[PUBLISH]

IN THE UNITED STATES COURT OF APPEALS

FOR THE ELEVENTH CIRCUIT

No. 16-16652

D.C. Docket No. 3:15-cr-00012-TCB-RGV-1

UNITED STATES OF AMERICA,

Plaintiff - Appellee,

versus

CHARLES CARROLL,

Defendant - Appellant.

Appeal from the United States District Court
for the Northern District of Georgia

(April 5, 2018)

Before WILSON and DUBINA, Circuit Judges, and GOLDBERG,* Judge.

WILSON, Circuit Judge:

---

*Honorable Richard W. Goldberg, Judge for the United States Court of International Trade, sitting by designation.

This case involves the dissemination of child pornography through a peer-to-peer file sharing program called Ares. A jury convicted appellant Charles Carroll of knowingly possessing and distributing hundreds of images and videos depicting the sexual exploitation of minors, 18 U.S.C. §§ 2252(a)(4)(B), (a)(2), some of whom were less than twelve years old. The district court applied five Guidelines enhancements and sentenced Carroll to 150 months in prison.

This appeal requires us to determine whether a lawful warrant supported the search of Carroll's home, whether the government put forth sufficient evidence to sustain his convictions, and whether the district court properly enhanced his sentence. Upon thorough review of the record and with the benefit of oral argument, we affirm in part, but we reverse Carroll's distribution conviction because the government failed to put forth any evidence that Carroll knew downloaded files were automatically placed into a shared folder accessible to the Ares peer-to-peer network.

I.

On October 22, 2014, the Georgia Bureau of Investigation (GBI) seized two laptops and an external hard drive from Carroll's Newnan, Georgia home. Forensic analysis later revealed that one of the laptops, a Dell, held 314 images and 65 videos of child pornography in its "unallocated space"—a place where deleted files can still be retrieved using special software. Those files were downloaded

from the peer-to-peer file sharing program Ares over the course of the previous eleven months. Some of the files had been downloaded and deleted, along with the Ares program itself, just days before the laptop's seizure.

Peer-to-peer networks like Ares are "so called because users' computers communicate directly with each other, not through central servers." *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913, 919–20, 125 S. Ct. 2764, 2770 (2005). This decentralized system allows users to search for files across the peer-to-peer network and then to download files directly from the computers of other users. Ares, like many peer-to-peer programs before it,[1] is available for free over the internet and is commonly used to share music and videos. When downloaded, Ares sets up a shared folder on the computer where, by default, it automatically places all subsequent downloads. Once a file is placed in the shared folder, it is immediately available for further dissemination.

Unless an Ares user changes the default settings or deliberately moves files out of the shared folder, downloaded files will remain freely accessible to anyone else on the Ares network—including the GBI Internet Crimes Against Children

[1] Peer-to-peer file sharing programs attracted hundreds of millions of users in the early 2000s, but have struggled to find legal footing because they often facilitate the unauthorized distribution of copyrighted material. *See Grokster*, 545 U.S. at 918–20, 125 S. Ct. at 2770–71; *see also* Clyde Haberman, *Grappling with the 'Culture of Free' in Napster's Aftermath*, N.Y. TIMES (Dec. 7, 2014), https://www.nytimes.com/2014/12/08/technology/grappling-with-the-culture-of-free-in-napsters-aftermath.html?_r=0; Josh Halliday, *LimeWire Shut Down by Federal Court*, GUARDIAN (Oct. 27, 2010), https://www.theguardian.com/technology/2010/oct/27/limewire-shut-down.

Task Force. About a month before the GBI searched Carroll's home, an agent tapped into the Ares network and discovered twenty-two "files of interest"[2] that were being shared from Carroll's IP address. Disguised as an Ares peer, the agent downloaded two videos directly from Carroll's computer, both of which contained child pornography. After tracing the IP address to Carroll's internet service account registered to his home in Newnan, the GBI sought out and received a warrant from the Georgia Superior Court, which it executed at Carroll's home on the morning of October 22.

Eight months later, a federal grand jury charged Carroll with one count of knowingly distributing a visual depiction of a minor engaged in sexually explicit conduct, 18 U.S.C. § 2252(a)(2), (b)(1), and one count of knowingly possessing a visual depiction of a minor engaged in sexually explicit conduct, 18 U.S.C. § 2252(a)(4)(B), (b)(2). Carroll filed a motion to suppress the evidence seized from his home, which the district court denied. A jury found Carroll guilty on both counts and made a special finding that Carroll possessed materials involving the sexual exploitation of a minor under the age of twelve. At sentencing, the district court applied five Guidelines enhancements, finding that: (1) the images depicted

[2] The GBI matched the Secure Hash Algorithm Version 1 (SHA-1) values of these files with the SHA-1 values of files known to contain child pornography. An SHA-1 value is a digital fingerprint unique to each file, which provides a means of identification that is extremely accurate and difficult to alter. The GBI, in cooperation with other agencies throughout the country, keeps a list of the SHA-1 values of known child pornography series. This allows it to cross-check the SHA-1 values in search results with its list to identify files of interest.

minors under twelve; (2) the images portrayed sadistic or masochistic conduct or violence; (3) the offense involved 600 or more images; (4) the offense involved use of a computer service; and (5) Carroll's testimony at trial obstructed justice. This produced a guideline range of 210 to 262 months; the district court sentenced Carroll to 150 months' imprisonment.

II.

We review de novo whether a search warrant is supported by probable cause, accepting the factual findings of the district court unless clearly erroneous. *United States v. Brundidge*, 170 F.3d 1350, 1352 (11th Cir. 1999) (per curiam). Likewise, we review de novo whether a warrant lacked the particularity required by the Fourth Amendment. *United States v. Bradley*, 644 F.3d 1213, 1258–59 (11th Cir. 2011). "We review the sufficiency of evidence to support a conviction de novo, viewing the evidence in the light most favorable to the government and drawing all reasonable inferences and credibility choices in favor of the jury's verdict." *United States v. Taylor*, 480 F.3d 1025, 1026 (11th Cir. 2007).

We review the district court's application of the Guidelines de novo and its findings of fact for clear error. *United States v. Smith*, 231 F.3d 800, 806 (11th Cir. 2000). Because Carroll argues for the first time on appeal that the district court erred in applying a sentencing enhancement for possession of more than 600

images involving the sexual exploitation of a minor, U.S.S.G. § 2G2.2(b)(7), we will review the application of that enhancement for plain error. *United States v. Rodriguez*, 398 F.3d 1291, 1298 (11th Cir. 2005). Plain error review requires a showing that (1) there was an error; (2) it was plain; (3) it affected substantial rights; and (4) it seriously affected the fairness, integrity, or public reputation of judicial proceedings. *Id.*

III.

Our discussion is divided into three parts. First, we address whether the warrant authorizing the search of Carroll's home met the requirements of the Fourth Amendment. Next, we consider the sufficiency of the evidence to support his possession and distribution convictions. Third, and finally, we review his sentence.

A.

We turn first to Carroll's claim that the district court erred in denying his motion to suppress the evidence obtained from his home. Carroll argues both that the warrant was unsupported by probable cause and that it abridged the Fourth Amendment's particularity requirement.

"Probable cause to support a search warrant exists when the totality of the circumstances allow[s] a conclusion that there is a fair probability of finding contraband or evidence at a particular location." *Brundidge*, 170 F.3d at 1352.

"We give great deference to a lower court's determination of probable cause." *Bradley*, 644 F.3d at 1263. The Fourth Amendment also requires a warrant to "particularly describ[e] the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV. Thus, "[a] warrant which fails to sufficiently particularize the place to be searched or the things to be seized is unconstitutionally over broad," and any evidence seized from the resulting search must be excluded from trial. *United States v. Travers*, 233 F.3d 1327, 1329 (11th Cir. 2000). While a search warrant must contain sufficient specificity to guard against a general search, "the test is the reasonableness of the description. Elaborate specificity is unnecessary." *United States v. Strauss*, 678 F.2d 886, 892 (11th Cir. 1982).

We find that the evidence contained in the affidavit supporting the warrant, in conjunction with the testimony of the investigating agents, strongly supported a conclusion that evidence of child pornography would be found at Carroll's home. The affiant, GBI Agent Sara Thomas, had seven years of experience in the GBI and was specially trained in computer investigations involving crimes against children. In the affidavit, she explained how the file sharing program Ares works and detailed how the GBI used Ares to download two files of interest—identified by their SHA-1 values as known child pornography files—from an IP address traced to Carroll's internet service provider. Agent Thomas then testified that she

viewed the two video files, and that she "knows from training and experience both to contain images of child pornography." She supported this conclusion with a description of the videos' SHA-1 values and file names:

> 1. !new pthc dark studio]227.mpg !
>
> 2. new ! (pthc) veronika little sister bj and cum inside mouth.wmv

She then explained how the acronym "PTHC," contained in both file names, stands for "pre-teen hard core," and is commonly used in searches to identify child pornography files.

Carroll contends that the Superior Court wholly abandoned its role in accepting these allegations without further scrutiny of the content of the files. We disagree. The Supreme Court has made it clear that an issuing magistrate is not required to personally view obscene material in order to make a probable cause determination. *See New York v. P.J. Video, Inc.*, 475 U.S. 868, 874 n.5, 106 S. Ct. 1610, 1614 n.5 (1986); *see also United States v. Smith*, 459 F.3d 1276, 1291 n.15 (11th Cir. 2006). And Agent Thomas, who possessed advanced technical proficiency and extensive experience investigating child exploitation, supported her testimony about the content of the videos with evidence of the matching SHA-1 values and graphic file names. While it may have been prudent to provide a more specific description of the content of the videos, we find that under these

circumstances the evidence and testimony contained in the affidavit supported a finding of probable cause.

We also conclude that the warrant satisfied the Fourth Amendment's particularity requirement. The warrant detailed the types of items to be seized at Carroll's home, all of which were reasonably tailored to the child pornography investigation. Carroll contends that the warrant permitted a general search of his home, but the warrant afforded the officers little latitude when it authorized the seizure of computers, related storage devices, and other media which might contain evidence of child pornography. The warrant was supported by probable cause, and the warrant reasonably described the place to be searched and the items to be seized. Accordingly, we affirm the denial of the motion to suppress the evidence seized during its execution.

B.

Next, we address Carroll's sufficiency of the evidence claims. Under 18 U.S.C. §§ 2552(a)(2) and 2552(a)(4)(B), it is unlawful for any person to knowingly possess or distribute, using any means or facility of interstate commerce, a visual depiction of a minor engaging in sexually explicit conduct. Carroll concedes that images depicting minors engaged in sexually explicit conduct were shared from his computer. The only issues before us are whether Carroll *knowingly* possessed and *knowingly* distributed those images.

1. Possession

Carroll first argues that because the child pornography files were discovered in the unallocated space of his computer when seized by the GBI, he cannot be held liable for knowingly possessing them without some further proof that he had the technological savvy to access them. He likens his case to several from our sister circuits that involved unwitting defendants whose computers automatically cached images from websites. *See United States v. Dobbs*, 629 F.3d 1199 (10th Cir. 2011); *United States v. Kuchinski*, 469 F.3d 853 (9th Cir. 2006). We are unconvinced by the comparison, and find that the evidence supports a conclusion that Carroll knowingly possessed the files found on his computer.

Child pornography was regularly downloaded to Carroll's Dell laptop over an eleven-month period. Carroll was home with exclusive control of his laptop during much of that time. Carroll lived alone. The only other people with access to his house were his mother and, on limited occasions, a cat sitter. The record shows that Carroll's Dell laptop was used to download child pornography on the same day it was used to file Carroll's tax return, that Carroll was travelling and without internet service during a notable gap in the sequence of child pornography downloads, and that Carroll's cat sitter did not know the password to the Dell laptop.

This is not a case of errant Googling and undetectable automatic-cache functions. *Cf. Dobbs*, 629 F.3d at 1204; *Kuchinski*, 469 F.3d at 862–63. Child pornography files were deliberately downloaded to the computer's hard drive. Obtaining the files required the predicate *manual* acts of downloading a peer-to-peer file sharing program, searching for files on the peer-to-peer network (using terms like "PTHC" calculated to return child pornography results), and then initiating—on 379 occasions—a file download. Carroll's argument—that he cannot be held liable for possessing the files because the files were deleted—asks us to create a perverse safe harbor for those in possession of child pornography. It also misses the point. The evidence proves that hundreds of images and videos of child pornography were manually downloaded and readily accessible while Carroll had exclusive control over his computer. Unlike in the cases on which Carroll relies, this evidence is probative of the question of knowing possession. *Cf. Dobbs*, 629 F.3d at 1205. Accordingly, we affirm his Section 2552(a)(4)(B) conviction.

2. Distribution

The distribution conviction is another matter. Carroll argues that the government failed to present any evidence that he knew he was sharing child pornography files when they were automatically placed in a shared folder, and that

he cannot be held liable for knowing distribution without some showing that he consciously allowed others to access those files. We agree.

Knowingly placing or leaving files in a shared folder connected to a peer-to-peer network undoubtedly constitutes distribution under 18 U.S.C. § 2252(a)(2). But Congress elected to proscribe only those acts of distribution that are accomplished with the requisite state of mind, and it is the government's burden to prove the statute's knowledge requirement beyond a reasonable doubt. This it did not do.

Nothing in the record demonstrates that Carroll intended to share files or that he was even aware that the contents of his Ares folder were automatically distributed to the peer-to-peer network. *See United States v. Chiaradio*, 684 F.3d 265, 282 (1st Cir. 2012) ("When an individual consciously makes files available for others to take and those files are in fact taken, distribution has occurred."). Instead, the government argues that Carroll was guilty of knowing distribution simply because he was using a peer-to-peer file sharing program and "that is what it is." But the fact that files were automatically shared from Carroll's Ares folder, without some evidence of his awareness of it, cannot carry the government's burden to prove knowing distribution beyond a reasonable doubt. And while indicia of knowledge surely may be gleaned from the nature of a peer-to-peer program itself, here, the government failed to put on any evidence that Ares, by

design, would have required Carroll to authorize file sharing or in any way recognize that his downloaded files were being shared. To the contrary, the government's own witness, former GBI agent Joel Cancilla, testified that Ares, by default, installs a shared folder, automatically places downloaded files into that folder, and distributes all contents of the shared folder to anyone else on the Ares network without prompting the user—even when the user is away from his computer.

In spite of this, the government asks us to hold that it would be impossible for an individual to use a peer-to-peer file sharing program and lack a full understanding of its operations. We think it unwise to adopt such a sweeping rule in this fact-sensitive context, where the mechanics of each peer-to-peer program may bear on the issue of knowledge in different ways. We recognize that in certain cases, the very design of the peer-to-peer program may foreclose any possibility that the user unwittingly shared files. It would be difficult to claim ignorance where, for example, the peer-to-peer program prompts the user during installation to choose whether or not he wants to share downloaded files, *see United States v. Spriggs*, 666 F.3d 1284, 1286–87 (11th Cir. 2012), requires the user to authorize file sharing for each particular peer that requests it, *see United States v. McElmurry*, 776 F.3d 1061, 1065 (9th Cir. 2015), or forces the user to acknowledge and accede to a licensing agreement explaining the peer-to-peer

process and then involves the user in setting up a shared folder, *see United States v. Shaffer*, 472 F.3d 1219, 1221 (10th Cir. 2007).[3] But according to this record, Ares has none of these characteristics, Carroll took none of these actions, and the government provided no other basis for his knowledge of distribution.[4] Thus to accept the government's argument, under these facts, would be to hold Carroll strictly liable. We refuse to do so. Without some proof that the defendant consciously shared files, either by authorizing their distribution or knowingly making them available to others, he cannot be held liable for knowing distribution under Section 2552(a)(2). And because no such proof was offered here, we must reverse Carroll's Section 2552(a)(2) conviction.

C.

Finally, we review the application of two Guidelines enhancements to Carroll's sentence: the U.S.S.G. § 2G2.2(b)(7) enhancement for possession of more than 600 images involving the sexual exploitation of a minor, and the

[3] While analysis of peer-to-peer file distribution under 18 U.S.C. § 2552(a)(2) and the U.S.S.G. § 2G2.2(b)(3)(F) sentencing enhancement is similar, the two do not completely overlap. U.S.S.G. § 2G2.2(b)(3)(F) can be applied based on a preponderance of the evidence, is reviewed for clear error, and, prior to a 2016 amendment, did not have a mens rea requirement. *See* U.S.S.G. Suppl. To App. C, amend. 801 (2016). Thus, we refuse the government's request to apply the rule in *United States v. Dodd*, 598 F.3d 449, 451–52 (8th Cir. 2010), that "[a]bsent concrete *evidence* of ignorance . . . a fact-finder may reasonably infer that the defendant knowingly employed a file sharing program for its intended purpose," to the substantive offense in 18 U.S.C. § 2552(a)(2), which places the burden on the government to prove knowing distribution beyond a reasonable doubt.

[4] We also note that the government did not put forth evidence that Carroll had some advanced technological proficiency that might have rendered his ignorance to the file sharing process implausible. *Cf. United States v. Richardson*, 713 F.3d 232, 234 (5th Cir. 2013) (defendant was a computer technician and admitted that he knew his shared folder was available to others).

U.S.S.G. § 2G2.2(b)(4) enhancement because the offense involved images portraying sadistic or masochistic conduct or other depictions of violence.

Carroll concedes that 314 images and 65 videos amount to 5,189 images under the Guidelines. *See* U.S.S.G. § 2G2.2(b)(7). Instead of contesting this calculation, he repeats his argument that he did not possess the images at all because they were located in the unallocated space of his computer at the time it was seized. We reject this theory for the same reasons that we did above. The evidence proved that the images were manually downloaded to Carroll's hard drive while Carroll had exclusive control of his laptop, and that they were readily accessible and viewable prior to being deleted. There is no question that they involved the sexual exploitation of minors. Accordingly, the district court did not err in applying the enhancement for possession of more than 600 such images.

Next, Carroll argues that depictions of minors engaged in sex acts with adults do not amount to sadistic or masochistic conduct without some additional evidence of intentional infliction of physical abuse, and, therefore, that the application of the Section 2G2.2(b)(4) enhancement to his offense constitutes impermissible double counting. The videos found on Carroll's computer depicted vaginal and anal penetration of girls under the age of twelve, as well as one video of a young girl tied up. We have held that both "adult men's vaginal and anal penetration of children [under twelve]" and "pictures of minors in bondage are

sufficient to warrant the sadistic conduct enhancement." *United States v. Caro*, 309 F.3d 1348, 1351–52 (11th Cir. 2002).

This was not double counting. The base offense punishes possession of images containing any sexual exploitation of a minor of any age, while the enhancement applied here increased the punishment because Carroll's images involved particular, violent sexual acts against children less than twelve years old, including at least one depiction of bondage. *United States v. Dudley*, 463 F.3d 1221, 1226–27 (11th Cir. 2006) ("Impermissible double counting occurs only when one part of the Guidelines is applied to increase a defendant's punishment on account of a kind of harm that has already been fully accounted for by application of another part of the Guidelines."). No doubt, these harms were not fully accounted for in the base offense. Accordingly, we affirm the application of the Section 2G2.2(b)(4) enhancement.

IV.

In conclusion, we affirm the denial of the motion to suppress the evidence seized from Carroll's home, we affirm his conviction for knowingly possessing a visual depiction of a minor engaged in sexually explicit conduct, 18 U.S.C. § 2252(a)(4)(B), and we affirm the application of the Guidelines enhancements for possession of more than 600 images involving the sexual exploitation of a minor, U.S.S.G. § 2G2.2(b)(7), some of which involved sadistic or masochistic acts and

violence, U.S.S.G. § 2G2.2(b)(4). We reverse Carroll's conviction for knowingly distributing a visual depiction of a minor engaged in sexually explicit conduct, 18 U.S.C. § 2252(a)(2), and we remand to the district court for resentencing consistent with this opinion.

AFFIRMED IN PART, REVERSED IN PART, AND REMANDED.