FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, *Plaintiff-Appellee,* v. MAX BUDZIAK, *Defendant-Appellant.*	No. 11-10223 DC No. CR 08-0284 RMW OPINION

Appeal from the United States District Court
for the Northern District of California
Ronald M. Whyte, Senior District Judge, Presiding

Argued and Submitted
July 17, 2012—San Francisco, California

Filed October 5, 2012

Before: A. Wallace Tashima, Richard R. Clifton, and
Mary H. Murguia, Circuit Judges.

Opinion by Judge Tashima

COUNSEL

Martine Cicconi, Criminal Division, U.S. Department of Justice, Washington, DC, for the plaintiff-appellee.

John J. Jordan, San Francisco, California, for the defendant-appellant.

OPINION

TASHIMA, Circuit Judge:

Max Budziak appeals his jury conviction on two counts of distributing child pornography in violation of 18 U.S.C.

§§ 2252(a)(2)(A) and 2252(b)(1), and one count of possessing child pornography in violation of 18 U.S.C. §§ 2252(a)(4)(B) and 2252(b)(2). Budziak contends that the evidence presented at trial was insufficient to convict him of distribution. He also asserts that the district court incorrectly instructed the jury on the definition of distribution, erroneously denied his motion for a new trial, and improperly denied him discovery on software that the Federal Bureau of Investigation ("FBI") used in its investigation into his online file-sharing activities. We have jurisdiction pursuant to 28 U.S.C. § 1291. We hold that the district court erred in denying Budziak's discovery requests, but deny the remainder of Budziak's challenges to his conviction.

I.

On June 6, 2007, FBI Special Agent Stacie Lane downloaded several images containing child pornography from an Internet Protocol ("IP") address registered to Max Budziak. On June 14, 2007, FBI Special Agent Richard Whisman conducted a search for child pornography on an online file-sharing network that led him to download 52 files from an IP address registered to Budziak. Both Lane and Whisman used an FBI computer program called "EP2P" to search for the child pornography files and to download them.

According to the FBI, EP2P is an enhanced version of LimeWire, a publicly available peer-to-peer file-sharing program that allows users to search for and download files stored on other users' computers. EP2P purportedly allows the FBI to view all files that a particular user on the file-sharing network is making available for download by other users at a given time. While the publicly available version of LimeWire typically downloads files by piecing together file fragments from multiple users, the enhanced EP2P software purportedly allows the FBI to download complete files from a single user.

Based on information he received from Agent Lane, FBI Special Agent Wade Luders obtained a warrant to search

Budziak's residence. On July 14, 2007, FBI agents executed the warrant. During their search of Budziak's home, agents discovered a desktop computer containing child pornography and an installed copy of the LimeWire program. The FBI seized the computer and conducted a forensic examination of its hard drive.

The FBI's examination of the hard drive revealed that five videos containing child pornography were saved on it in a folder labeled "shared." Files containing child pornography were also saved in other folders, including files containing two of the images Agent Lane had downloaded on June 6, and five of the images Agent Whisman had downloaded on June 14. None of the files had a creation date pre-dating July 2, 2007. The FBI also examined the "properties" file of the LimeWire software installed on Budziak's computer and concluded that the default settings had not been altered. LimeWire's default settings allow for file-sharing with other users.

On April 30, 2008, a grand jury returned an indictment charging Budziak with two counts of distribution of child pornography and one count of possession of material containing a visual depiction of a minor engaging in sexually explicit conduct. Budziak filed a motion to suppress, arguing that the affidavit supporting the warrant to search his residence contained false statements and material omissions about the LimeWire software and its uses. In response, the government submitted a declaration by Agent Luders, which outlined the differences between the publicly available LimeWire software and the FBI's EP2P program. The court denied Budziak's motion to suppress without prejudice, and instructed him to file a discovery motion if he wished to review the EP2P software. Budziak then filed three successive motions to compel, seeking discovery on the specifications of the FBI's EP2P software or a copy of the program. The district court denied each of those motions. Budziak subsequently filed a renewed motion to suppress, which the district court again denied.

The jury trial began on January 10, 2011. The government presented the testimony of Agents Lane, Whisman, and Luders who testified about their investigations and the search of Budziak's residence. Additionally, the government presented the testimony of Special Agent Michael Gordon, an expert witness on the use of EP2P in FBI investigations. Agent Gordon testified about the LimeWire program and its functions. He testified that LimeWire's default setting is to save files downloaded through the program into a "shared" folder, and to make files stored in that folder available for download by other users. He testified that LimeWire provides an option for users to disable the sharing function so other users cannot download their files. On cross-examination, he testified that it was possible that a user could accidentally share files through LimeWire that he wanted to keep private, if he was not familiar with the program. Agent Gordon also testified about the FBI's EP2P software and its capabilities. He testified that EP2P allows the FBI to download files from a single user, but it does not enable the FBI to override a user's settings to look at or download files not designated for sharing.

Budziak presented no witnesses at trial. At the close of the government's case in chief, Budziak moved for a judgment of acquittal as to the two distribution counts. The district court denied the motion. The jury convicted Budziak on all three counts alleged in the indictment. Prior to sentencing, Budziak filed a motion for a new trial or judgment of acquittal, based on juror misconduct. The district court denied the motion and sentenced Budziak to 60 months of imprisonment, followed by five years of supervised release.

II.

Budziak contends that there was insufficient evidence presented at trial to sustain his conviction for distribution of child pornography. We review the sufficiency of the evidence supporting a defendant's conviction de novo. *United States v.*

Green, 592 F.3d 1057, 1065 (9th Cir. 2010). We will affirm the conviction unless, viewing the evidence in the light most favorable to sustaining the verdict, no rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt. *United States v. Nevils*, 598 F.3d 1158, 1164 (9th Cir. 2010) (en banc).

[1] Budziak argues that evidence of a deliberate, affirmative action of delivery is required to support a conviction for distribution. According to Budziak, evidence that he stored child pornography in a shared folder that was accessible to other LimeWire users is insufficient to support a conviction for distribution because it is evidence of no more than passive possession. Although Budziak presents a question of first impression in this circuit, our sister circuits have considered — and rejected — the argument he asserts here. *See United States v. Chiaradio*, 684 F.3d 265, 281-82 (1st Cir. 2012); *United States v. Shaffer*, 472 F.3d 1219, 1223 (10th Cir. 2007); *see also United States v. Christy*, 65 M.J. 657, 664-65 (Army Ct. Crim. App. 2007).

In *Shaffer*, the defendant argued that there was insufficient evidence to convict him for distribution of child pornography because he did not actively transfer possession of any child pornography "by mail, e-mail, or handing it to another person." 472 F.3d at 1223 (internal quotation marks omitted). The Tenth Circuit disagreed, concluding that he engaged in distribution when he left images and videos containing child pornography on his computer and freely allowed other users to download those items through the file-sharing program Kazaa. *Id.* at 1223-24. The court compared Shaffer's distribution of child pornography to a self-service gas station owner's distribution of gasoline: "The owner may not be present at the station . . . . [a]nd neither the owner nor his or her agents may ever pump gas . . . . [but] we do not doubt for a moment that the gas station owner is in the business of 'distributing[ ]' . . . gasoline . . . ." *Id.* at 1223-24.

[2] Following the First, Eighth, and Tenth Circuits, we hold that the evidence is sufficient to support a conviction for distribution under 18 U.S.C. § 2252(a)(2) when it shows that the defendant maintained child pornography in a shared folder, knew that doing so would allow others to download it, and another person actually downloaded it. *Chiaradio*, 684 F.3d at 281-82; *United States v. Collins*, 642 F.3d 654, 656-57 (8th Cir. 2011); *Shaffer*, 472 F.3d at 1223. This definition of "distribution" is consistent with the plain meaning of the word. *Shaffer*, 472 F.3d at 1223 ("We have little difficulty in concluding that Mr. Shaffer distributed child pornography in the sense of having 'delivered,' 'transferred,' 'dispersed,' or 'dispensed' it to others.").

[3] We conclude that the evidence was sufficient to support the jury's finding that Budziak distributed files containing child pornography by maintaining them in a shared folder accessible to other LimeWire users. Although Budziak argues before this Court that he disabled the sharing function on his LimeWire software, he did not present evidence of that assertion to the jury. The government, on the other hand, presented evidence that file-sharing was enabled on Budziak's LimeWire program when they seized his computer; that there were multiple files containing child pornography in Budziak's shared folder when they seized the computer; that Budziak initially told FBI agents he had not changed the default settings on his LimeWire program; and that agents actually downloaded shared files containing child pornography from an IP address registered to Budziak in June 2007. Viewing the evidence in the light most favorable to the verdict, a reasonable jury could have found beyond a reasonable doubt that Budziak shared — and thus distributed — child pornography through LimeWire.

The evidence was also sufficient to support a finding that Budziak knew that he was sharing files containing child pornography. At trial, the government presented evidence indicating that Budziak was familiar with LimeWire and how it

functioned. It presented evidence that he had installed the latest version of the program; that he used the program to download files with some frequency; and that he knew enough about the program's functions to tell an FBI agent that he moved files out of the shared folder to other parts of his computer. A reasonable jury could have found beyond a reasonable doubt that Budziak's technical knowledge and familiarity with LimeWire demonstrated that he knew he was sharing files. *See Collins*, 642 F.3d at 656-57 (upholding distribution conviction where government presented evidence that defendant was knowledgeable about his computer); *United States v. Durham*, 618 F.3d 921, 928-29 (8th Cir. 2010) (distribution enhancement was not warranted because there was no evidence of defendant's knowledge that other LimeWire users could obtain files from his computer, nor evidence of his familiarity with the program).

III.

[4] Budziak contends that the instruction the district court gave to the jury on distribution was erroneous, because it did not require the jury to find that he personally took affirmative steps to send child pornography to another person. The government argues that this claim is unreviewable under the "invited error" doctrine because Budziak failed to object to the instruction before the district court. The "invited error" doctrine does not apply here. An error is "invited" and unreviewable only if a defendant "induced or caused the error," or if he "intentionally relinquished or abandoned a known right." *United States v. Perez*, 116 F.3d 840, 845 (9th Cir. 1997) (en banc). In contrast to other cases where we have found that the defendant invited an error in a jury instruction, the record here does not reflect that Budziak intentionally abandoned or rejected the element of the distribution instruction he now asserts the court should have included. *See United States v. Baldwin*, 987 F.2d 1432, 1437 (9th Cir. 1993) (government offered omitted instruction, but defendant rejected it); *United States v. Guthrie*, 931 F.2d 564, 567 (9th Cir. 1991) (trial

court offered to give omitted instruction, but defendant rejected the offer). We review the district court's instruction for plain error. *Perez*, 116 F.3d at 846.

[5] The district court instructed the jury that in order to find Budziak guilty, it would have to find that he "knowingly distributed" child pornography. The court defined "distribution" as "delivering, transferring, dispersing, or dispensing something to others," and instructed the jury that "[d]istribution includes allowing electronic access to an image or video stored on one's computer and then the image or video is downloaded by another person." The district court's instruction was not plainly erroneous. Until now, this Court had not yet resolved the issue of when the use of a file-sharing program constitutes "distribution." Accordingly, any error on the district court's part cannot be deemed to have been plain. *See United States v. Gonzalez-Aparicio*, 663 F.3d 419, 428 (9th Cir. 2011) ("To be plain, the error must be clear or obvious, and an error cannot be plain where there is no controlling authority on point and where the most closely analogous precedent leads to conflicting results." (internal quotation marks and citation omitted)). Moreover, the district court's definition of distribution comported with the Tenth Circuit's holding in *Shaffer*, 472 F.3d at 1223-24, which we adopt here.

IV.

Budziak argues that the district court erred in denying his motion for a new trial based on juror misconduct without holding an evidentiary hearing. We review the district court's ruling for abuse of discretion. *United States v. Ruiz Montes*, 628 F.3d 1183, 1187 (9th Cir. 2011); *United States v. Navarro-Garcia*, 926 F.2d 818, 822 (9th Cir. 1991).

Budziak's motion for a new trial or judgment of acquittal argued that more technically sophisticated members of the jury had improperly exposed other jurors to extraneous evidence. The affidavit Budziak attached to his motion alleged

the following facts: After the jury returned its verdict, two jurors spoke to defense counsel. They reported that during deliberations, several of the more "computer savvy" jurors speculated that Budziak may have re-installed his LimeWire program, which they suggested could explain the lack of forensic evidence of distribution of child pornography in June 2007.

When presented with an allegation of juror misconduct, a trial court should ordinarily hold an evidentiary hearing to hear admissible juror testimony and determine the precise nature of the extraneous information. *Ruiz Montes*, 628 F.3d at 1186. An evidentiary hearing is not required, however, if the court is able to determine without a hearing that the allegations if true would not warrant a new trial. *Navarro-Garcia*, 926 F.2d at 822. Here, the district court held that a new trial would not be warranted even assuming the truth of the allegations about the juror comments set forth in Budziak's motion.

[6] The court did not abuse its discretion in denying Budziak's motion. The alleged juror comments referred not to extraneous evidence, but to the jurors' personal life experiences with computers and with the LimeWire program. It is well established that "a juror's past personal experiences may be an appropriate part of the jury's deliberations." *Grotemeyer v. Hickman*, 393 F.3d 871, 879 (9th Cir. 2004) (quoting *Navarro-Garcia*, 926 F.2d at 821 (internal quotation marks omitted)); *see also Price v. Kramer*, 200 F.3d 1237, 1255-56 (9th Cir. 2000) (jurors' accounts of their own experiences with the police did not constitute extraneous evidence); *Hard v. Burlington N. R.R. Co.*, 812 F.2d 482, 486 (9th Cir. 1987) ("Jurors must rely on their past personal experiences when hearing a trial and deliberating on a verdict."). The district court correctly determined that the alleged juror conduct was not a legitimate subject of inquiry under the Federal Rules of Evidence. *See* Fed. R. Evid. 606(b) (prohibiting admission of juror testimony about jury deliberations, except

for evidence of extraneous prejudicial information); *Hard*, 812 F.2d at 485-86.

V.

Budziak contends that the district court erred in denying him discovery on the FBI's EP2P software. We review the district court's Rule 16 discovery rulings for abuse of discretion. *United States v. Stever*, 603 F.3d 747, 752 (9th Cir. 2010).

[7] Under Rule 16, a criminal defendant has a right to inspect all documents, data, or tangible items within the government's "possession, custody, or control" that are "material to preparing the defense." Fed. R. Crim. P. 16(a)(1)(E). Evidence is "material" under Rule 16 if it is helpful to the development of a possible defense. *United States v. Olano*, 62 F.3d 1180, 1203 (9th Cir. 1995). A defendant must make a "threshold showing of materiality" in order to compel discovery pursuant to Rule 16(a)(1)(E). *United States v. Santiago*, 46 F.3d 885, 894 (9th Cir. 1995). "Neither a general description of the information sought nor conclusory allegations of materiality suffice; a defendant must present facts which would tend to show that the Government is in possession of information helpful to the defense." *United States v. Mandel*, 914 F.2d 1215, 1219 (9th Cir. 1990).

[8] Budziak argues that he made a sufficient showing that discovery of the EP2P software was material to preparing his defense. We agree. All three of Budziak's motions to compel provided more than a general description of the information sought; they specifically requested disclosure of the EP2P program and its technical specifications. Budziak also identified specific defenses to the distribution charge that discovery on the EP2P program could potentially help him develop. In support of his first two motions to compel, Budziak presented evidence suggesting that the FBI may have only downloaded fragments of child pornography files from his "incomplete"

folder, making it "more likely" that he did not knowingly distribute any complete child pornography files to Agents Lane or Whisman. *Stever*, 603 F.3d at 753. In support of his third motion to compel, Budziak submitted evidence suggesting that the FBI agents could have used the EP2P software to override his sharing settings.

[9] In *United States v. Cedano-Arellano*, 332 F.3d 568 (9th Cir. 2003), we held that the defendant was entitled to discovery on the narcotics detector dog that "alerted" on his gas tank, *id*. at 570, because materials on the dog's qualifications "were crucial to his ability to assess the dog's reliability, a very important issue in his defense, and to conduct an effective cross-examination of the dog's handler." *Id.* at 571. Similarly, access to the EP2P software was crucial to Budziak's ability to assess the program and the testimony of the FBI agents who used it to build the case against him. Like the competency of the drug-sniffing dog in *Cedano-Arellano*, the functions of the EP2P software constituted a "very important issue" for Budziak's defense. Given that the distribution charge against Budziak was premised on the FBI's use of the EP2P program to download files from him, it is logical to conclude that the functions of the program were relevant to his defense. *Cf. Stever*, 603 F.3d at 753.

Much of the evidence the prosecution presented at trial was devoted to describing EP2P and the FBI's use of the program. Although Budziak had an opportunity to cross-examine the government's EP2P expert, he was denied background material on the software that could have enabled him to pursue a more effective examination. As the Third Circuit has held, "A party seeking to impeach the reliability of computer evidence should have sufficient opportunity to ascertain by pretrial discovery whether both the machine and those who supply it with data input and information have performed their tasks accurately." *United States v. Liebert*, 519 F.2d 542, 547-48 (3d Cir. 1975); *see also United States v. Dioguardi*, 428 F.2d 1033, 1038 (2d Cir. 1970) ("It is quite incomprehensible that

the prosecution should tender a witness to state the results of a computer's operations without having the program available for defense scrutiny and use on cross-examination if desired.").

[10] Although the government argued that the computer logs it provided Budziak demonstrated that he would not uncover any helpful information through discovery of the software, the declarations of Budziak's computer forensics expert stated otherwise.[1] In cases where the defendant has demonstrated materiality, the district court should not merely defer to government assertions that discovery would be fruitless. While we have no reason to doubt the government's good faith in such matters, criminal defendants should not have to rely solely on the government's word that further discovery is unnecessary. This is especially so where, as here, a charge against the defendant is predicated largely on computer software functioning in the manner described by the government, and the government is the only party with access to that software. Accordingly, we hold that it was an abuse of discretion for the district court to deny Budziak discovery on the EP2P program.

[11] To win reversal of his conviction, Budziak must show not only that the district court abused its discretion, but also that there is a likelihood that the outcome of the trial would have been different if discovery had been granted. *Stever*, 603 F.3d at 754 (citing *United States v. Chon*, 210 F.3d 990, 994-95 (9th Cir. 2000)). "This he cannot do, because the Govern-

[1]This evidence distinguishes the instant case from *Chiaradio*, where the First Circuit held that the defendant could not demonstrate prejudice resulting from nondisclosure of the EP2P source code. 684 F.3d at 277. In *Chiaradio*, the defendant "neither contradicted nor cast the slightest doubt upon" the government's testimony that the materials it had already provided to him verified that an FBI agent downloaded files containing child pornography from his computer. *Id.* In contrast, Budziak presented arguments and evidence suggesting that the materials disclosed by the FBI did not resolve all questions relevant to his defense.

ment has never surrendered the materials for review." *Id*. Because the EP2P evidence Budizak requested is not part of the appellate record, it is impossible for us to determine whether the result of Budziak's trial would have been different if it had been disclosed to him. *Id.* ("Without the actual material, there is no way to judge prejudice.")*; cf. United States v. Alvarez*, 358 F.3d 1194, 1209 (9th Cir. 2004) ("In this situation, it is impossible for us to determine whether the trial court abused its discretion by failing to release information in the files, because the files are not part of the appellate record."); *United States v. Bernal-Obeso*, 989 F.2d 331, 336 (9th Cir. 1993) ("Because neither we nor the trial court know what it is we are attempting to review, we cannot fulfill [our] responsibility on this record.").

[12] We therefore remand this case to the district court for a determination on whether the EP2P materials Budziak requested "in fact contain, or would have led to, information that might have altered the verdict." *Stever*, 603 F.3d at 754; *see also Pennsylvania v. Ritchie*, 480 U.S. 39, 57 (1987) ("Ritchie is entitled to have the [undisclosed evidence] reviewed by the trial court to determine whether it contains information that probably would have changed the outcome of his trial"); *Alvarez*, 358 F.3d at 1209 (following *Ritchie*). If the district court determines that the EP2P discovery could have affected the outcome of the trial, it shall order a new trial; if the court determines that the nondisclosure was harmless, it may reinstate the judgment of conviction. *Ritchie*, 480 U.S. at 58; *Alvarez*, 358 F.3d at 1209. We leave to the district court to determine in the first instance whether, on remand, a protective order or an *in camera* hearing is necessary to accommodate any law enforcement confidentiality concerns. *See United States v. Spires*, 3 F.3d 1234, 1238-39 (9th Cir. 1993).

VACATED and REMANDED.