FILED
United States Court of Appeals
Tenth Circuit

February 17, 2010

Elisabeth A. Shumaker
Clerk of Court

PUBLISH

UNITED STATES COURT OF APPEALS

TENTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

HAROLD G. HENDERSON,

Defendant-Appellant.

No. 09-8015

Appeal from the United States District Court
for the District of Wyoming
(D.C. No. 2:06-CR-174-WFD-1)

John H. Robinson, Jamieson & Robinson, LLC, Casper, Wyoming for the Defendant–Appellant.

Stephanie I. Sprecher, Assistant United States Attorney (Kelly H. Rankin, United States Attorney, with her on the briefs), Casper, Wyoming for the Plaintiff–Appellee.

Before **TACHA**, **SEYMOUR**, and **LUCERO**, Circuit Judges.

LUCERO, Circuit Judge.

While executing a warrant to search Harold Henderson's home, law enforcement officers discovered child pornography on Henderson's computer. Henderson filed a motion to suppress this evidence, arguing that it was obtained in violation of his Fourth Amendment rights and, therefore, that the exclusionary rule should preclude its introduction. On denial of his motion, Henderson conditionally pled guilty to receipt of child pornography, preserving his right of review. Exercising jurisdiction under 28 U.S.C. § 1291, we affirm the denial of Henderson's motion to suppress.

I

In June 2005, Special Agent Robert Leazenby of the Wyoming Division of Criminal Investigation conducted a state-wide digital child pornography probe. He received information that a computer with a particular internet protocol ("IP") address downloaded and shared two videos.[1] Each video had a secure hash algorithm ("SHA") value associated with child pornography.[2] Leazenby confirmed that videos with the

[1] As this court has previously explained:

> [A]n IP address . . . is a unique number identifying the location of an end-user's computer. When an end-user logs onto a[n] . . . internet service provider, they are assigned a unique IP number that will be used for that entire . . . session. Only one computer can use a particular IP address at any specific date and time.

United States v. Hamilton, 413 F.3d 1138, 1141 n.2 (10th Cir. 2005).

[2] An SHA value serves as a digital fingerprint:

Continued . . .

relevant SHA values depicted children engaging in sexual activity. He also received information from Bresnan Communications, an internet service provider, that the relevant IP address had been assigned to a computer located at 3824 Gregg Way, Apartment C, in Cheyenne, Wyoming.

Based in part on this information, Leazenby applied for and received a warrant to search the Gregg Way apartment. Leazenby's supporting affidavit provides his professional background; describes the general protocol investigating officers use to identify distributors of child pornography, including how officers usually determine that a computer at a given IP address has transferred a video with a particular SHA value; and states that Leazenby "learned" that a computer with the relevant IP address had shared videos with child-pornography-related SHA values.[3] His affidavit, however, does not

---

> Computer files offered on peer-to-peer software can be analyzed and identified by a mathematical algorithm known as [SHA]. A SHA value of a computer file is, so far as science can ascertain presently, unique. No two computer files with different content have ever had the same SHA value. From investigations of child pornography that have been conducted in the past, law enforcement maintains a database of the SHA values of computer files that have been discovered to contain known images of child pornography.

United States v. Klynsma, No. CR 08-50145-RHB, __ F.3d __, 2009 WL 3147790, at *6 (D. S.D. Sept. 29, 2009).

[3] The affidavit provides:

> On June 13, 2005 your Affiant was assigned to investigate a computer in Cheyenne, Wyoming that was sharing movies of child pornography. Affiant learned that on May 25, 2005, a computer with an IP address of

Continued . . .

identify: (1) who informed Leazenby that a computer with the relevant IP address had transferred child pornography; or (2) the method used <u>in this case</u> to establish that a computer at the specified IP address transferred videos with child-pornography-associated SHA values.

Upon executing the search warrant, law enforcement discovered that three individuals, including Henderson, lived in the Gregg Way apartment. The apartment also contained three computers. Agents conducted a forensic review of the three computers and found child pornography on Henderson's computer. Coincidentally, Henderson's computer was actually in the process of downloading child pornography while the agents conducted the search. This led to the seizure of Henderson's hard drive and related computer items.

Henderson was indicted for receipt and possession of child pornography in violation of 18 U.S.C. § 2252A(a)(2)(A), (a)(5)(B), (b)(1), and (b)(2). He initially pled guilty, but his resulting conviction and sentence were vacated because he had been erroneously advised regarding the mandatory minimum sentence for his crimes.

> 69.146.128.218 offered to contribute to the distribution of a movie file with the SHA value of ZZLGX2MOZQ7CX2353J5RYVKFJ7BPBPQE.
>
> . . .
>
> Your Affiant learned that on June 1, 2005, a computer with the same IP address of 69.146.128.218 offered to contribute to the distribution of a movie file with the SHA value QQ4CQNK5HG2IAAYHW3MRWZ2GFI5J4JRF.

After his case was set for a new trial, Henderson filed a motion to suppress evidence resulting from the search of his apartment. He argued that the warrant was not supported by probable cause and that police could not have reasonably relied on the warrant in good faith. In assessing probable cause, the district court noted that "the reliability of matching the SHA[] values and IP numbers cannot be disputed with any merit. The science behind 'fingerprinting' these computers . . . appears rock solid . . . ." Nevertheless, the court determined "the reliability of the information [is], in this case, insufficient to establish probable cause" because Leazenby's affidavit did not indicate the source of the listed IP address and SHA values. Despite this lack of probable cause, the court found that a reasonable officer could have relied upon the warrant in good faith; hence the evidence was admissible.

After this ruling, Henderson entered a conditional guilty plea to the receipt charge, and the possession charge was dismissed. The court sentenced Henderson to sixty-three months' imprisonment, followed by a life term of supervised release. Henderson timely appealed.

II

Under the exclusionary rule, the government may not introduce into evidence "tangible materials seized during an unlawful search [or] . . . testimony concerning knowledge acquired during an unlawful search." Murray v. United States, 487 U.S. 533, 536 (1988) (citations omitted). However, exclusion is far from assured if law enforcement has obtained a warrant, but the warrant is later determined to be unsupported by probable cause. If law enforcement could have acted in objective good faith in executing a warrant—that is, if an officer could have acted in objectively reasonable reliance on a magistrate's determination of probable cause—the exclusionary rule does not apply. United States v. Leon, 468 U.S. 897, 921-23 (1984).

The government wisely conceded at oral argument that Leazenby's affidavit is insufficient to establish probable cause. Notably, the affidavit fails to identify how Leazenby's source determined that a computer with the relevant IP address—rather than some other computer—shared videos with child-pornography-related SHA values.[4] Accordingly, the sole issue before us is whether the district court properly determined that evidence resulting from this unlawful search was nonetheless admissible due to the good faith exception. We review this question de novo. United States v. Vanness, 342 F.3d 1093, 1097 (10th Cir. 2003).

A

In Leon, the Supreme Court applied the good faith exception to a case in which "the affidavit included no facts indicating the basis for the informants' statements concerning [the defendant's] criminal activities and was devoid of information establishing the informants' reliability." 468 U.S. at 905. We are faced with a similar situation. This affidavit fails to disclose the source of Leazenby's information and does

[4] Although the district court determined that "[t]he science behind 'fingerprinting' . . . these computers appears rock solid," it apparently overlooked the fact that the affidavit does not state that Leazenby's source in fact engaged in the scientific, rock-solid method generally used by law enforcement.

not contain any information establishing the source's reliability. Further, the affidavit does not establish the method Leazenby's source used to match the illegal videos with the relevant IP address; consequently, it does not adequately indicate the basis for the source's statements that a computer at that IP address transferred child pornography. Although these errors make the search illegal, Leon counsels that they do not necessarily require application of the exclusionary rule.

We presume an officer's acts to be in objective good faith when supported by a warrant. United States v. Cardall, 773 F.2d 1128, 1133 (10th Cir. 1985). This presumption, however, is not absolute; it can be overcome by demonstrating that a warrant was "based on an affidavit so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable." Leon, 468 U.S. at 923 (quotation omitted). Reliance is "entirely unreasonable" only if the affidavit submitted in support of the warrant is "devoid of factual support." Cardall, 773 F.3d at 1133. An affidavit has enough factual support to justify reliance if it "establishe[s] a minimally sufficient nexus between the illegal activity and the place to be searched." United States v. Gonzales, 399 F.3d 1225, 1230-31 (10th Cir. 2005) (quotation omitted).

Leazenby's affidavit is not devoid of factual support. It states that Leazenby's source determined that a particular computer downloaded two videos with SHA values associated with child pornography. That computer had an IP address mapping to the Gregg Way apartment. Combined, these facts provide a minimal nexus between a computer in the Gregg Way apartment and the receipt and possession of child pornography.

B

Even if an affidavit is not devoid of factual support, an officer cannot hide behind the good faith exception if she "knows or should have known that a search warrant was invalid." United States v. McKneely, 6 F.3d 1447, 1455 (10th Cir. 1993). Law enforcement officials are presumed to have a reasonable knowledge of the law. Leon, 468 U.S. at 919 n.20. As a result, prior court decisions resting on functionally identical facts can put law enforcement on notice that an affidavit is insufficient to establish probable cause.

Leazenby's affidavit was based on a standardized form affidavit, which was used by law enforcement officials throughout Wyoming at the time of the investigation. Both the U.S. District Court for the District of Wyoming and this court have held that an affidavit based on the same standardized form did not establish probable cause. United States v. Stevahn, 313 Fed. App'x 138, 140-42 (10th Cir. 2009) (unpublished) (affirming district court's finding of no probable cause). But cf. United States v. Harrison, 566 F.3d 1254, 1256-57 (10th Cir. 2009) (declining to determine whether the form affidavit was sufficient to establish probable cause because the good faith exception applied). Henderson, however, has not pointed us to any similar decision issued before his apartment was searched. Accordingly, he has failed to prove that law enforcement was on notice that the form affidavit used by Leazenby was insufficient to establish probable cause.

III

Given that Henderson has not overcome the presumption that law enforcement officers acted in objective good faith when executing a warrant to search his home, we **AFFIRM** the district court's denial of his motion to suppress.

ENTERED FOR THE COURT

Carlos F. Lucero
Circuit Judge