[PUBLISH]

In the

United States Court of Appeals

For the Eleventh Circuit

No. 24-11308

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

versus

ANDREW EWING,

Defendant-Appellant.

Appeal from the United States District Court
for the Northern District of Florida
D.C. Docket No. 4:23-cr-00042-RH-MAF-1

Before NEWSOM, BRASHER, and WILSON, Circuit Judges.

BRASHER, Circuit Judge:

This appeal raises two issues that often arise in child pornography prosecutions. First, we must address the constitutionality of the government's efforts to gather electronic evidence over a peer-to-peer network. Specifically, we must decide whether law enforcement officers conducted a Fourth Amendment search when they used a special program—Torrential Downpour—to download pornographic images from a BitTorrent user. The Eighth Circuit has held that the government did not conduct a search when it used Torrential Downpour under similar circumstances, *see United States v. Hoeffener*, 950 F.3d 1037 (8th Cir. 2020), and we agree. Second, we must address how a district court should decide whether to show child pornography to a jury during a trial. We again agree with our sister circuits that district courts should be wary about the prejudicial nature of child pornography and should ordinarily review any objected-to pornographic images before ruling on an objection. But, because there was no objection to any specific image in this case, we cannot say the district court abused its discretion when it allowed the government to show a subset of pornographic images to the jury without first viewing those images. Because the district court committed no reversible error, we affirm.

I.

A grand jury charged Andrew Ewing with a single count of knowing possession of child pornography that involved a

prepubescent minor and a minor who had not attained 12 years of age in violation of 18 U.S.C. § 2252A(a)(5)(B), (b)(2). Because this appeal requires an understanding of the technology that the government used to determine that Ewing possessed child pornography, we start with an overview of that technology. Then we turn to the government's specific use of the technology and Ewing's motions to exclude evidence.

A.

BitTorrent is a peer-to-peer file-sharing protocol. It consists of a "distributed network" that allows users to share files for download instead of downloading a file from a single, centralized source. Because the protocol does not rely on a single server, the system is "very efficient" and "adds speed." The protocol is also open source, so numerous software programs use it to download files.

BitTorrent's end user license agreement lets users know that the software will allow other users to download files. To operate, BitTorrent requires, among other things, a torrent file or magnet link, which identifies other users with the sought-after file. After a user downloads a particular torrent file, BitTorrent's tracker associates the device's I.P. address with that file. The torrent file contains instructions to download one or more files. Using the torrent file and a "tracker" algorithm, the program sources and downloads pieces of files from multiple other users and then combines them into the desired content.

Users have control over the files they share, but not who they share them with. Users who possess every piece of a torrent

file and provide access to that file are called "seeders." When a user downloads the entire content of a file, BitTorrent automatically makes a user a "seeder," but a user can opt out of that role. A "sharer" is a user who has some but not all pieces of a file. Even if a user opts out of "seeding," he will still "share" data until he has downloaded the complete file. Users that acquire files, but opt not to provide that content to others, are called "leechers."

To distribute the load of network traffic, BitTorrent uses a "choking" algorithm to encourage downloads of a file from multiple users. As the government's expert defines the term: "[t]o choke is to say my BitTorrent client is no longer going to share with you." Simply put, the algorithm encourages downloading pieces of a file from multiple other computers instead of the entire file from a single computer.

Ewing's expert explained, with an analog example, how the choking algorithm affects a download. Suppose a user could download a bicycle from the BitTorrent network. The user would request a particular bicycle model, and BitTorrent would find manufacturers—"seeders" or "sharers"—of the various components for that desired bicycle model. Even if a single manufacturer could supply both the wheels and frame of the bicycle, the choking algorithm would direct the application to find each part from a different manufacturer. The bicycle would then be pieced together from many different manufacturers, and there would be "no native way to select who you got it from."

Although the choking algorithm ordinarily sources a download from multiple different seeders or sharers, sometimes, a download occurs from a single source. For example, when a user is "the only person in the world" with a file because he "created the content," then another user will download the entire file from that creator user. As the government's expert puts it, despite BitTorrent's choking algorithm, "[s]ingle source downloads happen naturally every day."

When officers want to ensure that a single-source download occurs, they use Torrential Downpour. The software alters the choking algorithm to force a single-source download. Torrential Downpour is not available to the public; it's exclusive to law enforcement. An officer inputs a "hash value"—the unique identifier of each video or photo associated with a child pornography file—into Torrential Downpour, then the software searches publicly available information on BitTorrent. That search returns I.P. addresses that have pieces of the file available for download. Then, the officer inputs that I.P. address into Torrential Downpour to force a single-source download of the file from that I.P. address.

The main reason police use Torrential Downpour is to connect pornographic material with a single I.P. address. This connection allows law enforcement to establish probable cause for a search warrant more easily. But, in the end, the officer "get[s] no more information than" anyone else who was not using Torrential Downpour.

B.

An officer used Torrential Downpour to download files, which contained child pornography, from Ewing's I.P. address. Then the police obtained a warrant and seized Ewing's computer.

At the time of seizure, Ewing's computer no longer had the BitTorrent client that he used when he downloaded the content. But computers store data anytime a user runs the application. So, even though Ewing deleted BitTorrent, "remnants" and "artifacts" from those applications remained on his devices. The police also obtained several other of Ewing's devices, which included files of child pornography.

C.

A grand jury charged Ewing with a single count of knowing possession of child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B), (b)(2).

Ewing sought to suppress the photographs and videos on the grounds that law enforcement violated his reasonable expectation of privacy under the Fourth Amendment. He said that, because he "merely search[ed] for and download[ed] files from other users' computers," he "did not knowingly share his files using BitTorrent." The government opposed that motion, and the district court held an evidentiary hearing on the matter. Two experts testified about BitTorrent's functionality and whether Ewing consented to sharing, meaning whether he was a "seeder," "sharer," or "leecher." The district court expressly found the government's

expert more credible and determined that Ewing had made "this stuff available to members of the public."

The district court issued an order confirming its ruling on the motion in limine. The district court found that "Torrential Downpour does not allow law enforcement access to any information that a user is not already making public." The software "just aggregates or assembles the file pieces differently—from one sharer instead of multiple sharers." Because "[l]aw enforcement's program, Torrential Downpour, did not access or obtain anything that Mr. Ewing was not publicly sharing," the court concluded that Ewing "did not have a legitimate expectation of privacy in computer files he was publicly sharing."

Before trial, Ewing also filed a motion in limine to prevent the government from showing the jury any images of child pornography. Ewing argued that he did not knowingly possess child pornography because he inadvertently downloaded the child pornography while searching for lawful content. But he sought to stipulate to the fact that the images and videos on his devices included "prepubescent minors or a minor who had not attained 12 years of age." He argued that, in light of his willingness to stipulate, the probative value of presenting the images to the jury would be "substantially outweighed by the danger of unfair prejudice" under Rule 403 of the Federal Rules of Evidence. The district court did not review the images or files and denied the motion.

At trial, the government presented snippets of pornographic videos and approximately thirty pornographic photographs. Ewing

renewed his objection, but the district court overruled it. The district court explained, in response to Ewing's objection to a subset of exhibits, that the government's presentation of the images was not "very long at all" and "as respectful" as it could be, rejecting any contention that the evidence was "overkill." In addition to the photos and videos, the government introduced evidence suggesting that Ewing searched for child pornography torrent files near the time the government used Torrential Downpour. The government also introduced evidence that Ewing recently used his desktop computer's media player to play child pornography videos.

After the jury found Ewing guilty, Ewing timely appealed the district court's ruling on his motion to suppress and motion in limine.

II.

Ewing raises two issues on appeal. First, he argues that the government unlawfully searched his computer when it used Torrential Downpour to download child pornography from his I.P. address. Second, he argues that the district court abused its discretion in allowing the government to publish pornographic images to the jury. We address each issue in turn.

A.

We start with whether the use of Torrential Downpour was a "search." The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."

U.S. Const. amend. IV. Absent an exception, a search without a warrant is unreasonable. *Illinois v. McArthur*, 531 U.S. 326, 330 (2001). And no exception to the warrant requirement covers the government's use of Torrential Downpour to download child pornography. So, if the government's action was a "search," that search was unlawful.

There are two ways to assess whether a government action is a "search." *United States v. Gregory*, 128 F.4th 1228, 1240–41 (11th Cir. 2024). First, the government searches an individual when it physically trespasses on an individual's property to obtain information. *United States v. Jones*, 565 U.S. 400, 404 (2012). Second, even without a physical occupation, the government may conduct a "search" if it invades someone's "reasonable expectation of privacy" to gather information. *Katz v. United States*, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

Ewing argues that the government's use of Torrential Downpour was a "search" under both lines of precedent. He says the government trespassed onto his property because Torrential Downpour allowed it to physically intrude on his computer files. And he says that the government used Torrential Downpour to invade his "reasonable expectation of privacy" because it allowed the government to download *entire* files instead of *pieces* of those files. The government argues that both theories fail for the same reason: no one used Torrential Downpour to download anything from Ewing's computer that he did not authorize the public generally to download.

1.

We start with the trespass theory. Ewing contends that the government "remotely intruded" onto his "computer files," which amounted to a trespassory search of his "digital chattel." He further contends that he consented to limited intrusions onto his chattels for a limited purpose, but the government exceeded that consent with the use of Torrential Downpour. We apply a mixed standard of review to this issue, assessing the district court's factual findings for clear error and its application of the law to facts *de novo*. *See United States v. Desir*, 257 F.3d 1233, 1235–36 (11th Cir. 2001).

The government argues that we must review Ewing's trespass theory for plain error because Ewing did not raise it in the district court. But we disagree. In Ewing's motion to suppress, he objected to evidence that he said was obtained from an "illegal search of his computer." It is true that, when explaining why he believed the government's action was a "search," his objection exclusively discussed a right to privacy theory. But Ewing's invocation of the right to privacy theory in the district court does not preclude reliance on a trespass theory on appeal. "Litigants can waive or forfeit positions or issues through their litigation conduct in the district court but not authorities or arguments." *ECB USA, Inc. v. Chubb Ins. Co. of N.J.*, 113 F.4th 1312, 1320 (11th Cir. 2024).

We believe this situation is comparable to the facts of *Yee v. City of Escondido*, 503 U.S. 519, 534 (1992). There, the plaintiff raised a Fifth Amendment "takings" claim in the trial court. Although the plaintiff had argued in the lower court that the government had

physically taken his property, the Supreme Court determined that the plaintiff could also argue on appeal that the government's action was a non-physical regulatory taking. *Id.* The key fact, according to the Court, was that the plaintiff had raised a takings claim in the lower courts, not that he had invoked a particular line of precedent. *See id.* The same is true here. The Supreme Court has explained that "Fourth Amendment rights do not rise or fall with the *Katz* formulation." *Jones*, 565 U.S. at 406. Although Ewing's "new argument is based on a different line of precedents," he makes the "same request" here as he made in the district court—to hold that the use of Torrential Downpour to target his files was a search. *In re Home Depot, Inc.*, 931 F.3d 1065, 1086 (11th Cir. 2019).

With the standard of review cleared up, we move to the merits of Ewing's trespass theory. Ewing argues that the government commits a trespassory search when it uses technology to manipulate a computer to access the information on it. Ordinarily, when an alleged search "involv[es] merely the transmission of electronic signals," we apply a reasonable expectation-of-privacy analysis to determine whether a search has occurred. *Jones*, 565 U.S. at 411. A trespass, on the other hand, usually involves the physical occupation of property. *Id.* at 404. But we will assume without deciding that Ewing is correct that the government commits a *trespassory* search when it uses technology to uncover private information stored on someone's computer or to dispossess someone of their use of the computer.

Even entertaining that assumption, we disagree with Ewing that the government did anything like that here. Three aspects of the government's conduct convince us that it did not commit a trespassory "search," even if it were possible to commit such a search without a physical intrusion onto someone's property.

First, the government used Torrential Downpour to access publicly shared files over a peer-to-peer network, not to hack into Ewing's computer. This use was not an "investigation [that] took place in a constitutionally protected area." *Florida v. Jardines*, 569 U.S. at 1, 7 (2013). Nothing in the record suggests that the government occupied Ewing's "persons, houses, papers, and effects." U.S. Const. amend. IV. Nor did the government bypass BitTorrent's protocols to access information stored on Ewing's private, local drive. The government did not need to intrude or interfere with Ewing's property to access the information it sought because the information it sought was disclosed to all users of the BitTorrent network.

Second, nothing in the record suggests that the government "dispossesse[d]" Ewing of the use of his desktop or "impaired" the desktop's "condition, quality, or value." Restatement (Second) of Torts § 218 (A.L.I. 1965). Again, we will assume without deciding that the digital manipulation of a computer that dispossesses its owner or impairs its use may be characterized as a trespassory search. Even so, Torrential Downpour never prevented Ewing from using his computer or otherwise impaired its use. It merely

requests and receives data that a "seeder" or "sharer" has exposed to the public for download.

Third, the government's investigation was not accomplished through an "unlicensed" intrusion. *Jardines*, 569 U.S. at 7. As Ewing sees it, he consented to sharing bits of data, but he never consented to sharing an entire file. He suggests that because other computers on the network maintained the child pornography files, law enforcement exceeded their "implied license" by downloading the file only from Ewing. Not so. Once Ewing enabled, or perhaps never disabled, the sharing feature on the BitTorrent network, he consented to users downloading content from his computer. He had no control over who downloaded it or whether they downloaded it from a single user or multiple users. Again, assuming without deciding that a digital search beyond the scope of a license could ever be a trespassory search, the government did not exceed the scope of any license here.

We cannot say that the government violated Ewing's Fourth Amendment rights under a trespass theory.

2.

Now to Ewing's argument that the government intruded upon his reasonable expectation of privacy by using Torrential Downpour to download content from his device and identify his I.P. address. Under that line of precedent, Ewing "must establish both a subjective and an objective expectation of privacy." *United States v. King*, 509 F.3d 1338, 1341 (11th Cir. 2007). "The subjective component requires that a person exhibit an actual expectation of

privacy," and "the objective component requires that the privacy expectation be one that society is prepared to recognize as reasonable." *Id.*

Ewing's privacy theory fails for the same reason as his trespass theory. Generally, a defendant has no reasonable expectation of privacy in files exposed to a public network or voluntarily to a third party. *Id.*; *United States v. Trader*, 981 F.3d 961, 967 (11th Cir. 2020). That principle is dispositive to our analysis here.

We have twice held that it is not a "search" when the government accesses electronic information revealed to third parties. In *King*, a defendant inadvertently shared his files on a military base's network such that "everyone on the network had access to all of his files." 509 F.3d at 1339, 1342. Even though the defendant mistakenly believed that his laptop's security settings prevented others from accessing the contents of his hard drive, his expectation of privacy was not objectively reasonable because his "files were exposed to thousands of individuals with network access, and the military authorities encountered the files without employing any special means or intruding into any area which [the defendant] could reasonably expect would remain private." *Id.* at 1342. Likewise, in *Trader*, we held that a defendant had no reasonable expectation of privacy in his email address or his internet protocol address because he had "affirmatively and voluntarily" disclosed them to a third party. 981 F.3d at 967–68. Specifically, the defendant had downloaded and used a messaging application "without taking

available steps to avoid disclosing his internet protocol address" or other information. *Id.*

Our precedents establish that Ewing had no reasonable expectation of privacy in the files here. "[E]veryone on the [BitTorrent] network" had access to Ewing's files because he made them publicly available for download. *King*, 509 F.3d at 1342. BitTorrent relies on a user's consent, like Ewing's, to enable peer-to-peer downloads and eliminate the need for centralized servers. When Ewing connected to the BitTorrent network, he stored his files in a "common area," *id.*, thus making the files available for other users on the network. Perhaps, Ewing mistakenly believed that BitTorrent's algorithm prevented individuals from downloading single-source files. But that subjective expectation is not enough. Whatever he thought he was doing, Ewing "voluntarily" and "affirmatively . . . disclos[ed] his internet protocol address," *Trader*, 981 F.3d at 967, to the BitTorrent network so that, upon a third party's request for a sought-after file, the software's algorithm would source and download content from Ewing, among other users.

The district court found that Ewing made his files publicly available. In other words, he wasn't a "leecher," and we cannot say that finding was clear error. Because Ewing exposed his files to the public on a peer-to-peer network where single-source downloads occur every day, "the expectation of privacy has . . . already been frustrated" by his own volition. *United States v. Jacobsen*, 466 U.S. 109, 117 (1984). And "[o]nce frustration of the original expectation

of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now nonprivate information." *Id.*

Ewing argues that this case is distinguishable from *King* and *Trader* because the government used a program that is available only to law enforcement, Torrential Downpour, to access his files. The Supreme Court has held that a Fourth Amendment search occurs when law enforcement uses "technology" that is "not in general public use" to collect "information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area.'" *Kyllo v. United States*, 533 U.S. 27, 34 (2001) (quoting *Silverman v. United States*, 365 U.S. 505, 512 (1961)); *see also King*, 509 F.3d at 1340 (search was lawful where a "computer specialist did not employ any 'special means' to access [the defendant's] computer"). And Ewing argues that this is exactly what the government did here—use a special program to access information inside his house that it otherwise would not have been able to access.

We disagree. Although Torrential Downpour is "not in general public use," Ewing's argument misunderstands how law enforcement used the program. The government used Torrential Downpour to get around BitTorrent's choking algorithm, which speeds up the download process by sourcing a sought-after file from multiple users across BitTorrent. That Torrential Downpour manipulated the choking algorithm is irrelevant to the "search" question. As the parties' experts explained, BitTorrent users can control the public accessibility of their data by disabling sharing.

But they have no control over how another user accesses the data that they make available. Ewing did not control the choking algorithm or direct the amount of data that he shared or to whom the algorithm sent those files.

The key fact for the purposes of our Fourth Amendment analysis is that Ewing consented to others downloading files from him. Although Torrential Downpour allowed law enforcement to override BitTorrent's choking algorithm, the government was limited to downloading files that Ewing "affirmatively" and "voluntarily" revealed to the public. *Trader*, 981 F.3d at 967. In other words, the "special" tool merely scanned publicly available information. It did not "shrink the realm of guaranteed privacy" by exposing information that was not already broadcast to the public. *Kyllo*, 533 U.S. at 34. Nor did it bypass the BitTorrent protocol to somehow gather information that was hidden to the rest of the public.

Because Ewing made the files available to the public on the BitTorrent network, the use of Torrential Downpour to access that information did not violate his reasonable expectation of privacy.

3.

Finally, we note that our decision is consistent with every circuit to have considered whether the government conducts a "search" when it downloads files that a person shares over a public network. Most on point, the Eighth Circuit held that the government's use Torrential Downpour to trace child pornography files to a defendant did not constitute a search. *United States v. Hoeffener*, 950 F.3d 1037, 1045 (8th Cir. 2020). As that court observed, "[t]he

record reflects that Torrential Downpour searches for download candidates in the same way that any public user of the BitTorrent network searches, and it only searches for information that a user had already made public by the use of the uTorrent software." *Id.* at 1044. A "defendant has no objectively reasonable expectation of privacy in files he shares over a peer-to-peer network, including those shared anonymously with law enforcement officers." *United States v. Shipton*, 5 F.4th 933, 936 (8th Cir. 2021). Other circuits have similarly rejected arguments that a user of a peer-to-peer file-sharing program maintains an objectively reasonable expectation of privacy. *See, e.g.*, *United States v. Weast*, 811 F.3d 743, 747–48 (5th Cir. 2016) (rejecting the argument because the defendant "made the child pornography files and related data publicly available by downloading them into a shared folder accessible through a peer-to-peer network"); *United States v. Ganoe*, 538 F.3d 1117, 1127 (9th Cir. 2008) (reasoning that a defendant's "decision to install and use file-sharing software, thereby opening his computer to anyone else with the same freely available program . . . failed to demonstrate an expectation of privacy that society is prepared to accept as reasonable"); *United States v. Perrine*, 518 F.3d 1196, 1205 (10th Cir. 2008) (explaining that peer-to-peer software that allowed access of defendant's information to outsiders, "vitiate[d] any expectation of privacy he might have in his computer and its contents"); *United States v. Conner*, 521 F. App'x. 493, 497 (6th Cir. 2013) (rejecting a defendant's argument that the government violated his reasonable expectation of privacy when it accessed the files through a peer-to-peer program).

We join these circuits in holding that the use of technology that merely accesses information voluntarily shared over a peer-to-peer network, such as Torrential Downpour, is not a search under the Fourth Amendment

* * *

Because law enforcement neither trespassed onto Ewing's property to obtain information nor invaded his reasonable expectation of privacy, we cannot say that the use of Torrential Downpour to download files from him was a search within the meaning of the Fourth Amendment.

B.

In addition to the suppression issue, Ewing also challenges the district court's decision to allow the government to show child pornography exhibits to the jury. Ewing argues that the district court should have reviewed the objected-to exhibits before ruling on his objections. And he argues that the court should not have shown those exhibits to the jury because the danger of unfair prejudice substantially outweighed any probative value. *See* Fed. R. Evid. 403. We review this issue for abuse of discretion. *See United States v. Dodds*, 347 F.3d 893, 897 (11th Cir. 2003). We believe that neither asserted error is grounds for reversal.

First, we cannot say the district court committed reversible error in failing to review the images before ruling on Ewing's objection. In a child pornography prosecution, pornographic images are often an important part of the government's case. The "force"

of this "graphic evidence" is "beyond simple linear schemes of reasoning." *United States v. Caldwell*, 586 F.3d 338, 343 (5th Cir. 2009). The "actual videos exploiting children in a child pornography case form the narrative" that jurors may expect to "unfold in the courtroom." *Id.* And, if this kind of evidence is not presented, "jurors may very well punish" the government "by drawing a negative inference." *Id.*

Even when this evidence is relevant, however, a district court should exercise care in permitting the government to display images and videos of child pornography because of its potential to inflame the jury. To that end, our sister circuits have held that a district court should ordinarily review any objected-to images before deciding whether to show them to the jury. *See United States v. Cunningham*, 694 F.3d 372, 386 (3d Cir. 2012) ("[W]e conclude that, speaking generally, a district court should personally examine challenged evidence before deciding to admit it under Rule 403."); *United States v. Loughry*, 660 F.3d 965 (7th Cir. 2011) (same); *United States v. Curtin*, 489 F.3d 935, 958 (9th Cir. 2007) (en banc) ("One cannot evaluate in a Rule 403 context what one has not seen or read."). We agree. A district court should ordinarily review pornographic images or a detailed description of those images before ruling on an objection to those images under Rule 403.

Nonetheless, we cannot say the district court committed reversible error by failing to review the images in this case. Ewing never objected to any specific images. Before the district court, he sought to prohibit the government from showing any child

pornography to the jury, or, alternatively, he requested that the district court arbitrarily limit the number of images. Had Ewing made a specific objection that notified the district court about particular images or videos he sought to exclude and explained his rationale, the district court could have reviewed the objected-to files before ruling on his objection. But we cannot say the district court erred in denying his general objection without first reviewing specific images.

Moreover, even if the district court had committed an error in this regard, the error would be harmless. Ewing has not argued that the government selectively introduced images that were not a representative sample of the files on his devices. Nor has he suggested that the government presented particularly egregious photographs or videos to the jury. And, after viewing the evidentiary presentation at trial, the district court reaffirmed its decision to show the images to the jury. Specifically, after the first day of trial, the court described the government's presentation of the images as not "very long at all" and "as respectful" as it could be, rejecting any contention that the evidence was "overkill."

Second, we cannot say the district court misapplied Rule 403 when it determined that the probative value of exposing this evidence to the jury was not substantially outweighed by its prejudicial effect. Ewing was charged with a single count of knowing possession of child pornography that involved a prepubescent minor and a minor who had not attained 12 years of age. *See* 18 U.S.C. § 2252A(a)(5)(B), (b)(2). In similar cases, we have allowed the

government to introduce a representative sample of pornographic images to "show that the images actually were child pornography" and "that [the defendant] knew the images were child pornography." *United States v. Dodds*, 347 F.3d 893, 896, 899 (11th Cir. 2003); *see also United States v. Alfaro-Moncada*, 607 F.3d 720, 734 (11th Cir. 2010) (permitting the publication of five still images of child pornography to prove a disputed fact that the defendant knew that he was in possession of child pornography).

Here too, the photographs and videos are probative of whether Ewing "knowingly" possessed child pornography that included a prepubescent minor or minor who had not attained 12 years of age. 18 U.S.C. § 2252A(a)(5)(B), (b)(2). Because Ewing argued that he inadvertently downloaded the content, the quantity and substance of those photographs and videos tended to disprove that contention. *See Dodds*, 347 F.3d at 899. Especially in light of the government's relatively limited presentation, the district court did not abuse its discretion when it concluded that the probative value of this evidence outweighed any unfair prejudice. *See* Fed. R. Evid. 403.

III.

Because the district court did not err in finding that the government did not perform an unlawful search or abuse its discretion in permitting the government to publish the child pornography exhibits, we **AFFIRM** the judgment of the district court.