FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,
            Plaintiff-Appellee,

v.

CHARLES A. BOROWY,
            Defendant-Appellant.

No. 09-10064

D.C. No.
3:08-cr-00007-LRH-
VPC-1

OPINION

Appeal from the United States District Court
for the District of Nevada
Larry R. Hicks, District Judge, Presiding

Argued and Submitted
November 4, 2009—San Francisco, California

Filed February 17, 2010

Before: Betty B. Fletcher, William C. Canby, Jr., and
Susan P. Graber, Circuit Judges.

Per Curiam Opinion

COUNSEL

Michael K. Powell, Assistant Federal Public Defender, Reno, Nevada, for defendant/appellant Charles A. Borowy.

Elizabeth A. Olson, Assistant United States Attorney, Reno, Nevada, for plaintiff-appellee United States of America.

OPINION

PER CURIAM:

Defendant Charles A. Borowy appeals the denial of his motion to suppress and seeks to vacate his guilty plea because of a violation of Rule 11 of the Federal Rules of Criminal Procedure. He argues that the evidence recovered by an FBI agent who accessed his shared files on the peer-to-peer file-sharing service LimeWire was unconstitutionally obtained and that the district court should have suppressed this evidence. He argues further that, because he was misinformed as to the term of supervised release to which he was subject, this court should vacate his guilty plea. We have jurisdiction under 28 U.S.C. § 1291 and affirm.

I. Background

On May 3, 2007, Special Agent Byron Mitchell logged onto LimeWire, a publically available peer-to-peer file-sharing computer program, to monitor trafficking in child pornography. Agent Mitchell conducted a keyword search in LimeWire using the term "Lolitaguy," a term known to be associated with child pornography. From the list of results

returned by this search, Agent Mitchell identified known images of child pornography using a software program that verifies the "hash marks" of files and displays a red flag next to known images of child pornography. At least one of these files was shared through what was later determined to be Borowy's IP address. Using the "browse host" feature of LimeWire, Agent Mitchell viewed a list of the names of all of the approximately 240 files being shared from Borowy's IP address, several of which were explicitly suggestive of child pornography and two of which were red-flagged. Agent Mitchell downloaded and viewed seven files from Borowy's IP address, four of which were child pornography. Prior to downloading the files, Agent Mitchell did not have access to the files' contents. Execution of a search warrant resulting from Agent Mitchell's investigation led to the seizure of Borowy's laptop computer, CDs, and floppy disks. Forensic examination of these items revealed more than six hundred images of child pornography, including seventy-five videos.

Borowy moved to suppress this evidence, arguing that Agent Mitchell's activities in locating and downloading the files from LimeWire constituted a warrantless search and seizure without probable cause that violated Borowy's Fourth Amendment rights. Borowy argued that because he had purchased and installed a version of LimeWire that allows the user to prevent others from downloading or viewing the names of files on his computer and because he attempted to engage this feature, he had a reasonable expectation of privacy in the files. However, for whatever reason, this feature was not engaged when Agent Mitchell downloaded the seven files from Borowy's computer, and there was no restriction on Agent Mitchell's accessing those files.[1] The district court refused to suppress the evidence, finding that Agent Mitchell's conduct was not a search under the Fourth Amendment

---

[1]Borowy asserts that this feature was not engaged because rebooting the computer caused it to reset to its default setting of sharing files. This explanation is not supported by evidence in the record.

and that Agent Mitchell had probable cause to download the files.

Borowy conditionally pleaded guilty to possession of child pornography under 18 U.S.C. § 2252A(a)(5)(B), reserving his right to appeal the suppression decision. The plea memorandum, the district court, and counsel for both the government and the defense initially informed Borowy that the maximum term of supervised release for this crime was not more than three years. However, at the beginning of Borowy's sentencing hearing, the district court and Borowy's attorney correctly noted that the relevant statute calls for a period of supervised release ranging from five years to life. *See* 18 U.S.C. § 3583(k). Borowy concedes that he made no objection at sentencing that he had been misinformed as to the supervised release term. Borowy was sentenced to forty-five months of imprisonment followed by lifetime supervised release.

II.   Discussion

A.   Motion to Suppress

We review motions to suppress de novo and a trial court's factual findings for clear error. *United States v. Howard*, 447 F.3d 1257, 1262 n.4 (9th Cir. 2006). We review de novo a district court's determination of probable cause to search. *United States v. Davis*, 530 F.3d 1069, 1077 (9th Cir. 2008).

[1] Under *Katz v. United States*, 389 U.S. 347 (1967), government conduct qualifies as a search only if it violates a reasonable expectation of privacy. Whether Agent Mitchell engaged in an unconstitutional search and seizure is largely controlled by *United States v. Ganoe*, 538 F.3d 1117, 1127 (9th Cir. 2008), *cert. denied*, 129 S.Ct. 2037 (2009), which held that the defendant's expectation of privacy in his personal computer could not "survive [his] decision to install and use file-sharing software, thereby opening his computer to anyone else with the same freely available program." This

result is consistent with that of other circuits that have considered the issue. *See United States v. Stults*, 575 F.3d 834, 842-43 (8th Cir. 2009) (citing *Ganoe*), *petition for cert. filed* __ U.S.L.W. __ (U.S. Dec. 11, 2009) (No. 09-8153); *United States v. Perrine*, 518 F.3d 1196, 1204-05 (10th Cir. 2008).

[2] Borowy argues that his case is distinguishable from *Ganoe* because of his ineffectual effort to prevent LimeWire from sharing his files. However, as in *Ganoe*, "[t]he crux of [Borowy's] argument is that he simply did not know that others would be able to access files stored on his own computer" and that, although Borowy intended to render the files private, his "technical savvy" failed him. *Ganoe*, 538 F.3d at 1127. Borowy, like Ganoe, was clearly aware that LimeWire was a file-sharing program that would allow the public at large to access files in his shared folder unless he took steps to avoid it. *See id.*; *see also United States v. Heckenkamp*, 482 F.3d 1142, 1147 (9th Cir. 2007) ("[P]rivacy expectations may be reduced if the user is advised that information transmitted through the network is not confidential and that [others] may monitor communications transmitted by the user."). Despite his efforts, Borowy's files were still entirely exposed to public view; anyone with access to LimeWire could download and view his files without hindrance. Borowy's subjective intention not to share his files did not create an objectively reasonable expectation of privacy in the face of such widespread public access. *See Ganoe*, 538 F.3d at 1127; *United States v. King*, 509 F.3d 1338, 1341-42 (11th Cir. 2007) (per curiam). Because Borowy lacked a reasonable expectation of privacy in the shared files, Agent Mitchell's use of a keyword search to locate these files did not violate the Fourth Amendment.

[3] Borowy also argues that the use of a "forensic software program" that is unavailable to the general public to confirm that the files contained child pornography rendered Agent Mitchell's conduct an unlawful Fourth Amendment search. We disagree. Borowy had already exposed the entirety of the contents of his files to the public, negating any reasonable

expectation of privacy in those files. *Cf. California v. Ciraolo*, 476 U.S. 207, 213-14 (1986) (finding the use of an aircraft to observe marijuana plants was not a Fourth Amendment search as it only revealed information accessible to any member of the public flying in the airspace); *cf. also Kyllo v. United States*, 533 U.S. 27, 40 (2001) ("Where, as here, the Government uses a device that is not in general public use, to explore details of the home *that would previously have been unknowable* without physical intrusion, the surveillance is a 'search' . . . .") (emphasis added). Moreover, the hash-mark analysis appears to disclose only whether the files in the list that Agent Mitchell's keyword search returned were known child pornography. *See United States v. Jacobsen*, 466 U.S. 109, 122-26 (1984); *United States v. Place*, 462 U.S. 696, 707 (1983) ("canine sniff" of luggage left in public place is not a Fourth Amendment search). In this context, the hash-mark analysis functioned simply as a sorting mechanism to prevent the government from having to sift, one by one, through Borowy's already publically exposed files.[2]

[4] Finally, Borowy argues, citing *Arizona v. Hicks*, 480 U.S. 321, 324-26 (1987), that by downloading the seven files to examine their contents, Agent Mitchell seized the files without probable cause in violation of the Fourth Amendment. *See also Soldal v. Cook County*, 506 U.S. 56, 68-69 (1992) (explaining that even in the absence of a search, seizures of property are subject to Fourth Amendment scrutiny). We need not resolve whether downloading a file constitutes

---

[2]Because we decide only the case in front of us, we reject Borowy's argument that our decision will allow unrestricted government access to all internet communications. We do not rule on whether, if confronted with different facts—for example, where the information was not already exposed to the public at large, where the hash-mark analysis might reveal more than whether a file is known child pornography, or where the government "vacuumed" vast quantities of data indiscriminately—we might find a Fourth Amendment violation. Here we are presented only with the limited case of a targeted search of publicly exposed information for known items of contraband.

a seizure of that file because the district court properly concluded that Agent Mitchell had probable cause. Probable cause "merely requires that the facts available to the officer would warrant a man of reasonable caution in the belief that certain items may be contraband or stolen property or useful as evidence of a crime." *Texas v. Brown*, 460 U.S. 730, 742 (1983) (internal quotation marks and citation omitted). As the district court noted, the file names for at least five of the files were explicitly suggestive of child pornography.[3] The list of these file names was obtained by searching for a term known to be associated with child pornography and two of the files were red-flagged as known child pornography. In light of this information, the district court correctly held that Agent Mitchell had probable cause to download the files.

B. Rule 11 Error

We conduct a plain error review of a Rule 11 violation to which no objection has been made. *See United States v. Benz*, 472 F.3d 657, 658-59 (9th Cir. 2006). To establish plain error the defendant must show "(1) error, (2) that is plain, (3) that affected substantial rights, and (4) that seriously affected the fairness, integrity or public reputation of the judicial proceedings." *Id.* at 659. The government concedes the first two elements of the plain error analysis. *See also* Fed. R. Crim. Proc. 11(b)(1)(H), (I). It disputes, however, that this error affected Borowy's substantial rights.

[5] To show that the error affected his substantial rights, Borowy must prove that there is a "reasonable probability that, but for the error, he would not have entered the plea." *United States v. Monzon*, 429 F.3d 1268, 1272 (9th Cir. 2005)

---

[3]Of the remaining two file names, it appears that the district court may have been exceedingly charitable as to at least one of them, which included the abbreviation "PTHC," in determining that it was not suggestive of child pornography. *See Stults*, 575 F.3d at 838 (explaining that "PTHC" is an abbreviation commonly associated with child pornography).

(internal quotation marks omitted). The inquiry includes " 'the overall strength of the Government's case and any possible defenses that appear from the record,' " " 'evidence tending to show that a misunderstanding was inconsequential to the defendant's decision, [and] evidence indicating the relative significance of other facts that may have borne on his choice regardless of any Rule 11 error.' " *Id.* (quoting *United States v. Dominguez Benitez*, 542 U.S. 74, 84-85 (2004)) (internal quotations marks omitted). "A defendant must thus satisfy the judgment of the reviewing court, informed by the entire record, that the probability of a different result is sufficient to undermine confidence in the outcome of the proceeding" but need not prove by a preponderance that the result would have been different. *Dominguez Benitez*, 542 U.S. at 83 & n.9 (internal quotation marks omitted).

Our sister circuits have reached divergent results when considering plain error Rule 11 violations on the basis of the same misinformation that was provided to Borowy. *Compare United States v. Rivera-Maldonado*, 560 F.3d 16, 21 (1st Cir. 2009) (finding this error affected the defendant's substantial rights) *with United States v. Luken*, 560 F.3d 741, 745 (8th Cir. 2009) (finding the error did not affect the defendant's substantial rights). While we are cognizant that the difference between a maximum three-year term of supervised release and a term of five years to life is substantial, we conclude that, on the facts of this case, Borowy has not shown that the error affected his substantial rights.

Perhaps the most revealing evidence on this point is that, at sentencing, Borowy cited the court's authority to impose lifetime supervised release as a factor the court should consider in reducing his prison term. Thus, rather than seeking to rectify or minimize the effect of the Rule 11 error by objecting at sentencing, arguing for a lesser term of supervised release, or seeking to withdraw his plea, *see United States v. Littlejohn*, 224 F.3d 960, 970-71 (9th Cir. 2000), Borowy actually attempted to turn the error to his advantage. Further-

more, because the district court correctly denied Borowy's suppression motion, the government had ample evidence of Borowy's possession of child pornography. *See Dominguez Benitez*, 542 U.S. at 85 ("When the record made for a guilty plea and sentencing reveals evidence, as this one does, showing both a controlled sale of drugs to an informant and a confession, one can fairly ask a defendant seeking to withdraw his plea what he might ever have thought he could gain by going to trial."). Borowy also received a substantial benefit from his guilty plea, which lowered the sentencing guideline range to 51 to 63 months rather than 70 to 87 months and resulted in the dismissal of Count One of the indictment, for which there is a 60 month statutory minimum sentence, *see* 18 U.S.C. § 2252A(b)(1); *Littlejohn*, 224 F.3d at 970-71.

[6] Given the strength of the government's case, the benefit that Borowy obtained by pleading guilty, and his focus on negotiating a lesser prison term, we conclude that Borowy has not demonstrated that the Rule 11 error affected his substantial rights.

AFFIRMED.