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[Unpublished]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 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.

---

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

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

The judgment is affirmed.

---

[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."