App. 1

United States Court of Appeals
for the Eighth Circuit

No. 16-3795

United States of America

Plaintiff-Appellee

v.

Alexander Patrick McArdle

Defendant-Appellant

Appeal from United States District Court
for the Southern District of Iowa – Des Moines

Submitted: June 9, 2017
Filed: August 7, 2017
[Unpublished]

Before WOLLMAN, GRUENDER, and SHEPHERD, Circuit Judges.

PER CURIAM.

Alexander McArdle entered a conditional guilty plea to one count of accessing with intent to view child pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B)

and 2252A(b)(2). He appeals from the district court's[1] denial of his motion to suppress evidence and his request for a hearing on the motion. We affirm.

Special Agent Rodrigo Rosas of the United States Department of Homeland Security submitted an affidavit in support of a search warrant application (the warrant affidavit), which set forth the following facts. While conducting an investigation into the distribution of child pornography over the Internet through a peer-to-peer file-sharing program, Homeland Security Special Agent Aaron Simon identified a computer at a particular Internet protocol address (IP address) that was potentially making child pornography files available for other users to download. Simon downloaded five video files from this computer (the affidavit videos). The first, second, fourth, and fifth videos depicted minors engaging in sexually explicit conduct that constituted child pornography under 18 U.S.C. § 2256(8). The affidavit stated that the third video depicted individuals engaging in sexually explicit conduct, but that it was "not apparent from the appearance of the participants whether or not they are minors." Simon learned that the IP address was registered to an apartment in West Des Moines, Iowa, and was told by the apartment manager that the apartment was occupied by Alexander McArdle.

A search warrant for McArdle's apartment was issued based on the affidavit. Officers executed the

---

[1] The Honorable John A. Jarvey, Chief Judge, United States District Court for the Southern District of Iowa.

warrant and seized an unconnected hard drive, a laptop computer, and a USB travel drive (the seized computer media). During an interview with the officers, McArdle admitted that he had viewed and possessed child pornography. He stated that he had hidden the child-pornography files by not saving them to his computer or by deleting them. The government found images and videos of child pornography on the seized computer media, but did not find the affidavit videos.

McArdle retained a forensic expert, Larry Smith, who prepared a written report after examining the affidavit videos and the seized computer media. Smith agreed that the first, fourth, and fifth videos depicted minors engaging in sexually explicit conduct, but stated that he could not identify the source of the videos. He stated that he could not tell the age of the individual in the second video and that the individuals in the third video appeared to be young adults. Smith reported that he was unable to find the affidavit videos on the seized computer media, but that he had found "evidence in the unallocated space that a file with the name [of the fifth video] may have once existed on the drive." He also stated that he "located evidence of the filename [of the first video] in the unallocated space, but that file does not exist on this drive."

McArdle moved to suppress all evidence stemming from the execution of the search warrant and requested a hearing on the motion. He argued that, because the affidavit videos were not present on the seized computer media, the statement that Simon had downloaded those videos from a computer using McArdle's

IP address must have been an intentional or reckless false statement that vitiated any probable cause for the search and thus violated his Fourth Amendment rights under *Franks v. Delaware*, 438 U.S. 154 (1978).

In denying the motion to suppress and the request for a hearing, the district court stated:

> The defendant's forensic expert's inability to duplicate the government's results from an examination of the defendant's computer does not demonstrate that the statements of Agent Rosas were either false or made with reckless disregard for the truth. Typically, forensic experts are able to reproduce such results. Sometimes they are not. The inability to replicate results through a forensic examination is simply not sufficient to demonstrate the requisite falsity or reckless disregard for the truth required in order to secure an evidentiary hearing pursuant to *Franks v. Delaware.*

D. Ct. Order of Mar. 10, 2016, at 5. The court thereafter denied McArdle's subsequent motion for reconsideration.

When a criminal defendant "makes a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit, and if the allegedly false statement is necessary to the finding of probable cause, the Fourth Amendment requires that a hearing be held at the defendant's request." *Franks*, 438 U.S. at 155-56. If the defendant establishes at the hearing by a preponderance of the

evidence that such intentional or reckless false statements were included in the affidavit and if without the false statements "the affidavit's remaining content is insufficient to establish probable cause," then "the search warrant must be voided and the fruits of the search excluded to the same extent as if probable cause was lacking on the face of the affidavit." *Id*. at 156. The requirement of making a substantial preliminary showing "is not lightly met." *United States v. Wajda*, 810 F.2d 754, 759 (8th Cir. 1987). "To mandate an evidentiary hearing, the challenger's attack must be more than conclusory and must be supported by more than a mere desire to cross-examine. There must be allegations of deliberate falsehood or of reckless disregard for the truth, and those allegations must be accompanied by an offer of proof." *Franks*, 438 U.S. at 171. "[W]e review the denial of a *Franks* hearing for abuse of discretion." *United States v. Arnold*, 725 F.3d 896, 898 (8th Cir. 2013) (quoting *United States v. Kattaria*, 553 F.3d 1171, 1177 (8th Cir. 2009) (en banc) (per curiam)).

We conclude that McArdle did not make the requisite preliminary showing that Rosas intentionally or recklessly included a false statement in the warrant affidavit. That Smith was unable to find the affidavit videos on the seized computer media does not establish that they were never present there. McArdle admitted that he had deleted files of child pornography from his computer to prevent others from discovering them. He argues that "[i]f the files *ever* existed on McArdle's seized equipment there would be evidence relating to their presence on the drives, whether the files were

deleted or not," because "[d]eleting a file does not destroy it, and it still leaves remnants to be found." Appellant's Br. 14-15. The sources that McArdle cites in support of this proposition, however, establish only that evidence of a deleted file may be found during a subsequent investigation, not that such evidence will always be found.[2] Indeed, the warrant affidavit explained that it had been Rosas's experience that in some cases in which the suspect admitted that child pornography had once been present, no files of child pornography were found on the suspect's computer because either the files had been deleted or the computer containing them had been removed from the premises. Moreover, as set forth above, forensic expert Smith stated that he had found evidence that the fifth affidavit video may have once existed on the seized computer media and that he found evidence of the first video's filename.

We also reject McArdle's argument that the district court improperly relied on extra-warrant-application information in stating in its denial order that "Typically, forensic experts are able to reproduce such results. Sometimes they are not." This statement was a reasonable inference from the above-described record

---

[2] For instance, the warrant affidavit explained that "digital information *can* [ ] be retained unintentionally"; that "the interplay between software applications and the computer operating systems *often* results in material obtained from the Internet being stored multiple times" and thus "attempts at deleting the material *often* fail"; and that "digital data that may have evidentiary value to th[e] investigation *could* exist in the user's computer media despite, and long after, attempts at deleting it."

materials regarding the evidence of deleted files that may remain on computer media.

The judgment is affirmed.

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF IOWA
CENTRAL DIVISION

UNITED STATES OF AMERICA, Plaintiff, vs. ALEXANDER PATRICK MCARDLE, Defendant.	No. 4:15cr0020-JAJ **ORDER** (Filed Mar. 10, 2016)

This matter comes before the court pursuant to the defendant's February 24, 2016 Motion to Suppress Evidence. [Dkt. 114] The government resisted the motion on February 26, 2016 [Dkt. 115] and the defendant filed a reply on February 29, 2016. [Dkt. 116] The government has recently moved to deny an evidentiary hearing.

The defendant brings this motion to suppress pursuant to *Franks v. Delaware*, 428 U.S. 154 (1978) challenging a search warrant presented by Homeland Security Special Agent Rodrigo Rosas to the Honorable Ross A. Walters, United States Magistrate Judge, Southern District of Iowa. The warrant sought evidence pertaining to the acquisition and distribution of child pornography pursuant to the ARES P2P file sharing network.

The Search Warrant

The eighteen page affidavit submitted in support of the warrant described Agent Rosas' background and experience [¶ 1], the technology used in the investigation [¶¶ 5-9], background information on computers and child pornography [¶¶ 11-18], background information for searching and seizing computers [¶¶ 19-31], information on child pornography collector characteristics [¶¶ 32-34], and a summary of the investigation [¶¶ 35-42].

In the summary of the investigation, Agent Rojas identified activities of Homeland Security Agent Aaron Simon. It states that on February 19, 2013 Agent Simon was investigating the sharing of child pornography files pursuant to the ARES P2P file sharing network. Agent Simon identified a computer with the IP address 173.22.91.208 as a potential source for at least two files of investigative interest. Investigators conducting key word searches or hash value searches for files relating to child abuse material including child pornography on the ARES network were directed to the above-described IP address. Law enforcement officers determined that the computer associated with that IP address had left its ARES program configured so as to permit the sharing of files from its shared folder. [¶¶ 35-37]

The affidavit further states that on five occasions between February 19, 2013 and March 28, 2013, Special Agent Simon was able to download particular files from the 173.22.91.208 IP address computer. [¶ 38] A

description of these images is found in paragraph 39. The first two images and the last two images are described as involving "two pre-pubescent females approximately 6-9 years old" "an 8-12 year old female" "an 11-14 year old female" and "a minor female approximately 11-14 years old" engaging in activity that qualifies as sexually explicit conduct prohibited by federal child pornography criminal statutes. The third image is a movie entitled "Sweet 15" depicting two females and two males having sex. The affidavit specifically states that it is not apparent from the appearance of the participants whether or not they are minors.

Agent Simon determined that the company that leases the above-described IP address was Mediacom. A subpoena sent to Mediacom showed that the IP address at times relevant to this investigation was leased to a "Grant McArdle" at the apartment that was ultimately searched. Prior to securing the warrant, Agent Rosas went to the location to check for unsecured wireless Internet networks and found none. Agent Simon determined that the apartment in question was registered to "Alexander" not "Grant" McArdle.

The Defendant's Franks v. Delaware Motion

The defendant has secured the assistance of a forensic computer examiner. The problems associated with the defendant's forensic evaluation of the computer have been the subject of several motions to continue the trial, a motion to dismiss and other filings. At first, it appeared that the defendant's expert could not

duplicate any of the government's results by examining a mirror image of the defendant's hard drive. After much activity between the parties, the expert has apparently been able to duplicate some, but not all, of the government's results.

With respect to the five files downloaded by Agent Simon and described in paragraphs 38-39 of the warrant affidavit, the defendant's forensic expert makes the following comments. First, with respect to the first, fourth and fifth images, the motion to suppress states, "McArdle's expert could not confirm the source of this material." With respect to the second image, the motion states, "According to McArdle's expert, he was unable to tell the age of the female." Finally, with respect to the third image, the motion states, "According to McArdle's expert, these appear to be young adults."

McArdle's expert cannot find the images/videos alleged to have been downloaded by the defendant on any of defendant's computer equipment. The expert found child pornography but did not find the listed pornography. Because the expert could not find it, the motion states, "There appears to be an inaccuracy or falsehood in the search warrant application." [Dkt. 114, ¶ 15] The motion states what we have all learned from forensic computer evaluations and that is that there are few ways to permanently delete files from a computer's hard drive and random access memory.

The question before the court is whether the expert's inability to replicate the information reported by Agent Simon and used by Agent Rosas to secure the

warrant is grounds for a *Franks v. Delaware* hearing and potential evidence suppression.

Franks v. Delaware

In order to prevail on a challenge to a warrant affidavit pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978), the challenger must show (1) that a false statement knowingly and intentionally or with reckless disregard for the truth, was included in the affidavit and (2) that the affidavit's remaining content is insufficient to establish probable cause. *United States v. Gladney*, 48 F.3d 309, 313 (8th Cir. 1995).

> To mandate an evidentiary hearing, the challenger's attack must be more than conclusory and must be supported by more than a mere desire to cross-examine. There must be allegations of deliberate falsehood or of reckless disregard for the truth, and those allegations must be accompanied by an offer of proof. They should point out specifically the portion of the warrant affidavit that is claimed to be false; and they should be accompanied by a statement of supporting reasons. Affidavits or sworn or otherwise reliable statements of witnesses should be furnished, or their absence satisfactorily explained. Allegations of negligence or innocent mistake are insufficient.

Franks v. Delaware, *supra*, at 171.

Further, in order to mandate a hearing, the challenged statements in the affidavit must be necessary to a finding of probable cause. *United States v. Flagg*,

919 F.2d 499 (8th Cir. 1990). *United States v. Streeter*, 907 F.2d 781, 788 (8th Cir. 1990) (contested material must be "vital" to probable cause). It must also be remembered that although the affidavit must contain statements that are truthful,

> This does not mean "truthful" in the sense that every fact recited in the warrant affidavit is necessarily correct. For probable cause may be founded upon hearsay and upon information received from informants, as well as upon information within the affiant's own knowledge that some times must be garnered hastily. But surely it is to be "truthful" in the sense that the information put forth is believed or appropriately accepted by the affiant as true.

Franks v. Delaware, *supra*, at 165.

Analysis

Agent Simon was reported to have used a computer to access the ARES P2P file sharing network. Using key word and hash value searches, the police had determined that a computer IP address associated with the defendant's residence was available for the sharing of child pornography. In the affidavit, Agent Simon's successful downloading of child pornography from that address is described by date, time, file name, hash value and a description of the contents of those files.

The defendant's forensic expert's inability to duplicate the government's results from an examination of the defendant's computer does not demonstrate that the statements of Agent Rosas were either false or made with reckless disregard for the truth. Typically, forensic experts are able to reproduce such results. Sometimes they are not. The inability to replicate results through a forensic examination is simply not sufficient to demonstrate the requisite falsity or reckless disregard for the truth required in order to secure an evidentiary hearing pursuant to *Franks v. Delaware.*

Upon the foregoing,

IT IS ORDERED that the defendant's Motion to Suppress Pursuant to *Franks v. Delaware* is denied without a hearing.

DATED this 10th day of March, 2016.

/s/ John A. Garvey
JOHN A. GARVEY, Chief Justice
UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF IOWA

UNITED STATES COURT OF APPEALS
FOR THE EIGHTH CIRCUIT

No: 16-3795

United States of America

Appellee

v.

Alexander Patrick McArdle

Appellant

Appeal from U.S. District Court for the
Southern District of Iowa – Des Moines
(4:15-cr-00020-JAJ-1)

ORDER

The petition for rehearing en banc is denied. The petition for rehearing by the panel is also denied.

Judge Kelly did not participate in the consideration or decision of this matter.

September 14, 2017

Order Entered at the Direction of the Court:
Clerk, U.S. Court of Appeals, Eighth Circuit.

/s/ Michael E. Gans