NOT RECOMMENDED FOR PUBLICATION
File Name: 23a0341n.06

No. 22-5984

UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

FILED
Jul 25, 2023
DEBORAH S. HUNT, Clerk

UNITED STATES OF AMERICA, Plaintiff-Appellee, v. CHRISTOPHER ROBERT HARPER, Defendant-Appellant.	)	ON APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF TENNESSEE OPINION

Before: McKEAGUE, GRIFFIN, and MURPHY, Circuit Judges.

GRIFFIN, Circuit Judge.

Defendant Christopher Harper claims he had a right to examine confidential software law enforcement used to download child pornography from his computer to ensure that it performed as the government proclaimed. The district court denied his motion to compel, and a jury convicted him of possessing child pornography. On appeal, he challenges that denial and the sufficiency of the evidence supporting his conviction. We affirm.

I.

As part of an investigation into the distribution of child pornography, FBI special agent Stephen Lies used a software designed for law-enforcement purposes called "Torrential Downpour" to search the BitTorrent peer-to-peer file-sharing network for illicit materials. With that network "a typical user . . . [generally] receive[s] multiple pieces of a file from several different sources," but the software Lies used allowed him to conduct "single-source

downloads"—i.e., from a sole IP address. *See United States v. Clark*, 24 F.4th 565, 570 (6th Cir. 2022) (brackets omitted). Lies identified a computer offering for download several files with titles suggesting child pornography and was able to download a partial "video file [that] depicted a prepubescent female appearing to be under 12 years of age engaged in masturbating a male, vaginal sex, and the lascivious exhibition of the pubic area."

Lies traced the IP address to a house in Memphis, Tennessee, and interviewed its residents. He learned that Harper lived at the house when the video was downloaded. So Lies interviewed Harper, who both confirmed he used to live at that house and that he owned a laptop, which he agreed to make available to law enforcement. Lies searched the laptop and discovered—despite its having the operating system reinstalled (to perhaps clear it of incriminating evidence)—several deleted files indicative of child pornography. Those included numerous file names referencing child pornography, as well as searches conducted on the BitTorrent network that are "commonly used to search for image and video files depicting prepubescent minors engaged in sexually explicit conduct." Although the video Lies downloaded was not there, a deleted file with the same name was.

A grand jury indicted defendant on two counts: (1) distributing child pornography in violation of 18 U.S.C. § 2252(a)(2); and (2) possessing child pornography in violation of 18 U.S.C. § 2252(a)(4)(B). Before trial, Harper broadly moved to compel the government to produce an installable version of the Torrential Downpour software, as well as the user manual, training materials, and source code. A magistrate judge denied Harper's motion following an evidentiary hearing, which the district court adopted. A jury subsequently convicted defendant on the possession count, and the district court imposed a sixty-three month sentence.

II.

Harper first asserts the district court erroneously denied his motion to compel the production of information about Torrential Downpour. On abuse-of-discretion review, *United States v. Pirosko*, 787 F.3d 358, 365 (6th Cir. 2015), we discern no error meriting reversal.

The Federal Rules of Criminal Procedure require the government to produce, "[u]pon a defendant's request," all "data" and "documents" (among other things) that are "material to preparing the defense." Fed. R. Crim. P. 16(a)(1)(E)(i). But when the request seeks information cloaked in law enforcement privilege, we must weigh the competing interests of a defendant's articulated needs in receiving that information with the government's desire to protect it from disclosure. *Pirosko*, 787 F.3d at 365. Application of this balancing test means the government does not have "a blank check to operate its file-sharing detection software sans scrutiny," for the discovery of such materials ensures "that the government's investigative methods [are] reliable, both for individual defendants . . . and for the public at large." *Id.* at 366. Yet, given the sensitive nature of the government's investigative methods, we require a "defendant to produce some evidence of government wrongdoing." *Id.*

The district court concluded Harper did not satisfy this "wrongdoing" threshold. It did so by noting that Harper's expert, Richard Connor, admitted he had no "way to dispute or refute" Agent Lies's testimony, so he wanted access to the software "to see how it operated" and confirm it worked as advertised. Other than asserting that it would be "theoretically" possible for a virus to modify the government's software to render it suspect, Connor offered no evidence of governmental wrongdoing.

On review of this evidence, we cannot conclude the district court abused its discretion. Harper "has not shown that the government engaged in wrongdoing (the only way the evidence

could help his defense) in employing the technique. He commissioned an expert to evaluate the technique, but the expert could not identify any errors in the government's efforts." *United States v. Harney*, 934 F.3d 502, 508 (6th Cir. 2019); *accord Pirosko*, 787 F.3d at 366. And, as in *Harney*, the government offered for Connor "to conduct a forensic examination" of the data downloaded from Harper's computer, which would have "reveal[ed] the computer logs, show[n] when law enforcement officers connected to Harper's computer, and what files were downloaded." That offer went unclaimed. *See Harney*, 934 F.3d at 508 ("Nor did Harney to our knowledge try to use the information the United States offered to give him to show that the technique didn't operate as expected."). Left with "nothing more than conjecture about what the additional evidence might show," Harper "comes up short." *Id.*

Defendant resists this conclusion, asserting he demonstrated governmental wrongdoing because Lies ultimately downloaded only a portion of the video. With that fact, he argues *United States v. Budziak*, 697 F.3d 1105 (9th Cir. 2012), is instructive because the defendant there both "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," and "that the FBI agents could have used the . . . software to override his sharing settings." *Id.* at 1112 (citation omitted). But we see nothing in this record that indicates Lies's partial download of a video was in any way demonstrative of governmental wrongdoing. *See Pirosko*, 787 F.3d at 365 (similarly distinguishing *Budziak*). Without that showing, the district court did not abuse its discretion when it denied Harper's motion to compel.

III.

The only other issue on appeal is whether the government sufficiently proved the elements of possessing child pornography. A defendant claiming insufficient evidence "faces a high bar" on appeal. *United States v. Persaud*, 866 F.3d 371, 379–80 (6th Cir. 2017). This is because we must uphold a jury's conviction if, "after viewing the evidence in the light most favorable to the prosecution, *any* rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt." *Jackson v. Virginia*, 443 U.S. 307, 319 (1979). We can sustain a conviction based on circumstantial evidence alone, and the evidence need not disprove every hypothesis except that of guilt. *United States v. Lindo*, 18 F.3d 353, 357 (6th Cir. 1994). A sufficiency claim does not allow us to "weigh the evidence presented, consider the credibility of witnesses, or substitute our judgment for that of the jury." *United States v. Jackson*, 470 F.3d 299, 309 (6th Cir. 2006) (citation omitted). Rather, we "draw all available inferences and resolve all issues of credibility in favor of the jury's verdict." *Id.* (citation omitted).

Harper asserts the government failed to prove the Torrential Downpour software worked as Lies claimed and therefore "did not establish that a complete video was ever downloaded." This repackaging of his denial-of-discovery issue is not well taken. Here the jury heard how Special Agent Lies used the Torrential Downpour software to isolate the IP address of Harper's computer and download a video that "depicted the sexual abuse of a prepubescent child," which was played at trial. And it learned that, while the specific video was no longer on Harper's computer when searched, residual evidence of that video was recovered (along with many other files with names indicative of child pornography), and the video was accessed on the same day Lies downloaded it. Based on this and other evidence, any rational trier of fact could have found that Harper

"knowingly possesse[d]" a visual depiction of a "minor engaging in sexually explicit conduct." 18 U.S.C. § 2252(a)(4)(B).

IV.

We affirm the district court's judgment.