In the

United States Court of Appeals

For the Seventh Circuit

No. 20-3189

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

THOMAS J. OWENS,

Defendant-Appellant.

Appeal from the United States District Court for the
Eastern District of Wisconsin.
No. 18-cr-00157 — **William C. Griesbach**, *Judge*.

ARGUED SEPTEMBER 28, 2021 — DECIDED NOVEMBER 19, 2021

Before FLAUM, KANNE, and SCUDDER, *Circuit Judges*.

FLAUM, *Circuit Judge*. It is criminal "distribut[ion]" of child pornography within the meaning of 18 U.S.C. § 2252(a)(2) to knowingly make a file containing child pornography available for others to access and download via a peer-to-peer file-sharing network. *See United States v. Ryan*, 885 F.3d 449, 453 (7th Cir. 2018). The government has developed an investigative practice where it employs a confidential software program to participate in the peer-to-peer network and detect

and download child pornography files shared therein. Once a file is downloaded and its illicit contents verified, the government ascertains the IP address of the sharing user, contacts the Internet service provider to identify the residence associated with the IP address, obtains a search warrant, and seizes the suspect's electronics. Often, the downloaded file is then located on the suspect's device, and the government can verify that the file was indeed made available for downloading. Yet sometimes the file cannot be located on the device or there are questions about the defendant's sharing settings.

In the case before us now, Thomas Owens was arrested and charged with the distribution and possession of child pornography after a government investigator used such a program, Torrential Downpour Receptor ("TDR"), to download a video file containing child pornography from a folder shared via the BitTorrent network at an IP address later associated with Owens. Nonetheless, a forensic search of Owens's computer at the time he was arrested failed to locate the file on his computer. Owens moved to compel the production of information relating to the government's download of the file pursuant to Federal Rule of Criminal Procedure 16. The district court held an evidentiary hearing and denied the motion; Owens now appeals that decision after entering a guilty plea preserving that right.

Given that we review a district court's Rule 16 decision only for abuse of discretion, we reverse only if a defendant can demonstrate that the pretrial disclosure of the disputed evidence would have enabled the defendant "to substantially alter the quantum of proof in his favor." *United States v. Orzechowski*, 547 F.2d 978, 984–85 (7th Cir. 1976) (quoting

United States v. Marshall, 532 F.2d 1279, 1285 (9th Cir. 1976)). Because Owens falls short of meeting that burden, we affirm.

I. Background

A. The BitTorrent Network and Torrential Downpour Receptor

BitTorrent is a peer-to-peer file sharing network that is used to distribute large amounts of data over the Internet, such as movies, videos, music, and images. In contrast to a centralized network, which relies on a single server to provide an entire file directly to each user, peer-to-peer networks like BitTorrent enable users to download portions of a file from numerous other users simultaneously. In this way, BitTorrent users can avoid slow download speeds that occur as a result of the sharing server's restricted upload bandwidth. As the defense expert explained to the district court, because most individual Internet users' accounts provide for faster file download (using, for example, 200 megabits per second to stream Netflix on several TVs at once) than upload (using 30 to 50 megabits per second to, say, transfer photos to an online drive), the rate at which a file is downloaded from a single server is limited by the rate the file is uploaded from that server—and the upload rate is usually slow. Peer-to-peer networks circumvent this problem through multi-source downloads.

To download and share files over the BitTorrent network, a user must first install a BitTorrent software "client"—a program that allows the user to interface with the BitTorrent network. Then, as the district court pointed out, a user seeking a particular file on the BitTorrent network can search the Internet for a "torrent," which is a "text-file containing instructions

on how to find, download, and assemble the pieces of the image or video files the user wishes to view." *See United States v. Gonzales*, No. CR-17-01311, 2019 WL 669813, at *1 (D. Ariz. Feb. 19, 2019). Owens's expert also described a "torrent" as a "recipe for obtaining and assembling a given set of contents."

Once a user downloads the torrent corresponding to the file he is seeking, the user can open the torrent using the BitTorrent software client, and the BitTorrent network will match the initiating user with other users who have the same torrent. Upon being matched, the computers will engage in a "handshake" and exchange the "info hash"[1] associated with the torrent to confirm that it is the same one. Once that is verified, the initiating user's client software will download pieces of the target file from the other users and assemble them, producing the complete file. The client software then makes the now-complete file accessible to other BitTorrent users in a shared folder on the user's computer; it also "seeds" the file, querying the BitTorrent network and making outbound connections to IP addresses that are in need of the data just downloaded.

The BitTorrent client software used by the government in this case, TDR, is a modified version of the BitTorrent protocol. As the district court explained:

> TDR [was] … developed by law enforcement in conjunction with the University of

[1] The info hash is a string of letters and numbers that precisely and uniquely identifies the torrent. Each piece of the file also has its own "hash value" that must be matched to the information in the torrent before it is downloaded to the initiating user. Both the government's expert and Owens's agreed that if the hash value of two files matches up, then the chances are "astronomically small" that the two files are different.

> Massachusetts at Amherst. TDR acts as a BitTorrent user and searches the Internet for [IP] addresses offering torrents for known child pornography files. When such an IP address is found, the program connects to that address and attempts to download the child pornography. The program generates detailed logs of the activity and communications between the program and the IP address.

(citation and internal quotation marks omitted). Crucially, the district court noted, "[u]nlike traditional BitTorrent programs, TDR is designed to download files only from a single IP address—rather than downloading pieces of files from multiple addresses—and does not share those files with other BitTorrent users."

The software's capacity for single-source downloads is important because if the government "only downloaded fragments of child pornography files," it is "'more likely' that [the defendant] did not knowingly distribute any complete child pornography files." *See United States v. Budziak*, 697 F.3d 1105, 1112 (9th Cir. 2012) (citation omitted).

B. The Investigation into Owens's BitTorrent Activity

In May 2018, an investigator from the Oshkosh police department employed TDR to determine that Owens's IP address was associated with a torrent corresponding to a particular child pornography video. The investigator used TDR to perform a single-source download of the video two times: first on May 21 and again on May 22.

Another investigator viewed the downloaded video and verified that it contained child pornography. The filename of

the video is long, explicit, and accurately describes the content of the video. The government identified Owens as the owner of the suspect IP address, then obtained a search warrant on Owens's residence. During the search, which was carried out on June 28, agents found thousands of depictions of child pornography but were unable to locate the particular video file that had been twice downloaded.

The download of that file nevertheless forms the basis of the distribution charge against Owens. Owens was also charged with two counts of possession based on other files recovered during the search of his home.

C. Owens's Motion to Compel Discovery

Owens argues that the government's failure to locate the file on his computer is evidence that he may never have possessed or distributed that file. To gather ammunition to prove this theory, Owens filed a motion under Rule 16(a)(1)(E) to compel the government to produce TDR, its source code, and all supporting documents, such as user manuals, technical specifications, and white papers. Rule 16 requires the government to permit a defendant to inspect items within its possession, custody, or control if, as Owens asserts here, "the item is material to preparing the defense." Fed. R. Crim. P. 16(a)(1)(E).

The government produced logs generated by TDR that described the two downloads, as well as details about the investigating officer's training and experience with TDR. However, it opposed Owens's motion for additional information, asserting that the items requested were not material, and even so, they were properly excluded from discovery under the law enforcement investigatory privilege. *See Dellwood Farms, Inc.*

v. Cargill, Inc., 128 F.3d 1122, 1125 (7th Cir. 1997) (explaining that the law enforcement investigatory privilege balances "the need of the litigant who is seeking privileged investigative materials … against the harm to the government if the privilege is lifted"). The government argued that disclosure would result in irreversible harm to pending and ongoing criminal investigations.

1. Evidence Submitted

The district court held an evidentiary hearing on Owens's motion to compel. The court heard testimony from Owens's expert, Peyton Engel, an attorney at a law firm in Madison, Wisconsin, who has specialized in computer security for over a decade. Engel's past work included conducting forensic investigations and incident response. He testified in state court as an expert witness on at least ten occasions, and he previously worked with both the defense bar and law enforcement. The government also presented an expert witness, Detective Robert Erdely, who assisted in the creation of TDR (although he did not write its source code) and retired from the Pennsylvania State Police Computer Crime Unit. In addition to developing TDR, Erdely has numerous certifications in computer systems and forensics. Both experts explained how BitTorrent works, as well as how TDR interacts with the BitTorrent network, and each opined on the likelihood that the downloaded file had existed on Owens's computer. The government also offered exhibits based on the forensic search of Owens's computer.

Owens's expert explained why it would be "material to preparing [his] defense" to verify how TDR operates. Engel testified that all software has "bugs," and so without independent verification, he could not rule out the possibility that

TDR could produce a "false positive." In other words, TDR could have reported that it detected and downloaded a file containing child pornography from Owens's IP address when, in fact, it did not.

Several facts presented at the hearing raise concerns about a possible false positive in this case. First and foremost, the parties agree that the downloaded file was never located on Owens's devices. Additionally, Detective Erdely testified that TDR identifies a computer as "associated with" a contraband file if it possesses the torrent for that file, but that is not the same as possessing the file itself. Furthermore, Detective Erdely conceded that TDR is a "set it and forget it" program—after an investigator sets initial parameters, such as which torrent to search for, it runs on its own. Engel analogized this case to one involving a radar gun or breathalyzer, where defense attorneys are permitted to verify that the instruments were properly calibrated and operated correctly when such evidence forms the basis of a prosecution.

Engel also noted that TDR's download of the target file from Owens's IP address was faster than he would expect if TDR had truly conducted a single source download. Engel explained that, in his experience reviewing TDR logs, it was not uncommon for the logs to describe a single-source download that took hours, or even more than a day. Here, however, each download of the target file was very quick, "on the order of less than a minute or maybe even seconds." This raised the question whether TDR had actually engaged in a normal, multi-source download of the file.

The government introduced evidence to counter these facts. Detective Erdely testified that TDR is an exceedingly simple program, which makes it less likely to have buggy

code. He testified that TDR only had one bug in its lifetime relating to file downloads, and it was that the program did not account for filenames that exceeded 260 characters. Instead of resulting in a false positive, that issue simply shut down the program, and it was promptly fixed. Erdely also dismissed Engel's concern about the download speed, explaining that Owens's Internet service provider, AT&T U-verse, is known to have an extraordinarily large upload bandwidth, and the file at issue is relatively small.

The government also presented circumstantial evidence that the file was, in fact, on Owens's device at the time TDR performed the two downloads. First, logs produced by TDR indicate that the suspect computer was running the BitTorrent client software "BitComet 1.50," and the forensic examination of Owens's computer revealed that it installed BitComet 1.50 the day before TDR downloaded the file at issue. Second, the forensic examination of Owens's computer shows that twenty minutes after BitComet was installed, a torrent with an info hash matching the torrent of the file at issue was downloaded and loaded into Owens's BitComet program. And third, the "most recently used" folder on Owens's computer lists the filename of the video at issue. As noted above, this filename is long, explicit, and describes the file's content. The "most recently used" folder also reflects that the file was "used" during the time when investigators were downloading the file from Owens's IP address using TDR.

Detective Erdely also stated that a false positive would be practically impossible in this case, where the TDR program had logged matching info hashes relating to the torrent, as well as a hash value match for every downloaded piece of the

226-piece video file. Additionally, Erdely explained that, unlike an operator of a radar gun or breathalyzer, an investigator can only configure two settings in TDR, neither of which could generate a false positive. The investigator can (1) ensure that TDR will only connect with IP addresses from a particular geographical jurisdiction, and (2) determine which illicit torrents TDR will detect.

As for the investigative privilege invoked by the government, Detective Erdely testified that if a user is given a license to TDR, it will "expose[] each and every torrent file [the government is] investigating," a database that it has taken over eight years to compile. He also asserted that access to TDR would expose investigators' contact information and IP addresses that are the subject of active investigations.

Nonetheless, Owens has repeatedly emphasized that he is not seeking disclosures of torrents or hash values associated with known child pornography files. Owens also elicited testimony from Erdely that it is possible to run validation testing on TDR software using a benign file, that validation demonstrations have been performed for defense counsel in some cases, and that the FBI performed an independent validation of TDR's single-source download methodology. The government never offered Owens a validation demonstration or access to the FBI's independent validation.

2. The District Court's Denial

The district court denied Owens's motion to compel, concluding that he had not demonstrated materiality. It focused on Owens's assertion that all software has bugs, and it concluded that the claim boiled down to mere speculation that TDR could have logged a false positive in this case. The court

credited Erdely's testimony that (1) TDR is a simple program that is unlikely to have bugs, and (2) if a bug did occur, it would not result in a false positive.

In its materiality analysis, the court also accepted the government's circumstantial evidence that the target file had, at the time of the downloads, existed on Owens's computer. Given the evidence, the district court concluded that access to TDR would not enable Owens to "significantly alter the quantum of proof in his favor."

Turning to the law enforcement investigatory privilege, the district court found that providing access to TDR would expose thousands of torrents and hash values it has taken law enforcement years to amass and give criminals "the key to not get caught." Because it concluded that Owens failed to demonstrate materiality, the court concluded that this risk clearly weighed against ordering disclosure of TDR's inner workings. The district court did not explicitly consider whether there were ways to limit this risk, such as by limiting Owens's expert's access or entering a protective order.

The government dismissed the possession charges, and Owens entered a conditional guilty plea to the distribution charge, which preserved his right to appeal the denial of his motion to compel. The district court imposed the mandatory five-year minimum sentence of incarceration. *See* 18 U.S.C. § 2252(b)(1).

Owens now appeals.

II. Discussion

A. Standard of Review

Before we can reach the central question of this appeal, we must first resolve a dispute about the applicable standard of review.

Rule 16 requires the government to "permit the defendant to inspect and to copy … papers, documents, [and] data" within the government's control if they are "material to preparing the defense." Fed. R. Crim. P. 16(a)(1)(E). Evidence is material to preparing the defense if it would "significantly help[] in 'uncovering admissible evidence, aiding witness preparation, corroborating testimony, or assisting impeachment and rebuttal.'" *See United States v. Gaddis*, 877 F.2d 605, 611 (7th Cir. 1989) (quoting *United States v. Felt*, 491 F. Supp. 179, 186 (D.D.C. 1979)); *see also United States v. Naggs*, No. 18-CR-130, 2020 WL 5105792, at *1 (E.D. Wis. Aug. 31, 2020). In other words, there must be some indication that the disclosure of the disputed evidence would enable the defendant "to substantially alter the quantum of proof in his favor." *Orzechowski*, 547 F.2d at 984 (citation omitted); *see also United States v. Baker*, 453 F.3d 419, 425 (7th Cir. 2006) (quoting 2 Charles Alan Wright, Federal Practice and Procedure § 254 (3d ed. 2000)) (same). Notably, information may be material even if it is not exculpatory. *See United States v. Mackin*, 793 F.3d 703, 709–11 (7th Cir. 2015).

To compel discovery pursuant to Rule 16(a)(1)(E), a "defendant must make at least a *prima facie* showing that the requested items are material to his defense." *United States v. Thompson*, 944 F.2d 1331, 1341 (7th Cir. 1991). "This materiality standard normally 'is not a heavy burden.'" *United States*

v. Lloyd, 992 F.2d 348, 351 (D.C. Cir. 1993) (citation omitted); *see also United States v. Lucas*, 841 F.3d 796, 804 (9th Cir. 2016) (explaining that the *prima facie* showing of materiality is generally a "low threshold" (citation omitted)). However, "[n]either 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 [g]overnment is in possession of information helpful to the defense." *United States v. Clarke*, 979 F.3d 82, 97 (2d Cir. 2020) (quoting *United States v. Mandel*, 914 F.2d 1215, 1219 (9th Cir. 1990)), *cert. denied*, No. 20-7593, 2021 WL 1602723 (Apr. 26, 2021); *see also United States v. Caputo*, 373 F. Supp. 2d 789, 793 & n.1 (N.D. Ill. 2005) ("To make a *prima facie* showing, a defendant cannot rely on general descriptions or conclusory arguments, but must convincingly explain how [discovery] will significantly help him uncover admissible evidence, prepare witnesses, or corroborate, impeach, or rebut testimony.") (collecting cases).

Ordinarily, "[w]e review a district court's ruling on a motion to compel discovery for abuse of discretion." *United States v. Kienast*, 907 F.3d 522, 530 (7th Cir. 2018). Owens nevertheless contends that we must apply a de novo standard of review here because he raises "issues of constitutional dimensions." He argues that his claim is properly analyzed under the Sixth Amendment's Confrontation Clause. In this vein, he cites *Crawford v. Washington*, 541 U.S. 36 (2004), *Melendez-Diaz v. Massachusetts*, 557 U.S. 305 (2009), and *Bullcoming v. New Mexico*, 564 U.S. 647 (2011), for the proposition that he is entitled to cross-examine the "bias," "reliability," and "believability" of TDR. He also analogizes TDR to a confidential informant, whose "identity" must be disclosed "whenever the informer's testimony may be relevant and helpful to the

accused's defense," such as when the "informer was the sole participant, other than the accused, in the transaction charged." *See Roviaro v. United States*, 353 U.S. 53, 61–62, 64 (1957).

However, the First, Second, Sixth, Eighth, and Ninth Circuits have addressed the precise discovery issue raised by Owens over the course of the past decade, and no circuit applied a de novo standard of review or used a Confrontation Clause framework. Furthermore, Owens fails to persuade us that such an approach would be appropriate here, where the operator of TDR would be available for cross-examination. Accordingly, we review the district court's denial for abuse of discretion.

B. Other Circuits' Approaches

As just noted, several of our sister circuits have considered whether a defendant has made an adequate showing of materiality in similar circumstances, and a review of these cases is informative. We begin with *United States v. Chiaradio*, 684 F.3d 265 (1st Cir. 2012), and *United States v. Budziak*, 697 F.3d 1105 (9th Cir. 2012), which came first and set the stage for what it means to make a *prima facie* case of materiality in this context.

In *United States v. Chiaradio*, the First Circuit affirmed the district court's denial of Chiaradio's motion to compel access to the government's proprietary software. 684 F.3d at 276–77. In that case, the government used an enhanced version of LimeWire (another peer-to-peer file-sharing program) called "EP2P," (short for "enhanced peer-to-peer software") to download several child pornography files from an IP address registered to Chiaradio, who was then charged with possessing and distributing child pornography. *Id.* at 271–72.

Although the government had already produced "a digital file recording the transfer from the defendant's laptop to [the law enforcement agent's] computer" and "a copy of the FBI guide detailing how to reconstruct an EP2P session manually (using only the recording and publicly available programs)," Chiaradio also sought EP2P's source code. *Id.* at 277. He claimed that "he had to obtain the source code in order to determine whether he could credibly challenge the reliability of the technology and, thus, block the expert testimony proffered by the government on the EP2P program and how it implicated the defendant." *Id.*

The First Circuit took "no view" on whether the defendant had demonstrated materiality. But because the defendant "neither contradicted nor cast the slightest doubt upon" testimony indicating that agents had reconstructed and verified the file transfer, the court found it "pellucid that the forbidden files were located on the defendant's computers and transferred to [the agent]." *Id.* As such, the court held that any purported error in EP2P's functioning was harmless, and so was the denial of the defendant's motion to compel. *Id.*

Owens argues that this case is more like *United States v. Budziak*, where the Ninth Circuit held that the defendant had adequately demonstrated materiality and reversed the district court's decision denying discovery. *See* 697 F.3d at 1111–13. As in *Chiaradio*, the government used EP2P to download child pornography files from the defendant's shared LimeWire folder. *Id.* at 1107. A forensic examination of Budziak's computer revealed multiple child pornography files, including several of the images the FBI had downloaded. *Id.* The creation date of the files, however, post-dated the FBI's downloads. *Id.* Budziak was charged with multiple counts of

possessing and distributing child pornography, and he moved three times to compel disclosure of the government's EP2P program. *Id.* at 1108. The district court denied his motions, and he was convicted on each count after a jury trial. *Id.*

On appeal, the Ninth Circuit held that the district court abused its discretion when it denied Budziak's motions to compel. It noted that Budziak identified "specific defenses to the distribution charge that discovery on the EP2P program could potentially help him develop," and "presented evidence"—in the form of an affidavit from his expert—"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." *Id.* at 1112 (citation omitted). Budziak also submitted evidence "suggesting that the FBI agents could have used the EP2P software to override his sharing settings." *Id.* Based on this evidence, the court found that "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." *Id.*

The Ninth Circuit also distinguished *Chiaradio*, because unlike the defendant in that case, "Budziak presented arguments and evidence suggesting that the materials disclosed by the FBI did not resolve all questions relevant to his defense. *Id.* at 1112–13 n.1. In discounting the government's assertion that "the computer logs it provided Budziak demonstrated that he would not uncover any helpful information through discovery of the software," the Ninth Circuit cautioned district courts not to "merely defer to government assertions that discovery would be fruitless" if a defendant made a threshold showing of materiality. *Id.* at 1112–13.

The court went on to warn:

> 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.

Id. at 1113. The Ninth Circuit remanded the case to the district court to determine whether the EP2P materials did "in fact contain, or would have led to, information that might have altered the verdict." *Id.* (citation omitted).

The Second, Sixth, and Eighth Circuits have also recently considered this issue, largely following the principles announced in *Chiaradio* and *Budziak*.

In *United States v. Pirosko*, the Sixth Circuit held that the defendant failed to demonstrate materiality (and, in any event, the law enforcement investigative privilege would operate to shield production of the software) where the defendant only supported his motion to compel with a conclusory letter from his expert claiming that errors in the program may have existed because the government's disclosures "le[ft] otherwise answerable questions unanswered." 787 F.3d 358, 366 (6th Cir. 2015).[2] Unlike the defendant in *Budziak*, the court

[2] The Sixth Circuit made this statement when discussing the law enforcement investigative privilege, but because the privilege analysis "weigh[s] the government's concerns against the needs articulated by [the

concluded, "Pirosko has failed to produce any [evidence that the program did not operate as described] here, even after receiving the government's computer logs, which included information on when law enforcement officials were able to connect to his computer and what files they were able to download from his shared folder." *Id.*

The Sixth Circuit nonetheless admonished the government that "this conclusion should not be read as giving the government a blank check to operate its file-sharing detection software sans scrutiny. As a general matter, it is important that the government's investigative methods be reliable, both for individual defendants like Pirosko and for the public at large." *Id.* "Still," the court wrote, "we think that it is important for the defendant to produce some evidence of government wrongdoing." *Id.*

In *United States v. Clarke*, the Second Circuit recognized that,

> when a defendant's guilt is predicated on the government offering proof that a government agent downloaded files from the defendant's computer, information about the program by which the downloading was accomplished is likely to be "material to preparing the defense" and therefore subject to disclosure under [Rule] 16(a)(1)(E)(i), so as to enable the defendant to challenge the government's proof.

---

defendant]," *see Pirosko*, 787 F.3d at 365—in other words, the analysis weighs the government's concerns against the materiality of the evidence to the defense—this discussion appropriately informs our materiality analysis.

979 F.3d at 97. Nonetheless, the court determined that it "need not decide whether the [g]overnment's reasons for withholding disclosure outweighed [the defendant's] need for it" because the defendant was not prejudiced by the nondisclosure. *Id.* at 98.

Like this case, *Clarke* involved BitTorrent and a version of Torrential Downpour; government investigators downloaded child pornography from the defendant's shared folder on the BitTorrent network, and he was charged with possession and transportation. *Id.* at 86–87. Clark sought a copy of the Torrential Downpour program or its source code for testing and evaluation. *Id.* at 88. His proffered theory was that the allegedly downloaded files were stored only on his external hard drive and could not have been accessible to the public via the BitTorrent network. *Id.* Clarke sought to test whether Torrential Downpour could access non-public information on his computer. *Id.*

The government provided Clarke with (1) copies of the files downloaded by the agents (as well as forensic images of the corresponding data recovered on the defendant's computer equipment); (2) over 200 pages of data logs detailing the agents' downloads of files from his computer; (3) a "forensic report" of the computer equipment seized; and, crucially, (4) an in-person demonstration of how Torrential Downpour operated. *Id.* at 97. The government's expert also "submitted evidence showing that files downloaded and saved to an external hard drive by a Department of Justice investigative analyst, using the same version of uTorrent used by Clarke, were accessed by other BitTorrent users." *Id.* at 98.[3] The Second

[3] The program uTorrent is a BitTorrent software client. *Clarke*, 979 F.3d at 87.

Circuit held that the district court was entitled to credit this evidence over the defendant's "speculation" that it was not possible to download files from an external hard drive over the BitTorrent network. *Id.* Accordingly, the court held that "given the extensive disclosures that were made to Clarke," there was "no indication" that "he was in any way prejudiced by the district court's denial of his demand for disclosure of the program itself and its source code." *Id.* at 98–99.

Finally, in *United States v. Hoeffener*, the Eighth Circuit concluded that the defendant's request to access the program at issue was nothing more than a "fishing expedition." 950 F.3d 1037, 1043 (8th Cir. 2020). *Hoeffener* also involved Torrential Downpour and BitTorrent, but there, unlike this case, the defendant was charged only with receipt and possession of child pornography. *Id.* at 1040. The government disclosed:

> (1) a printout of a Powerpoint presentation about the installation and use of uTorrent version 2.2.1 (the file-sharing software used by Hoeffener at the time of the online investigation); (2) a compact disc depicting a simulation of how law enforcement personnel use the software program; (3) the log of activity occurring during the online investigation of Hoeffener's computer, along with testimony explaining these materials from a detective who helped create and train law enforcement personnel on the use of the software program; (4) the length of time the program had been used by the St. Louis Metropolitan Police Department; and (5) a list of the program's authorized users.

Id. at 1043.[4] The Eighth Circuit also noted that the defendant's retained expert had been granted access to Torrential Downpour the prior year by a district court in the District of Arizona following *Budziak*. *Id.* at 1043 n.3.

In addition to these materials, Hoeffener sought the source code and manuals relating to the program to evaluate whether there had been a Fourth Amendment violation. *Id.* at 1043. But, the Eighth Circuit concluded, Hoeffener only offered "mere speculation that the software program could possibly access non-public areas of his computer or that there was a possibility that it malfunctioned during the officers' investigation into Hoeffener's sharing of child pornography." *Id.* at 1044. The court held that this was insufficient to meet the threshold *prima facie* showing of materiality.

These cases show that, in general, a defendant will not be able to make a *prima facie* case that disclosure of the government's confidential software is material to his defense if he cannot present a cogent defense theory, supported by some facts, which discovery relating to the software would help develop. *See, e.g.*, *Chiaradio*, 684 F.3d at 277; *Hoeffener*, 950 F.3d at 1044. Furthermore, a defendant may yet fail to make a *prima facie* showing of materiality if the government presents evidence based on information produced to the defendant that fatally undermines the proffered theory. *See, e.g.*, *Clarke*, 979 F.3d at 98. But, where the government's evidence does not "resolve all questions relevant to [the proffered] defense," then discovery is likely appropriate, subject to any privileges

[4] The detective who testified was Detective Erdely, the same witness for the government in this case.

the government may prove to be applicable. *See Budziak*, 697 F.3d at 1112–13 n.1.

C. Application to the Instant Case

Returning to the case before us on appeal, as the district court in this case correctly acknowledged, the burden of making a *prima facie* showing of materiality typically "is not a heavy burden." *Lloyd*, 992 F.2d at 351. Rather, a defendant must simply present facts indicating that the evidence will "play an important role in uncovering admissible evidence, aiding witness preparation, corroborating testimony, or assisting impeachment or rebuttal." *Id.* (citation omitted). Furthermore, the evidence need not be exculpatory. *See Mackin*, 793 F.3d at 709–11.

We join our sister circuits in underscoring that the government does not have "a blank check to operate its file-sharing detection software sans scrutiny," *Pirosko*, 787 F.3d at 366, and "criminal defendants should not have to rely solely on the government's word that further discovery is unnecessary," *Budziak*, 697 F.3d at 1113. We also emphasize that "[i]n cases where the defendant has demonstrated materiality,"—and by that, we mean simply that the defendant has made a threshold showing of materiality—"the district court should not merely defer to government assertions that discovery would be fruitless." *Id.* at 1112–13.

Concerns about materiality aside, we review a district court's discovery ruling for abuse of discretion, and we will reverse only where "there is 'an appreciable risk that prejudice resulted.'" *United States v. Bastanipour*, 697 F.2d 170, 177 (7th Cir. 1982) (quoting *United States v. Dioguardi*, 428 F.2d 1033, 1038 (2d Cir. 1970)); *see also United States v. Kohli*, 847

F.3d 483, 493–94 (7th Cir. 2017) (reviewing the government's failure to disclose material information pursuant to Rule 16 for harmless error); *Orzechowski*, 547 F.2d at 985 (holding that "we cannot say that these items were material within the meaning of Rule 16, or that their exclusion, if error, was not harmless"); *Pirosko*, 787 F.3d at 365 (noting that "[r]eversal [for a district court's Rule 16 error] is appropriate only if the abuse was not harmless error" (internal quotation marks and citation omitted)). Accordingly, a defendant has a much heavier burden on appeal than he does when presenting a Rule 16 motion to compel to the district court. And where the district court has not clearly erred by crediting evidence that a defendant possessed or distributed an illicit file—irrespective of any questions raised about the government's confidential software—then an appealing defendant will have an uphill battle indeed.

Here, we hold that Owens suffered no prejudice from the district court's decision, and thus we need not opine on materiality. The government presented evidence that undermined Owens's proffered "false positive" theory, which the district court was entitled to credit.[5] In particular, the district court

[5] Owens maintains that the district court should not have relied on Erdely's testimony about the way TDR functions because it amounted to improper "*ipse dixit*." *See Ipse dixit*, Black's Law Dictionary (11th ed. 2019) (defining *ipse dixit* as "[s]omething asserted but not proved"). But Owens's concerns are misplaced. Our caselaw describes an expert's *ipse dixit* as occurring where "there is simply too great an analytical gap between the data and the opinion proffered." *See C.W. ex rel. Wood v. Textron, Inc.*, 807 F.3d 827, 832 (7th Cir. 2015) (quoting *Gen. Elec. v. Joiner*, 522 U.S. 136, 138 (1997)). To identify improper *ipse dixit*, "[t]he critical inquiry is whether there is a connection between the data employed and the opinion offered; it is the opinion connected to existing data 'only by the *ipse dixit* of the expert' that is properly excluded under Rule 702." *Gopalratnam v. Hewlett-*

did not clearly err when it accepted Erdely's testimony that the torrent relating to the target file had been opened in Owens's BitComet application while the investigation was occurring, as well as the evidence that a file with the same filename as the illicit video was present in Owens's "most recently used" folder. This testimony was based on the forensic analysis of Owens's computer, which the government produced to defense counsel.

Given these facts, Owens cannot demonstrate that access to TDR would "substantially alter the quantum of proof in his favor." *Orzechowski*, 547 F.2d at 984 (citation omitted). Substantial evidence indicates that Owens accessed and shared the file at issue, which is untainted by any questions raised about TDR's functions. And because Owens was not prejudiced as a result of the government's non-disclosure, we need not address whether the district court properly applied the law enforcement investigative privilege to the case at hand.

III. Conclusion

For the foregoing reasons, we AFFIRM the judgment of the district court.

Packard Co., 877 F.3d 771, 781 (7th Cir. 2017) (quoting *Manpower, Inc. v. Ins. Co. of Pennsylvania*, 732 F.3d 796, 806 (7th Cir. 2013)). Erdely, however, was not attempting to create a bridge between raw data and his expert opinion. He was testifying about the nature of TDR based on his experience developing and working with the program. Therefore, it was not improper for the district court to rely on Erdely's testimony.