-2022

USA v. Nathan Weyerman

NOT PRECEDENTIAL

UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

_____

No. 21-1896

_____

UNITED STATES OF AMERICA

v.

NATHAN STEWART WEYERMAN,
Appellant

_____

On Appeal from the United States District Court
for the Eastern District of Pennsylvania
(D.C. No. 2-19-cr-00088-001)
District Judge: Honorable Paul S. Diamond

_____

Submitted Pursuant to Third Circuit L.A.R. 34.1(a)
May 5, 2022

_____

Before: CHAGARES, Chief Judge, GREENAWAY, JR., and PORTER, Circuit Judges.

(Filed: May 17, 2022)

_____

OPINION*

_____

* This disposition is not an opinion of the full Court and pursuant to I.O.P. 5.7 does not constitute binding precedent.

CHAGARES, Chief Judge.

This appeal arises from the District Court's denial of defendant Nathan Weyerman's motion to suppress evidence seized based on a search warrant. Weyerman argues that the search warrant affidavit omitted material facts about the reliability of an algorithm used to establish probable cause. For the following reasons, we will affirm the judgment of the District Court.

I.

We write primarily for the parties and recite only the facts essential to our decision. On September 12, 2018, the Federal Bureau of Investigation ("FBI") applied for a warrant to search two addresses in Philadelphia for evidence of illegal distribution, transportation, receipt, and possession of child pornography. The affidavit accompanying the application, which was written by Special Agent Rebecca A. Quinn, described the basis for probable cause.

As set forth in the affidavit, the FBI's investigation centered on "Freenet," an "Internet-based, peer-to-peer . . . network that allows users to anonymously share files." Appendix ("App.") 71. Once Freenet software is downloaded, a computer running Freenet "connects directly to other computers running Freenet, which are called its 'peers.'" App. 72. Each person who downloads Freenet agrees to provide the entire network with a portion of storage space on the individual user's hard drive so that all users can upload and share files across the network. When a user uploads a file (for example, an image or video) onto Freenet, the software "breaks the file into pieces . . . and encrypts each piece." App. 72. Those encrypted pieces are "distributed randomly

and stored throughout the Freenet network of peers." App. 72. The Freenet software then creates an index that lists all the individual pieces that make up a file and contains a unique "key" that is used to download the file.

When a Freenet user wants to download a file, the user downloads the index piece, which enables the user to retrieve the remaining pieces of the file. Those pieces have been stored on the hard drives of other users, so the Freenet software will request the remaining pieces of the file from Freenet peers. The requests for file pieces are divided up in "roughly equal amounts among the user's peers." App. 73. If, for example, a user "has 10 peers and requests 1000 pieces of a file," the software requests one hundred pieces from each of the ten peers. App. 73. If one of those ten peers "does not have the particular requested pieces in its storage, that peer will then divide up and ask its peers for the pieces, and so on." App. 73. To prevent this process from continuing indefinitely, Freenet only allows a request to be forwarded eighteen times.

Freenet attempts to hide the identity of the original requester "by making it difficult to differentiate whether a request for a piece that comes in from a peer originated with that peer . . . or whether that peer was simply forwarding a different peer's request." App. 75. But Freenet does not create full anonymity for its users. The software does not, for example, mask a computer's IP address.

Law enforcement has been investigating the trafficking of child pornography on Freenet since 2011. Law enforcement officers use a modified version of the Freenet software ("Law Enforcement Nodes") to assist these investigations. Like ordinary Freenet users, Law Enforcement Nodes can receive, fill, and relay requests for file pieces.

But Law Enforcement Nodes can also log certain information, such as the IP addresses of a user's peers, the number of peers those peers claim to have, the remaining number of times a request for a piece may be forwarded, and more. Law enforcement officers "collect keys associated with suspected child pornography files" and investigate Freenet users who request pieces associated with those keys. App. 78.

To aid these investigations, Professor Brian Levine and other researchers developed a mathematical algorithm ("the Algorithm") that can be applied when a peer sends a request to a law enforcement node to determine "whether it is significantly more probable than not that the peer is the original requester of" the file. App. 78. The Algorithm relies on four variables: (1) the number of download requests made to the law enforcement node; (2) the number of peers directly connected to the requester, including the law enforcement node; (3) the total number of requests made by a downloader of the given file; and (4) the number of peers of a hypothetical original requester.

Special Agent Quinn observed in the instant investigation that on four separate occasions, a Freenet user requested from Freenet Law Enforcement Nodes large numbers of pieces from files with keys associated with child pornography. Agent Quinn used the key to download the files and discovered that they all contained child pornography. She then applied the Algorithm and determined that this requester was likely the original requester.

Law enforcement then determined that the Freenet user's IP address was controlled by Verizon and subpoenaed Verizon for subscriber information related to that IP address. The results of the subpoena showed that the account holder was Nathan

Weyerman at his girlfriend's address in Philadelphia. Law enforcement also determined through public databases where Weyerman resided. Law enforcement then served a second subpoena on Verizon and confirmed that there was internet service at Weyerman's apartment and that Weyerman was the internet subscriber.

Magistrate Judge Marylin Heffley approved warrants for both addresses. The FBI searched both residences and recovered a laptop computer, a desktop computer, and drives that contained child pornography video and image files from Weyerman's apartment.[1] A grand jury charged Weyerman with receiving and possessing child pornography. Weyerman moved to suppress the recovered evidence on the ground that the FBI lacked probable cause to search his apartment because the FBI relied on an unreliable Algorithm to determine that Weyerman had retrieved child pornography from Freenet. The District Court held a hearing on the motion, and Professor Levine appeared as a witness to explain the Algorithm. The court denied the motion to suppress, holding that probable cause supported the warrant and that, in the alternative, the Government relied on the warrant in good faith. Weyerman timely appealed.

II.[2]

Weyerman advances a single argument on appeal: that the District Court erred in failing to suppress evidence because the search warrant affidavit omitted material facts

[1] The FBI did not recover anything from Weyerman's girlfriend's apartment.

[2] The District Court had jurisdiction under 18 U.S.C. § 3231. We have jurisdiction under 28 U.S.C. § 1291.

about the reliability of the Algorithm. Weyerman points to Franks v. Delaware, 438 U.S. 154 (1978), which held that a district court must hold a "Franks" hearing when a defendant "makes a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included . . . in the warrant affidavit, and . . . the allegedly false statement is necessary to the finding of probable cause." Id. at 155–56. The Government argues that Weyerman failed to preserve this argument for appeal because his argument before the District Court pertained only to the accuracy of the Algorithm, not to whether Agent Quinn omitted material facts about the Algorithm from her affidavit. We agree.

Weyerman does not that contend that he requested a Franks hearing in the District Court, and, instead, claims that the hearing that took place before the District Court constituted a Franks hearing. See Weyerman Reply Br. 4 (The "procedural history" of this case "can only be framed under Franks . . . ."). But this hearing did not address any alleged omission in the search warrant affidavit. It addressed only whether the Algorithm was reliable enough to establish probable cause.[3] Weyerman appears to concede as much, stating that while he "did not label his district court argument under Franks, he uses this label on appeal because it is the only possible explanation for what occurred in the district court proceedings." Weyerman Reply Br. 4. But regardless of how

[3] Indeed, in his motion to suppress that prompted the hearing, Weyerman argued that the Algorithm was not accurate enough to determine whether he was the original requestor of the files such that law enforcement officers had probable cause to search his home. The motion made no mention of any alleged omissions in the warrant affidavit.

Weyerman labeled his argument, Franks requires a defendant to make a preliminary showing that the officer swore a false affidavit "knowingly and intentionally, or with reckless disregard for the truth." Franks, 438 U.S. at 155. Weyerman made no effort to do so before the District Court. He therefore forfeited his Franks argument. See United States v. Olano, 507 U.S. 725, 733 (1993) ("[F]orfeiture is the failure to make the timely assertion of a right.").

III.

Because Weyerman did not preserve the Franks issue before the District Court, the standard of review is plain error. Id. at 731–34. Federal Rule of Criminal Procedure 52(b) provides this Court with limited authority to consider and correct errors that were forfeited because they were not raised in the District Court. Under this standard, the defendant must demonstrate that there is "(1) an error, (2) that is plain, and (3) that the plain error affects his substantial rights." United States v. Aguirre-Miron, 988 F.3d 683, 687 (3d Cir. 2021). Once all three prongs are met, we may exercise our discretion to correct the error if it "seriously affects the fairness, integrity or public reputation of judicial proceedings." Rosales-Mireles v. United States, 138 S. Ct. 1897, 1905 (2018) (quoting Molina-Martinez v. United States, 578 U.S. 189, 914 (2016) (citations omitted)).

We consider whether the District Court erred in failing to suppress evidence on the ground that Special Agent Quinn recklessly omitted material facts from the search warrant affidavit in violation of Franks. A defendant must prove at a Franks hearing that (1) the affiant knowingly or recklessly made an omission that created a falsehood in applying for a warrant; and (2) the omission was material, such that probable cause does

not exist under a corrected affidavit. United States v. Yusuf, 461 F.3d 374, 383 (3d Cir. 2006). An omission is made with reckless disregard if an officer withholds a fact that "any reasonable person would know that a judge would want to know." United States v. Desu, 23 F.4th 224, 234 (3d Cir. 2022) (quoting Wilson v. Russo, 212 F.3d 781, 783 (3d Cir. 2000)).

Weyerman has failed to demonstrate that Special Agent Quinn recklessly omitted material facts from the warrant affidavit. Weyerman argues that, while the Algorithm relies upon four variables, Agent Quinn described only three of those variables in her affidavit. The three variables that were included in her affidavit change depending on the size and type of file requested, as well as other information law enforcement receives. But the fourth variable — the number of peers of a hypothetical original requester — is always fixed at eight in the Algorithm. On average, users have about thirty peers, and the number eight is an "extremely conservative" estimate based on real world counts previously observed, as well as on Freenet statistics. App. 113. A 2017 peer-reviewed academic paper explained that using eight as the variable led to a false positive rate of 0–3%. Weyerman has not shown that Agent Quinn recklessly omitted the fourth variable, particularly given Agent Quinn's otherwise detailed description of the Algorithm and the fact that she applied the Algorithm to four separate transmissions before seeking the search warrant. And given the low error rate resulting from the use of the number eight, adding the fourth variable back into a "corrected affidavit" does not negate probable cause. See Yusuf, 461 F.3d at 383. The District Court therefore did not err, much less

plainly err, in failing to suppress evidence discovered in the execution of the search warrant.

IV.

For the foregoing reasons, we will affirm the judgment of the District Court.