RECOMMENDED FOR FULL-TEXT PUBLICATION
Pursuant to Sixth Circuit I.O.P. 32.1(b)

File Name: 15a0098p.06

UNITED STATES COURT OF APPEALS

FOR THE SIXTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

JOSEPH PIROSKO,

Defendant-Appellant.

No. 14-3402

Appeal from the United States District Court
for the Northern District of Ohio at Akron.
No. 5:12-cr-00327—Christopher A. Boyko, District Judge.

Argued: April 21, 2015

Decided and Filed: May 21, 2015

Before: SILER, MOORE, and STRANCH, Circuit Judges.

COUNSEL

ARGUED: Wendi L. Overmyer, OFFICE OF THE FEDERAL PUBLIC DEFENDER, Akron, Ohio, for Appellant. Laura McMullen Ford, UNITED STATES ATTORNEY'S OFFICE, Cleveland, Ohio, for Appellee. **ON BRIEF:** Wendi L. Overmyer, Melissa M. Salinas, OFFICE OF THE FEDERAL PUBLIC DEFENDER, Akron, Ohio, for Appellant. Laura McMullen Ford, UNITED STATES ATTORNEY'S OFFICE, Cleveland, Ohio, for Appellee.

OPINION

KAREN NELSON MOORE, Circuit Judge. On June 6, 2012, federal agents executed a search warrant on Joseph Pirosko's hotel room. They seized a laptop computer and a USB drive; a later analysis revealed numerous images and video files depicting child pornography on both

devices. A grand jury returned a two-count indictment against Pirosko, charging him with knowingly receiving and distributing numerous computer files containing visual depictions of real minors engaged in sexually explicit conduct, in violation of 18 U.S.C. § 2252(a)(2), and knowingly possessing a computer and a USB storage device, each containing child pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B).

After his indictment, Pirosko filed a motion to compel discovery, requesting that the district court "order that the government disclose the law enforcement tools and records used . . . to search Mr. Pirosko's computer equipment." The district court denied this motion, citing the sensitive nature of the computer programs and Pirosko's lack of a demonstrated need for discovery. Pirosko then filed a motion to suppress, arguing that his Fourth Amendment rights were violated because the government's search warrant was obtained using unreliable and unsupported information. The district court again denied this motion. Pirosko subsequently entered a conditional guilty plea with respect to the first count in his indictment. At sentencing, the district court found Pirosko's Guidelines range to be between 262 and 327 months of imprisonment. He ultimately received a sentence of 240 months of imprisonment, the statutory maximum.

Pirosko makes four arguments on appeal. First, he contends that the district court abused its discretion in denying his motion to compel discovery. He substantially reiterates these arguments with respect to his motion to suppress. In addition, Pirosko also claims, for the first time, that the government used unconstitutional warrantless tracking in order to obtain its search warrant. Finally, Pirosko asserts that his sentence is greater than necessary to comply with the purposes of 18 U.S.C. § 3553(a). These claims are without merit. Accordingly, we **AFFIRM** Pirosko's conviction and sentence.

I. BACKGROUND

A. Facts

According to the criminal complaint, Officer Edward Sexton of the Nebraska Department of Justice noticed, in March 2012, an IP address sharing several "notable" files of child pornography via a file-sharing program. R. 1-1 (Criminal Compl. at 12) (Page ID #13). Sexton

observed that there were three different Globally Unique Identifier (GUID) numbers on this particular IP address.[1] Of these three numbers, two had last been used in 2008 and 2009. The third had been in more frequent use, first logging into the Gnutella file-sharing network in January 2012. Sexton began tracking this third GUID. He set up a direct connection and attempted to obtain a list of all notable files being shared by the associated computer and, when possible, downloaded directly some of the files being shared. Over the next few months, Sexton was able to connect with the GUID and download shared files numerous times. He also found the GUID associated with IP addresses from hotels across the country. After examining the guest lists at each of these hotels, Sexton determined that the GUID in question belonged to Joseph Pirosko. On June 4, 2012, Sexton submitted an affidavit in support of a search warrant for material in Pirosko's hotel room in Wooster, Ohio. The district court granted this warrant, and officers seized Pirosko's computer, where they found numerous files containing child pornography on the shared folder of his LimeZilla account. Officers also seized a USB drive.

B. Motion to Compel

After an initial discovery request, in response to which the government provided Pirosko with an opportunity to review the equipment that it had seized, Pirosko filed a motion to compel discovery of the "law enforcement tools . . . [used] to assess information in connection with the particular GUID . . . associated with Mr. Pirosko's computer equipment." R. 26 (Mot. to Compel Disc. at 2) (Page ID #175). Pirosko stated that he was entitled to these materials pursuant to Federal Rule of Criminal Procedure 16, which states that,

> Upon a defendant's request, the government must permit the defendant to inspect and to copy or photograph books, papers, documents, data, photographs, tangible objects, buildings or places, or copies or portions of any of these items, if the item is within the government's possession, custody, or control and:
>
> **(i)** the item is material to preparing the defense;
> **(ii)** the government intends to use the item in its case-in-chief at trial; or
> **(iii)** the item was obtained from or belongs to the defendant.

[1]Each internet network is assigned a separate IP address; this address refers to the physical location of that particular network. A GUID number is produced whenever a peer-to-peer (P2P) file-sharing application (like LimeZilla) is installed or updated on a computer, and remains associated with the computer whenever the file-sharing program is in use. R. 1-1 (Criminal Compl. at 11) (Page ID #12). Pirosko's GUID number thus remained the same over the course of the investigation, even though he logged onto different internet networks (with different IP addresses) across the country.

Fed. R. Crim. P. 16(a)(1)(E). In support of this motion, Pirosko submitted a letter from Interhack, a computer analysis company, which noted that "[a]nalysis of the tools used by investigators to create records can determine whether law enforcement officers manipulated data on the subject computer, the error rates in records used, or whether the GUID in question at a particular time is connected to a particular installation of *LimeZilla*." R. 26-1 (Exh. in Mot. to Compel Disc. at 4) (Page ID #181).

The government responded by noting that it had connected with Pirosko's computer using ShareazaLE, a proprietary program used exclusively by law enforcement. According to the government, this program allows officials to download files exclusively from a target's computer (users of publicly available file-sharing programs download from multiple sources in order to expedite the download process). It opposed Pirosko's request for access, stating that ShareazaLE was a form of "sensitive law enforcement surveillance software protected . . . by qualified privilege." R. 32 (Resp. to Mot. to Compel Disc. at 4) (Page ID #199). In addition, the government argued that Pirosko had failed, under Federal Rule of Criminal Procedure 16, to show materiality. The district court denied Pirosko's motion to compel, relying largely on the government's privilege argument and finding that Pirosko had failed to show a particular need for access.

C. Motion to Suppress

Pirosko subsequently filed a motion to suppress, alleging that the government's search warrant had relied on unreliable information. This motion largely repeated arguments made in his motion to compel. Pirosko also claimed that Sexton's affidavit would not qualify as expert evidence under *Daubert*. In response, the government argued that Pirosko had failed to meet the burden necessary to warrant a *Franks* hearing. Furthermore, the government contended that, even if its search warrant affidavit lacked probable cause, it would nonetheless fall within the good-faith exception. The district court agreed with the government's position. In addition, it stated that "even if the Court eliminated all mentions of the law enforcement database or the GUIDs, the Court finds that it was reasonable for the magistrate to find probable cause," because Pirosko "was a guest at hotels in Nebraska, Missouri, New Jersey, Utah and Ohio over a three-month period" and, during each of these stays, Pirosko "connected to the same peer-to-peer

network, used the same software, and downloaded images of child pornography from a computer." R. 42 (District Ct. Op. Den. Mot. to Suppress at 7) (Page ID #342).

D. Plea Agreement and Sentencing

Pirosko agreed to plead guilty to count one of his indictment, which charged him with "knowingly receiv[ing] and distribut[ing], using any means or facility of interstate and foreign commerce, numerous computer files, which files contained visual depictions of real minors engaged in sexually explicit conduct," in violation of 18 U.S.C. § 2252(a)(2). R. 8 (Indictment at 1) (Page ID #89); R. 45 (Plea Agreement at 2) (Page ID #350). Under the terms of his plea agreement, Pirosko waived his right to appeal except with respect to the district court's decision to deny his motion to compel, the district court's decision to deny his motion to suppress, the determination of his criminal history category at sentencing, and any sentence greater than necessary to comply with the purposes of 18 U.S.C. § 3553(a). *Id.* at 5 (Page ID #353).

At sentencing, the district court found Pirosko's Guidelines range to be between 262 and 327 months of imprisonment, pursuant to an offense level of 39 and a criminal history category of I. In making Pirosko's offense level determination, the district court started with a base offense level of 22, added twenty levels in various enhancements, and subtracted three levels for acceptance of responsibility. Pirosko received a sentence of 240 months of imprisonment, the statutory maximum. On appeal, Pirosko contends that the district court erred in denying his motion to compel and his motion to suppress. With respect to his motion to suppress, Pirosko asserts, for the first time, that officers engaged in unconstitutional warrantless tracking of his computer. Pirosko also contends that his sentence is procedurally and substantively unreasonable. With respect to his procedural-unreasonableness argument, Pirosko claims specifically that the district court erred in applying a two-level enhancement for distribution, a five-level enhancement for pattern of activity, and a five-level enhancement for number of images.

II. DISCUSSION

A. Motion to Compel

1. Standard of Review

"We review the denial of a motion to compel production, as an evidentiary matter within the trial court's discretion, for an abuse of discretion." *United States v. Blood*, 435 F.3d 612, 627 (6th Cir. 2006). "An abuse of discretion occurs when we are left with the 'definite and firm conviction that the [district] court . . . committed a clear error of judgment in the conclusion it reached upon a weighing of the relevant factors' or 'where it improperly applies the law or uses an erroneous legal standard.'" *United States v. Haywood*, 280 F.3d 715, 720 (6th Cir. 2002) (quoting *Huey v. Stine*, 230 F.3d 226, 228 (6th Cir. 2000)). "Reversal is appropriate only if the 'abuse' was not harmless 'error.'" *United States v. Vasilakos*, 508 F.3d 401, 406 (6th Cir. 2007).

2. Analysis

a. Law Enforcement Privilege

In evaluating the government's privilege argument, we agree with the district court's decision to apply a balancing approach, weighing the government's concerns against the needs articulated by Pirosko. We have applied this sort of framework before. *See United States v. Gazie*, 786 F.2d 1166, 1986 WL 16498, at *8–*9 (6th Cir. 1986) (Table) (applying balancing approach with respect to argument regarding the location of government surveillance equipment).

In the context of this case, the government argues that granting Pirosko's motion to compel would compromise the integrity of its surveillance system and would frustrate future surveillance efforts. Pirosko, on the other hand, contends that the government should have turned over a copy of its software, thereby allowing his experts to determine whether ShareazaLE gives government officials "the ability to manipulate settings or data on the target computer (even unintentionally)," "whether the software allows agents to override shared settings to download files that a normal user would not be able to download," and "the error rate" associated with the software. Appellant Br. at 18–19. Pirosko cites several cases where

defendants have purportedly been allowed access to the government's software, including the Ninth Circuit's decision in *United States v. Budziak*, 697 F.3d 1105 (9th Cir. 2012).

His reliance on these cases is not well taken. In its opinion denying Pirosko's motion to compel, the district court pointed to a number of reasons why this case was not simply a re-iteration of *Budziak*. Budziak, for instance, had filed multiple motions to compel. "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." 697 F.3d at 1112. "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." *Id.* Pirosko has failed to produce any such evidence, simply alleging that he might have found such evidence had he been given access to the government's programs.

Tellingly, in *Budziak*, the Ninth Circuit also noted that, "[a]lthough 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." *Id.* The court then stated, in an accompanying footnote, that

> 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. 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. In contrast, Budziak presented arguments and evidence suggesting that the materials disclosed by the FBI did not resolve all questions relevant to his defense.

Id. at n.1 (citations omitted).

To summarize, in deciding to deny Pirosko's motion to compel, the district court had before it the First Circuit's decision in *United States v. Chiaradio*, 684 F.3d 265, 278 (1st Cir. 2012), where the defendant did not provide any evidence of government error, and the Ninth Circuit's decision in *Budziak*, where the defendant did provide evidence of error. Here, the *strongest* evidence of error was a single sentence in a letter by Interhack, a firm hired by Pirosko, which stated that "[t]he [government's] affidavit does not show which tools, which records, or

the means by which those records were created, leaving otherwise answerable questions unanswered." R. 26-1 (Exh. in Mot. to Compel Disc. at 4) (Page ID #181). That lone allegation is simply not enough to overcome the numerous facts supporting the government's position that it legitimately obtained child pornography from Pirosko's shared folders.

To be clear, 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. Still, we think that it is important for the defendant to produce some evidence of government wrongdoing. We have held as much in cases involving more traditional police investigation techniques. *See, e.g.*, *United States v. Boxley*, 373 F.3d 759, 761 (6th Cir. 2004) (stating that, with respect to dog sniffs, "it is not necessary for the government to show that the dog is accurate one hundred percent of the time, because a very low percentage of false positives is not necessarily fatal to a finding that a drug detection dog is properly trained and certified") (internal quotation marks omitted). Pirosko has failed to produce any such evidence 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. Pirosko has, moreover, conceded that he did not turn off his upload settings—he simply argues that his settings allowed for a low rate of downloading, a point that we discuss in greater detail below. It would not have been difficult for Pirosko, armed with this information, to establish some evidence of government wrongdoing, had any such wrongdoing actually occurred: he knew the size of the files being downloaded, the approximate download speed, and the time when the government allegedly downloaded these files. What remains is a simple exercise in arithmetic. Pirosko has either failed to do this exercise or, having done it, has realized that the math simply does not add up. In any event, he has failed to demonstrate that the district court abused its discretion in denying his motion to compel discovery.

As a final note, the remaining decisions cited by Pirosko are likewise unavailing. In fact, one of the primary cases relied upon by Pirosko—*United States v. Crowe*, No. 11 CR 1690 MV (D.N.M. Apr. 3, 2013)—actually points in favor of the government, not Pirosko. In that case, the

district court denied Crowe's motion to compel discovery, but granted Crowe's motion for independent evaluation by an expert of the government's software, pursuant to Federal Rule of Criminal Procedure 16. *Id.* at 15. Yet in reaching this decision, the district court noted that, "[a]s in *Budziak*, in this case, Defendant submitted the testimony of his expert witness, Tami Loehrs, who indicated that during her examination of Defendant's computer, some of the files alleged to have been found by law enforcement in the shared space of Defendant's computer, were not found there during her analysis." *Id.* at 13. Pirosko has, as we have already noted, not submitted any such evidence. More importantly, *Crowe*'s reliance on Loehrs's affidavit appears to have been a mistake. In fact, in a subsequent case, *United States v. Thomas*, Nos. 5:12-cr-37, 44, 97, 2013 WL 6000484 (D. Vt. Nov. 8, 2013), the district court considered and completely discredited Loehrs's statements. In *Thomas*, as in *Crowe*, Loehrs prepared a report summarizing her knowledge of the government's software. After reviewing this report, the district court stated in *Thomas* that "Ms. Loehrs's declarations . . . [we]re misleading in several respects." *Id.* at *12. The district court continued, finding that:

> As a preface to a list of twenty-five cases identified in her declarations, Ms. Loehrs states; [sic] "I have also learned through hundreds of forensic examinations on cases involving undercover P2P investigations and allegations of child pornography, that files are being identified by law enforcement's automated software as containing child pornography when, in fact, they do not." However, none of the cases listed in Ms. Loehrs's declarations appeared to have resulted in a judicial finding to that effect.

Id. (citation omitted). "In her declaration . . . , Ms. Loehrs stated that she did not find the files identified in the *Neale* search warrant affidavit on Defendant Neale's computer when she examined it." *Id.* Yet she essentially retracted this statement on cross-examination. The district court also noted that "[t]he most troubling aspect of Ms. Loehrs's expert opinions in this case is her reliance on her work in other cases which was either disproved or rejected." *Id.* at *14. If anything, *Crowe* and *Thomas* point in the government's favor—both cases show that allowing Pirosko access without any evidence of error would needlessly expose the government's enforcement tools to examination and pointlessly drag out the course of litigation.

b. Materiality

Pirosko's arguments fail also for a second reason: he cannot establish materiality. In interpreting the issue of materiality, we have held that Federal Rule of Criminal Procedure 16 applies only to "'shield' claims that 'refute the Government's arguments that the defendant committed the crime charged.'" *United States v. Robinson*, 503 F.3d 522, 532 (6th Cir. 2007) (quoting *United States v. Armstrong*, 517 U.S. 456, 462 (1996)). Requests for discovery fall outside the scope of this provision if a defendant is "not seeking the discovery to aid in the preparation of his defense," but is "attempting to obtain the discovery for the purpose of gathering materials to support various sentencing arguments." *Robinson*, 503 F.3d at 532.

The purpose of Pirosko's motion to compel is not to aid in the preparation of his defense, but to contradict the district court's finding of distribution at sentencing—a point made by Pirosko in his brief and by his counsel at oral argument. After all, Pirosko was charged with violating 18 U.S.C. § 2252(a)(2), which penalizes the knowing receipt *or* distribution of child pornography. Pirosko does not contest that he received child pornography—his arguments pertain only to distribution. Although a finding of distribution can result in a sentencing enhancement under the Guidelines, such a finding is *not* required for a conviction under 18 U.S.C. § 2252(a)(2).

To be sure, Pirosko's indictment and plea agreement did charge him with both receipt *and* distribution. *See* R. 8 (Indictment at 1) (Page ID #89); R. 45 (Plea Agreement at 3) (Page ID #351). But "[i]t is settled law that an offense may be charged conjunctively in an indictment where a statute denounces the offense disjunctively. Upon the trial the government may prove and the trial judge may instruct in the disjunctive form used in the statute." *United States v. Murph*, 707 F.2d 895, 896–97 (6th Cir. 1983) (citation omitted); *see also United States v. Jones*, 533 F. App'x 562, 572 (6th Cir. 2013) (citing *Murph*).

Even if distribution were a required element for conviction, discovery of the government's software would have been immaterial. In his sentencing memorandum, Pirosko submitted a report that concluded that he had taken actions that were "consistent with a user attempting to disable file sharing." R. 52-1 (Exh. A in Pirosko Sentencing Mem. at 13) (Page ID #566). But, on this same page, the report noted that, although Pirosko attempted to reduce his

upload speed by moving a graphical slider on his computer screen, "[w]hat . . . the user might see logically as 'zero percent' is in fact not an actual upload speed of zero." *Id.* In addition, the report stated that "[t]he data are characteristic of the user manually changing the [number of upload slots] from 20 to 1," not 20 to 0. These facts corroborate the screenshot taken of Pirosko's computer, included as an exhibit by the government in its sentencing memorandum. R. 53-1 (Exh. A in Gov't Sentencing Mem. at 1) (Page ID #699). That screenshot shows Pirosko's upload speed to be 10.94 kilobytes per second (not 0 kilobytes per second) and includes a dialog box that reads: "[t]o turn off uploads, reduce your upload slots to zero." *Id.*

Such circumstances are consonant with a finding of distribution. Although we have yet to analyze distribution with respect to 18 U.S.C. § 2252(a)(2) in detail, our sister circuits have typically adopted some version of the test applied by the Ninth Circuit: "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." *United States v. Budziak*, 697 F.3d 1105, 1109 (9th Cir. 2012); *see United States v. Husmann*, 765 F.3d 169, 174 (3d Cir. 2014) (citing *Budziak*). Here, Pirosko admits that he maintained child pornography in a shared folder. The screenshot and the report both demonstrate that he knew (or should have known) that others would have been able to download from this shared folder. And another person—Officer Sexton—was in fact able to download from Pirosko's shared folder. Whether the government used its software to manipulate Pirosko's upload speed is therefore irrelevant.

In a related context, we have held that the "knowing use of LimeWire [a file-sharing program similar to LimeZilla] . . . is sufficient to trigger [U.S.S.G.] § 2G2.2(b)(3)(F)'s two-level enhancement" for distribution of child pornography. *United States v. Conner*, 521 F. App'x 493, 500 (6th Cir. 2013). "[T]he purpose of a file sharing program is to share, in other words, to distribute, and knowing use of such a program qualifies as conduct that involve[s] . . . distribution." *Id.* (internal quotation marks omitted); *see also United States v. Bolton*, 669 F.3d 780, 782–83 (6th Cir. 2012) (discussing with approval decisions by other courts "to hold that the government may prove distribution [under the Guidelines] merely by showing that the defendant

knowingly used a peer-to-peer file-sharing program to download child pornography"). We discussed in *Conner* the Eighth Circuit's decision in *United States v. Durham*, 618 F.3d 921 (8th Cir. 2010), where that court, "[u]nique among courts that have addressed this issue," "held that the presumption that users of peer-to-peer software understand they are sharing files with others can be rebutted by the defendant." *Conner*, 521 F. App'x at 500. We declined to adopt this analysis, yet did note that Conner could not "point to concrete evidence of ignorance in the record that would raise the issue the *Durham* court confronted." *Id.* at 501 (internal quotation marks omitted). The facts here are even more egregious: Pirosko's actions show a better-than-average understanding of the LimeZilla program, as he changed his settings to minimize (but not eliminate) the downloading of his files. He has also, like Conner, presented no concrete evidence of ignorance nor contested the fact that officers like Sexton would have been able to download shared files from his computer without manipulating his sharing settings.

To summarize, Pirosko cannot show materiality because a finding of distribution is not necessary under 18 U.S.C. § 2252(a)(2). Even if it were necessary, Pirosko has admitted to facts—that he maintained a shared folder, that he made files in this folder available for download, and that some of these files were actually downloaded—that would make discovery of the government's software immaterial. The district court did not abuse its discretion in denying his motion to compel.

B. Motion to Suppress—Unreliable and Unsupported Information

1. Standard of Review

We "review[] the district court's denial of a *Franks* hearing under the same standard used to review the district court's denial of a motion to suppress: factual findings are reviewed for clear error and conclusions of law are reviewed de novo." *United States v. Rose*, 714 F.3d 362, 369–70 (6th Cir. 2013). "A defendant is entitled to a *Franks* hearing if he: 1) makes a substantial preliminary showing that the affiant knowingly and intentionally, or with reckless disregard for the truth, included a false statement or material omission in the affidavit; and 2) proves that the false statement or material omission is necessary to the probable cause finding in the affidavit." *Id.* at 370 (citing *Franks v. Delaware*, 438 U.S. 154, 171–72 (1978)).

2. Analysis

With respect to his motion to suppress, Pirosko argues that "the district court blindly accepted the government's claims at face value without providing Pirosko any access or opportunity to rebut those claims." Appellant Br. at 44. Had Pirosko been handed a copy of the government's software, he might have been able to uncover evidence that the affiant (Officer Sexton) "knowingly and intentionally, or with reckless disregard for the truth, included a false statement or material omission in the affidavit." *Rose*, 714 F.3d at 370. Pirosko then discusses whether the evidence supporting probable cause for his warrant would pass muster under *Daubert*—a standard used to evaluate admissibility of expert evidence at trial.

These arguments are meritless. Sexton's affidavit contained more than ten pages of statements detailing his experience and qualifications, the software he used, and the files he was able to download from Pirosko's computer. Pirosko has not pointed to a single misstatement in this affidavit, a specific prerequisite for obtaining a *Franks* hearing. His allegation that he might have been able to point to a misstatement if he were allowed to examine the government's software is the very sort of speculative claim that district courts are not supposed to hear. Moreover, Pirosko does not dispute that he was a guest at each of the hotels where he used the local wireless network to access child pornography, which would have, standing alone, been sufficient to find probable cause. Finally, it is unclear what relationship Pirosko wants us to draw between *Daubert* and *Franks*. *Daubert* is about expert evidence at trial, a right that Pirosko forfeited by pleading guilty. *Franks* is about whether a defendant has made allegations sufficient to merit a hearing regarding the validity of a search warrant affidavit. These cases have little to do with one another; certainly, we have never held that a search warrant affidavit must always be supported by evidence admissible under *Daubert*.

C. Motion to Suppress—Unconstitutional Warrantless Tracking

1. Standard of Review

We have already discussed the applicable standard of review for motions to suppress. In addition, the government contends that this particular claim is barred because of the appeal-waiver provision within Pirosko's plea agreement. We "review[] the question of whether a

defendant waived his right to appeal his sentence in a valid plea agreement *de novo*." *United States v. Smith*, 344 F.3d 479, 483 (6th Cir. 2003).

2. Analysis

a. Appeal Waiver

In *United States v. Woosley*, 361 F.3d 924, 928 (6th Cir. 2004), we "decline[d] to consider Woosley's additional contention that the district court erred in denying his motion for a *Franks* hearing, because his conditional plea only reserved the right to appeal the district court's ruling—entered September 10, 2002—denying his motion to suppress." In reaching this decision, we noted that "Woosley's motion for a *Franks* hearing was not part of his motion to suppress, and it was not disposed of in the district court's September 10, 2002, order." *Id.* "Accordingly, Woosley may not appeal the district court's adverse ruling on his motion for a *Franks* hearing, as he did not reserve his right to appeal that issue." *Id.* We have, in an unpublished decision, since extended *Woosley* to apply to a situation nearly identical to the one in this case. In *United States v. Vanderweele*, 545 F. App'x 465, 468 (6th Cir. 2013), we observed that "Vanderweele's plea only 'reserves the right . . . to seek review of the U.S. District Court's denial of his motion to suppress evidence.'" "This language," we noted, "preserves only the arguments he made below." *Id.* In his motion to suppress, Vanderweele made three arguments. On appeal, he tried to make a fourth: that he was illegally detained. *Id.* at 469. We held that he had "waived his right" to make this argument. *Id.*

Woolsey and *Vanderweele* provide a clear answer to the case at hand. The pertinent provision in Pirosko's plea agreement states that he "expressly and voluntarily waives [his] rights [to appeal], except," with respect to "(b) this Court's denial of [his] motion to suppress (R. 34)." R. 45 (Plea Agreement at 5) (Page ID #353). Pirosko's motion to suppress did not argue that the government engaged in unconstitutional warrantless tracking—it presented no such legal argument nor did it cite any of the supporting cases, like *United States v. Jones*, 132 S. Ct. 945 (2012), to which Pirosko now refers in his brief.

Pirosko alternatively argues that the district court failed to comply with Federal Rule of Criminal Procedure 11(b)(2), which requires the court to "Ensur[e] That a Plea Is Voluntary."

Fed. R. Crim. P. 11(b)(2). This provision states that, "[b]efore accepting a plea of guilty or nolo contendere, the court must address the defendant personally in open court and determine that the plea is voluntary and did not result from force, threats, or promises (other than promises in a plea agreement)." *Id.* Pirosko contends that he did not, during his plea colloquy, "directly answer[] the district court's question regarding [whether he had received] any threats or force." Appellant Reply Br. at 7. This argument is disingenuous. The plea colloquy transcript reads as follows:

> THE COURT: Has anyone made any threats or promises, other than what's set forth in this plea agreement, to either force or compel you to enter a plea of guilt this morning?
>
> MR. WARNER: Do you want me to answer that question for you? . . . [W]e discussed this on Friday at length about whether or not there are threats, and there certainly has been negotiations. This has been adversarial between Mr. Pirosko, so I mean, he feels that he is in a spot where there has been, certainly, you know, if you do A, B will happen.
>
> If you do B, C will happen, and that make[s] him feels threatened, but I explained to him that that's not what [the] Court means when it says threats [sic]. What it means threats, it means me telling him if you don't do this, I am going—you know, something off the record, and that is my impression of what threats means.
>
> THE COURT: Okay. Mr. Pirosko, so that we are all on the same page, I understand that there is no good choice. It is pick your poison, and that is what Mr. Warner is talking about; that it is just a bad situation that you are confronted with, and no choice of yours is going to be satisfactory to you. I understand that.
>
> But what I am asking you is whether your plea is going to be voluntary, in other words, your own decision to do this based upon all the information that you have. That's really what I am asking.
>
> THE DEFENDANT: Sir, I sinned, and I am going to plead guilty, yes, sir.
>
> THE COURT: Okay. And will you be doing this voluntarily?
>
> THE DEFENDANT: Yes, sir.

R. 59 (Plea Hr'g Tr. at 6–7) (Page ID #726–27). Pirosko did not raise a Rule 11 objection at his plea hearing. His objection is therefore reviewed for plain error, *United States v. Murdock*, 398 F.3d 491, 496 (6th Cir. 2005), a hurdle that it clearly cannot overcome.

b. Merits

Pirosko's claim would also fail on the merits. It is true that we have recognized that individuals have a reasonable expectation of privacy in data on non-shared folders on their

computer. *Guest v. Leis*, 255 F.3d 325, 333 (6th Cir. 2001). But we have never extended this reasoning to apply to files in a shared folder. *See Conner*, 521 F. App'x at 497 ("Public exposure of information in this manner defeats an objectively reasonable expectation of privacy under the Fourth Amendment."); *United States v. Stults*, 575 F.3d 834, 842–43 (8th Cir. 2009) (collecting cases). After all, files in a shared folder cannot, by definition, be considered files that an individual expects to be kept private.

Pirosko's reliance on *United States v. Jones*, 132 S. Ct. 945 (2012), is unavailing. *Jones* held that attaching a GPS device on a suspect's vehicle without his or her consent constituted a search, in violation of the Fourth Amendment. *See id.* at 954. In reaching its decision, the majority expressly declined to endorse the concurrence's view that "relatively short-term monitoring of a person's movements on public streets is okay, but . . . longer term GPS monitoring in investigations *of most offenses* is no good." *Id.* (internal quotation marks omitted). Pirosko asks that we adopt the concurrence's theory nonetheless. That request flies directly in the face of Supreme Court precedent. Moreover, his theory would, if taken seriously, give a free pass to on-the-road downloaders of child pornography: i.e., under his theory, your rights are not violated if you download from a single location (e.g., your home), but they are violated if you travel across the country, using a hotel's wireless network to download and upload files. We decline to adopt this reading of *Jones*.

D. Procedural and Substantive Unreasonableness

1. Standard of Review

"We review challenges to the reasonableness of a sentence for abuse of discretion." *United States v. Kamper*, 748 F.3d 728, 739 (6th Cir. 2014). "Sentences must be both procedurally and substantively reasonable." *Id.* When reviewing a sentence for procedural reasonableness, we must "ensure that the district court committed no significant procedural error, such as failing to calculate (or improperly calculating) the Guidelines range, treating the Guidelines as mandatory, failing to consider the § 3553(a) factors, selecting a sentence based on clearly erroneous facts, or failing to adequately explain the chosen sentence." *Gall v. United States*, 552 U.S. 38, 51 (2007). We review the district court's legal interpretation of the Guidelines de novo, *United States v. Settle*, 414 F.3d 629, 630 (6th Cir. 2005), but "accept

factual findings made by the district court at sentencing unless they are clearly erroneous," *United States v. Phillips*, 516 F.3d 479, 483 (6th Cir. 2008) (citations omitted).

"If the sentence is procedurally sound, we next evaluate whether it was substantively reasonable." *Kamper*, 748 F.3d at 739. "A reviewing court will find that a sentence is substantively *unreasonable* 'where the district court select[s] the sentence arbitrarily, bas[es] the sentence on impermissible factors, fail[s] to consider pertinent § 3553(a) factors, or giv[es] an unreasonable amount of weight to any pertinent factor.'" *United States v. Tate*, 516 F.3d 459, 469 (6th Cir. 2008) (quoting *United States v. Ferguson*, 456 F.3d 660, 664 (6th Cir. 2006)).

2. Analysis

a. Procedural Unreasonableness

i. Distribution Enhancement

The district court did not err in applying an enhancement for distribution, for the reasons stated above in Part II.A.2.b.

ii. Pattern-of-Activity Enhancement

U.S.S.G. § 2G2.2(b)(5) provides for a five-level offense enhancement "[i]f the defendant engaged in a pattern of activity involving the sexual abuse or exploitation of a minor." U.S.S.G. § 2G2.2(b)(5) (2013). The Commentary to this provision defines pattern of activity as "any combination of two or more separate instances of the sexual abuse or sexual exploitation of a minor by the defendant, whether or not the abuse or exploitation (A) occurred during the course of the offense; (B) involved the same minor; or (C) resulted in a conviction for such conduct." *Id.* at cmt n.1. The district court identified three such prior incidents: Pirosko's prior conviction for sexual abuse of a child and letters submitted by Pirosko's now-adult daughters detailing their prior sexual abuse or exploitation.

Pirosko's PSR goes into detail on his prior conviction, *see* PSR at ¶ 37, which the government also discussed at sentencing, *see, e.g.*, R. 60 (Sentencing Hr'g Tr. at 35–41) (Page ID #784–90). Pirosko does not challenge the district court's finding of sexual abuse or exploitation on this point. *Id.* at 30 (Page ID #779).

Both of Pirosko's daughters submitted letters documenting Pirosko's sexual abuse or exploitation of them as minors, portions of which are reprinted in Pirosko's PSR. PSR at ¶ 17. In both letters, the daughters report sleeping in twin beds next to one another, and Pirosko coming into their rooms at night to sexually exploit or abuse them. One of Pirosko's daughters concedes that she did not immediately remember the details of these events when first questioned by investigators in 2003, in relation to Pirosko's conviction in Germany. She writes, however, that "[a] few weeks after [Pirosko] was arrested I began hav[ing] horrible nightmares about my sister and I being molested as children." *Id.* In addition to these letters, the probation officer reported speaking to Pirosko's ex-wife, the mother of Pirosko's daughters. "She reported that . . . [i]n addition to their own two daughters, she also suspected the defendant of molesting three other children that she was aware of (one being the daughter of his second wife . . .)." *Id.* at ¶ 46.

Pirosko challenges these allegations by submitting a letter from his mother and by questioning the sufficiency of the evidence presented against him. R. 52-6 (Exh. F-1 Pirosko Sentencing Mem. at 1–3) (Page ID #667–69). The letter from Pirosko's mother, however, offers little by way of support to Pirosko. In fact, the letter actually states, at various points, that Pirosko's mother "chose to believe the girls," *id.* at 2 (Page ID #668), and that she "believe[s] the girls are telling the truth a[s] they believe the truth to be," *id.* at 3 (Page ID #669). She ends by noting that the daughters' account "may be their truth, but it *may* not have really happened." *Id.* (emphasis added). This is speculation—it does not provide any factual basis to vitiate the accounts given by Pirosko's daughters.

Pirosko's sufficiency-of-the-evidence challenge also fails. Pirosko claims that it was inappropriate for the court to base its finding on a set of out-of-court letters. We have considered this sort of claim before. *See United States v. Paull*, 551 F.3d 516, 527 (6th Cir. 2009) ("The district court's reliance on Barry's letter without live testimony from Barry is clearly permissible under our law."). Moreover, the letters provided by Pirosko's daughters corroborate one another, are consistent with the reports of Pirosko's ex-wife, and are arguably also consistent with the letter submitted by Pirosko's mother. Pirosko is correct that the letter in *Paull* was somewhat more specific than the letters at issue here. But Pirosko's daughters both were young children

when he sexually abused or exploited them, a fact that might have made specific recall more difficult. In addition, the accompanying evidence—the accounts given by Pirosko's ex-wife and Pirosko's mother—lend further support to the district court's finding in this case. The district court did not clearly err in considering these circumstances sufficient evidence for a finding of past sexual abuse or exploitation.

iii. Number-of-Images Enhancement

Finally, the district court awarded a five-level enhancement because it found that the offense conduct involved 600 or more images. U.S.S.G. § 2G2.2(b)(7)(D). Pirosko concedes that his conduct involved at least 234 images. The only question is whether the district court clearly erred in counting additional images found on a USB device seized during the search of his hotel room.

At sentencing, the district court noted that, with respect to the USB device, "the bottom line is, they had to get on those thumb drives somehow, and again, it is not by accident. That's a given. Mr. Pirosko would have had to put those on there." R. 60 (Sentencing Hr'g Tr. at 18–19) (Page ID #767–68). This finding was not clearly erroneous. It is common knowledge that a USB drive functions as an external storage device. These drives store files when an individual places those files onto the device. These drives do not come pre-loaded with child pornography.

Pirosko misreads our decision in *United States v. Keefer (Keefer II)*, 490 F. App'x 797 (6th Cir. 2012). In that case, we *upheld* the district court's decision to apply a five-level enhancement. We had originally remanded the case for resentencing, holding that "the evidence at [Keefer's initial] sentencing did not show knowledge of all the images" on his computer. *Id.* at 798 (discussing *United States v. Keefer (Keefer I)*, 405 F. App'x 955, 959 (6th Cir. 2010)). We noted that it was possible for Keefer not to have had knowledge of images of child pornography on his computer's unallocated space. In *Keefer II*, however, the government presented testimony from an agent that "addressed our prior concerns about the general lack of an explanation regarding how images appear in a computer's unallocated space." *Id.* at 800. The agent explained that, although it was possible for images to appear on a computer's unallocated space via accidental viewing, the data on Keefer's computer were not consistent with such an account. *Id.* at 800–01. Keefer failed to offer any sort of explanation in response. *Id.* at

801. *Keefer* thus supports the government's position, not Pirosko's. Moreover, contrary to Pirosko's assertion that "[t]he government presented no evidence at sentencing to prove the USB device's deleted files had ever been accessed or viewed by Pirosko," Appellant Br. at 60, the government's sentencing memorandum contained an exhibit documenting when various files on the USB device had been created, modified, and accessed. *See, e.g.*, R. 53-2 (Exh. B to Gov't Sentencing Mem. at 7) (Page ID #706). The district court did not clearly err in awarding a five-level enhancement for images stored on Pirosko's USB device.

b. Substantive Unreasonableness

Finally, Pirosko contests the substantive reasonableness of his sentence. Pirosko received the statutory maximum of 240 months of imprisonment, a sentence actually below his calculated Guidelines range. Sentences within a defendant's Guidelines range are presumptively substantively reasonable, a presumption that naturally extends to sentences below the Guidelines range. *See United States v. Curry*, 536 F.3d 571, 573 (6th Cir. 2008).

Pirosko has failed to overcome this presumption. The record indicates that the district court sufficiently discussed the various 18 U.S.C. § 3553(a) factors, including the nature and circumstances of his conduct, Pirosko's history and characteristics, the need for the sentence, sentencing disparities, and the need for restitution. We have already concluded that the district court properly calculated Pirosko's Guidelines range. It did not abuse its discretion in according Pirosko the statutory maximum sentence. Pirosko's remaining arguments, regarding the harshness of the Guidelines with respect to child pornography offenders, are likewise unavailing. We have heard these arguments before. *See United States v. Bistline*, 665 F.3d 758, 762–64 (6th Cir. 2012); *United States v. Hill*, 462 F. App'x 586, 588 (6th Cir. 2012); *United States v. Dattilio*, 442 F. App'x 187, 194 (6th Cir. 2011). We cannot, in the context of these cases, hold that the district court abused its discretion here.

III. CONCLUSION

For the foregoing reasons, we **AFFIRM** Pirosko's conviction and sentence.