NOT PRECEDENTIAL

UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

No. 10-3634

UNITED STATES OF AMERICA

v.

ROBERT EUGENE BEATTY,

Appellant

On Appeal from the United States District Court
For the Western District of Pennsylvania
(Crim. No. 1-08-cr-00051-001)
District Judge: Honorable Sean J. McLaughlin

Submitted under Third Circuit L.A.R. 34.1(a)
July 14, 2011

BEFORE: SLOVITER, FUENTES, and FISHER, *Circuit Judges*

(Opinion Filed: July 14, 2011)

OPINION OF THE COURT

FUENTES, *Circuit Judge*.

Robert Beatty appeals the District Court's decision to deny his motion to suppress evidence of contraband retrieved from a search of his home computer, as well as

subsequent statements made to law enforcement officials. For the reasons set forth below, we will affirm.

I.

We write primarily for the parties and therefore discuss only the facts necessary to explain our decision. Pennsylvania State Trooper Robert Pearson had been conducting an online investigation of child pornography using a peer-to-peer ("P2P") network. *See e.g., United States v. Stults*, 575 F.3d 834, 837 (8th Cir. 2009) (explaining the purpose of a P2P network). Using search terms that typically yield child pornography, Pearson was able to locate eleven files with graphic titles implicating sex acts with a child. With the help of a Wyoming Internet Crimes Against Children ("Wyoming ICIC") Task Force database, Pearson was able to cross reference and match each file's Secured Hash Algorithm ("SHA1") to known child pornography files. *See e.g.*, *United States v. Miknevich*, 638 F.3d 178, 181 n.1 (3d Cir. 2010) (noting the significance of the SHA1 is that it can act like a fingerprint for a message or data file). It was later determined that these files belonged to appellant Robert Beatty.

Based on this information, Federal Bureau of Investigations ("FBI") special agent Tom Brenneis applied for a warrant to search Beatty's home. The supporting affidavit included the process by which the files were retrieved and the exact name of each file. The affidavit did not state that Pearson or Brenneis opened and viewed any of the files. Following the issuance and execution of a search warrant, the police seized Beatty's

computer, which contained hundreds of child pornographic movies and arrested him. Shortly after, Beatty made various inculpatory statements to the police.

Beatty was charged with one count of receiving/distributing visual depictions of minors engaged in sexually explicit conduct, in violation of 18 U.S.C. §§ 2252(a)(2) and 2252 (b)(1). Beatty was also charged with one count of possessing visual depictions of minors engaged in explicit sexual conduct which had been shipped in interstate and foreign commerce, in violation of 18 U.S.C. §§ 2252 (a)(4)(B) and 2252(b)(2). He moved to suppress evidence recovered from the search of his home and computer, as well as statements he made to the FBI. Specifically, he challenged the adequacy of the probable cause on which the search warrant was issued.

The District Court held that the "highly graphic titles of the files … and [] Pearson's confirmation that these same files were among those identified by the Wyoming ICAC Task Force as 'known child pornography'" was enough to establish probable cause that evidence of a crime would be found on Beatty's computer. *United States v. Beatty*, No. 1:08-cr-51-SJM, 2009 WL 5220643, at *4 (W.D. Penn. Dec. 31, 2009). Beatty filed a timely appeal. The District Court had jurisdiction pursuant to 18 U.S.C. § 3121 and we have jurisdiction over the District Court's final order pursuant to 28 U.S.C. § 1291.

Our review of the District Court's decision denying Beatty's motion to suppress for lack of probable cause is plenary. *United States v. Loy,* 191 F.3d 360, 365 (3d Cir. 1999). However, we must not conduct a *de novo* review of the magistrate judge's finding

of probable cause. *See United States v. Whitner*, 219 F.3d 289, 296 (3d Cir. 2000). It is our job to determine that the magistrate had a "substantial basis" to conclude that the affidavit supporting the warrant established probable cause. *United States v. Jones*, 994 F.2d 1051, 1054 (3d Cir. 1993). During this process, we must only assess the facts presented to the magistrate judge, in this case, what was before her within the "four corners" of the supporting affidavit. *Id.* at 1055. In doing so, we must pay great deference to the magistrate judge's finding of probable cause. *Illinois v. Gates*, 462 U.S. 213, 236 (1983). But, this "does not mean that reviewing courts should simply rubber stamp a magistrate [judge]'s conclusion." *United States v. Tehfe*, 722 F.2d 1114, 1117 (3d Cir. 1983).

II.

A.

The Fourth Amendment protects the right to be free from "unreasonable searches and seizures." U.S. Const. amend. IV. If a warrant is issued , it must be based "upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." *Id.* A magistrate judge may find probable cause when, after considering the totality of the circumstances, "there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Gates*, 462 U.S. at 238. As opposed to a "neat set of legal rules," probable cause is a "fluid concept-turning on the assessment of probabilities in particular factual contexts."

Id. at 232. As such, the warrant's supporting affidavit must be read in a common sense and nontechnical matter. *Id.* at 230-31.

B.

Beatty argues that the warrant's supporting affidavit was facially deficient. Among other reasons, he argues that 1) an overly broad and unconstitutional definition of "child pornography" tainted the reliability of the description of the files and 2) no one involved in the issuance of the warrant viewed the files, which, combined with the lack of a reasonably specific description of the contents of the files, did not allow the magistrate judge to make an independent assessment of probable cause. App. Br. 19.

We start by addressing the issue of taint. The Government contends that this Court "embrace[s] redaction as a practice and principle of law." *United States v. Christine*, 687 F.2d 749, 755 (3d Cir. 1982). When an affidavit has been tainted unconstitutionally, our precedent allows us to redact that taint from the warrant, "striking from [it] those severable phrases and clauses that are invalid for lack of probable cause or generality and preserving those severable phrases and clauses that satisfy the Fourth Amendment." *Id.* at 754. Beatty alleges that the supporting affidavit made use of 18 U.S.C. §§ 2256(8)(b) & (d) and its erroneous and unconstitutional definition of "child pornography," which tainted the magistrate judge's ability to determine probable cause. *See Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002) (striking down these sections of the statute as overbroad and unconstitutional). This argument falls short because even when 18 U.S.C. §§ 2256(8)(b) & (d) are redacted from the affidavit, there is still enough information

available to a magistrate judge to allow for an independent assessment of probable cause. *See Beatty*, 2009 WL 5220643, at *8-10 (discussing the history of two statutory definitions in question and why they were deemed unconstitutional).

We disagree with Beatty's remaining argument because the magistrate judge does not have to view the images herself. Beatty cites to decisions in other circuits to bolster this contention. *See United States v. Battershell*, 457 F.3d 1048, 1051-53 (9th Cir. 2006)*; United States v. Syphers*, 426 F.3d 461, 467 (1st Cir. 2005); *United States v. Chrobak*, 289 F.3d 1043, 1045 (10th Cir. 2002). However, in *United States v. Miknevich*, a case recently decided by this court, we expressly rejected the notion that a magistrate judge must review the contents of the actual files in question. 638 F.3d at 183. In *Miknevich*, we reasoned that without viewing the actual images, the "magistrate [judge] could have drawn a reasonable inference of the file's contents based on its highly descriptive name and SHA1 value." *Id.* at 184. The District Court came to the same conclusion in this case, and we agree that the titles and SHA1 values of the files established probable cause.

Just as we found in *Miknevich*, the graphic titles of the files found on Beatty's computer "contained highly graphic references to specific sexual acts involving children."[1] *Id.* Additionally, the SHA1 values belonging to the files on Beatty's computer bore the same SHA1 values as known child pornography in the Wyoming ICIC

[1] The files include names such as "r@ygold- pedo - 13yo brother fucks 11yo sister and sperm inside 61 943 812.mpg," "(Pthc) 14yo Isabel – (Rape and Fuck) (R@ygold.mpg (sic)," and "(Hussyfan) (phtc) (r@ygold) (babyshivid) Jessica 11yo get fuckt (sic) good.mpg." J.A. 103

Task Force database. Together, these factors allowed a strong inference to be made by the magistrate judge which establishes probable cause. Therefore, the District Court correctly concluded that "the Magistrate Judge was entitled to infer from the highly descriptive and graphic file names and the other information presented in the affidavit [the SHA1 values] that there was a fair probability that [Beatty's] computer would contain material prohibited under either 18 U.S.C. §§2252 or 2252A." *Beatty*, 2009 WL 5220643, at *11.[2] The motion to suppress was properly denied.

III.

For the foregoing reasons, we will affirm the District Court's decision to deny the motion to suppress both the files found on Beatty's computer and his subsequent statements.

[2] We will not reach the issue of good faith reliance on a warrant as we have already decided that the affidavit supporting the warrant was sufficient to establish probable cause.