[DO NOT PUBLISH]

IN THE UNITED STATES COURT OF APPEALS

FOR THE ELEVENTH CIRCUIT

No. 16-15844
Non-Argument Calendar

D.C. Docket No. 6:15-cr-00252-RBD-GJK-1

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

versus

TIMOTHY MICHAEL SEDLAK,

Defendant-Appellant.

Appeal from the United States District Court
for the Middle District of Florida

(September 25, 2017)

Before TJOFLAT, JULIE CARNES and JILL PRYOR, Circuit Judges.

PER CURIAM:

A jury convicted Timothy Michael Sedlak on two counts of production of child pornography, in violation of 18 U.S.C. §§ 2251(a) and 2251(e), and one

count of possession of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(5)(B) and 2252A(b)(2). Sedlak appeals his convictions on the ground that the District Court erred in denying his motion to suppress on the basis that the warrant—which authorized Secret Service agents to search his electronic storage devices for evidence of "hacking" and led (during the search) to the discovery of child pornography—was overbroad and that none of the relevant exceptions to the exclusionary rule applied.[1]

We review a district court's denial of a motion to suppress under a mixed standard. While the district court's findings of fact are reviewed for clear error, its application of the law to those facts is reviewed *de novo*. *United States v. Bervaldi*, 226 F.3d 1256, 1262 (11th Cir. 2000). "Further, when considering a ruling on a motion to suppress, all facts are construed in the light most favorable to the prevailing party below." *Id.* (citation omitted). "[W]e may affirm the denial of a motion to suppress on any ground supported by the record." *United States v. Caraballo*, 595 F.3d 1214, 1222 (11th Cir. 2010) (citation omitted).

The Fourth Amendment prohibits unreasonable searches and seizures and requires a search warrant to particularly describe the place to be searched and the things to be seized. U.S. CONST. amend. IV. A search warrant that does not

[1] The search warrant was obtained after law enforcement traced the hacking of the computer system of a charitable organization in New York to two Internet Protocol ("IP") addresses linked to Sedlak's residence in Ocoee, Florida, and to the subscriber of the IP addresses, Sedlak.

sufficiently particularize the things to be sought and seized is unconstitutionally overbroad. *United States v. Travers*, 233 F.3d 1327, 1329 (11th Cir. 2000). Any evidence seized as the result of an overbroad warrant must be excluded from the trial of the defendant. *Id.* A warrant is sufficient when it describes the place to be searched with particularity so as to direct the searcher to confine his search to the place described. *United States v. Burke*, 784 F.2d 1090, 1092 (11th Cir. 1986). However, the particularity requirement must be applied with a "practical margin of flexibility," depending on the type of property to be seized and the nature of the activity under investigation. *United States v. Wuagneux*, 683 F.2d 1343, 1349 (11th Cir. 1982). In determining the sufficiency of a warrant's description, we consider whether the description is "as specific as the circumstances and the nature of the activity under investigation permit." *Id.*

We have recognized that effective investigation of complex white collar crimes may require "the assembly of a 'paper puzzle' from a large number of seemingly innocuous pieces of individual evidence," and that the complexity of a crime cannot be used as a shield against detection when the government has shown probable cause that a suspect possesses evidence of a crime. *Id.* We have rejected the claim that the lack of a written "search protocol" in a warrant infringes a defendant's Fourth Amendment rights where unresponsive documents were

opened, but not analyzed. *United States v. Khanani*, 502 F.3d 1281, 1290–91 (11th Cir. 2007).

When law enforcement officers act in the objectively reasonable belief that their conduct does not violate the Fourth Amendment, the exclusionary rule does not provide a deterrent effect. *Travers*, 233 F.3d at 1329. Thus, when an officer has obtained a search warrant in good faith from a judge or magistrate and acted within its scope, an exception applies and the evidence obtained will not be excluded. *Id.* The good faith inquiry is confined to the "objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal despite the magistrate's authorization." *United States v. Leon*, 468 U.S. 897, 922 n.23 (1984). However, the good faith exception does not apply where the issuing judge "wholly abandoned his judicial role," or where the warrant is "so facially deficient" that the executing officers cannot presume it to be valid. *United States v. Martin*, 297 F.3d 1308, 1313 (11th Cir. 2002) (quotation omitted).

We find no error in the District Court's denial of Sedlak's motion to suppress. Considering the specific circumstances and complexities of a hacking investigation, the warrant was sufficiently particularized within the allowable margin of flexibility. *See Wuagneux*, 683 F.2d at 1349. The fact that there was no specific search protocol limiting the time frame of searchable electronically stored information did not render the warrant overbroad. *See Khanani*, 502 F.3d at 1290–

91. Furthermore, the agents who executed the search obtained the warrant in good faith, acted within its scope, and acted in the objectively reasonable belief that their conduct did not violate the Fourth Amendment. Therefore, the good faith exception to the exclusionary rule applies.

AFFIRMED.