

United States Court of Appeals
For the Eighth Circuit

No. 17-2178

United States of America

Plaintiff - Appellee

v.

Anthony Allen Jean

Defendant - Appellant

Appeal from United States District Court
for the Western District of Arkansas - Fayetteville

Submitted: February 16, 2018

Filed: June 1, 2018

Before LOKEN, BENTON, and ERICKSON, Circuit Judges.

BENTON, Circuit Judge.

After a bench trial, Anthony A. Jean pled guilty to receiving child pornography in violation of 18 U.S.C. § 2252A(a)(2), (b)(1), and possessing child pornography in violation of 18 U.S.C. § 2252(a)(4)(B), (b)(2). He appeals, arguing that the district

court¹ erred in denying his motion to suppress evidence obtained by a warrant using the Network Investigative Technique (NIT). He also claims the court abused its discretion by denying his motion to disclose the NIT's codes. Having jurisdiction under 28 U.S.C. § 1291, this court affirms.

In 2014, the FBI began investigating a child pornography website "Playpen." It offered users the opportunity to advertise, view, and distribute child pornography. The website's host, the Onion Router, gave anonymity to users, hiding identifying information and requiring access to Playpen through a nondescript web address. Playpen required users to create a username and password.

On February 20, 2015, a United States Magistrate Judge for the Eastern District of Virginia granted the FBI's warrant to search computers, "wherever located," accessing Playpen. The warrant approved the use of NIT, a computer program that reveals Playpen's users. The NIT would "cause" the user's computer to send its Internet Protocol address, operating system information and username, and Media Access Control address to the FBI.

FBI agents discovered a user named "regalbegal." This username belonged to Jean, living in Arkansas. On July 9, 2015, executing an Arkansas search warrant, the agents seized Jean's computer and other devices with child pornography. He admitted downloading and viewing child pornography. He confirmed his username was "regalbegal."

Jean moved to suppress his statements and all evidence from the search. He asserted that the search was unauthorized because the warrant was issued in the Eastern District of Virginia, not Arkansas. The district court denied his motion. He

¹The Honorable Timothy L. Brooks, United States District Judge for the Western District of Arkansas.

then moved to compel disclosure of the complete NIT code, arguing it was material to his defense. The court denied disclosure of the exploit and server codes. Jean pled guilty, preserving his right to appeal the rulings on the motions to suppress and compel.

Jean challenges the NIT warrant under Federal Rule of Criminal Procedure 41(b)(4). His challenge is preempted by this court's decision in *United States v. Horton*, 863 F.3d 1041 (8th Cir. 2017). There, the NIT warrant was upheld under the good faith exception to the exclusionary rule. *Id.* at 1052. This court noted that “the costs of exclusion in this case are substantial. Suppression here would extend beyond the present defendants and impact multiple cases within this circuit.” *Id.* The district court did not err in denying Jean's motion to suppress.

This court reviews “rulings on pretrial motions for production for an abuse of discretion,” reversing “only on a showing that the error was prejudicial to the substantial rights of the defendant.” *United States v. White Horse*, 316 F.3d 769, 773 (8th Cir. 2003) (citation omitted). A defendant may “discover certain documents and tangible objects upon a showing that they are ‘material to the preparation of his defense.’” *United States v. Krauth*, 769 F.2d 473, 476 (8th Cir. 1985). “Material” means “helpful to the defense.” *E.g.*, *United States v. Vue*, 13 F.3d 1206, 1208 (8th Cir. 1994). Inculpatory and exculpatory evidence can “assist in ‘the preparation of the defendant's defense.’” *United States v. Marshall*, 132 F.3d 63, 67 (D.C. Cir. 1998). But a showing of materiality “is ‘not satisfied by a mere conclusory allegation that the requested information is material to the preparation of the defense.’” *Krauth*, 769 F.2d at 476 (citation omitted). Even if a defendant successfully shows materiality, the district court may allow the government to withhold information to “further and protect the public interest in effective law enforcement.” *Barnes v. Dormire*, 251 F.3d 767, 769 (8th Cir. 2001), *citing Roviario v. United States*, 353 U.S. 53, 59 (1957).

Jean argues that the district court abused its discretion by not compelling disclosure of the complete source code for all software it used to identify him, specifically the exploit and server codes. Jean believes these codes were material to his defense. The district court disagreed, finding “Jean’s argument fails to ‘demonstrate that the requested evidence bears some abstract logical relationship to the issues in the case.’” Summarizing the testimony of Jean’s own expert, the district court found that the likelihood of any help to Jean’s defense was “vanishingly small.” The district court did not abuse its discretion in denying the motion to compel.

Alternatively, the court invoked the law-enforcement privilege to prevent disclosure of the exploit code, finding “any need . . . is greatly outweighed by the public’s interest in keeping the exploit secret.” Jean contends a protective order could alleviate this concern. But the court deemed a protective order insufficient: “The risk that the information might inadvertently be leaked or otherwise used by third parties is too great.” The court further found, “Mere knowledge of the particular vulnerability exploited here could potentially lead the expert to later build his own exploit, or assist others in doing so, thereby effectively circumventing a protective order.” The district court did not clearly err in making these findings.

* * * * *

The judgment is affirmed.
