In the

United States Court of Appeals

For the Seventh Circuit

No. 23-2207

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

WARREN SIEPMAN,

Defendant-Appellant.

Appeal from the United States District Court for the
Northern District of Illinois, Eastern Division.
No. 18-cr-130 — **Harry D. Leinenweber**, *Judge*.

ARGUED MAY 13, 2024 — DECIDED JULY 11, 2024

Before SCUDDER, ST. EVE, and PRYOR, *Circuit Judges*.

ST. EVE, *Circuit Judge*. On three separate occasions, an automated government software program accessed and downloaded child pornography from Warren Siepman's computer over a peer-to-peer file sharing network. The central issue in this appeal is whether that amounts to "transportation" of child pornography under federal law. It does.

I. Background

A. Factual Background

In late 2016, Homeland Security Investigations ("HSI") agents began investigating individuals making child pornography available to others on the internet over peer-to-peer file sharing networks. Peer-to-peer file sharing programs enable computer users to share and receive electronic files over the internet with a network of others. *See United States v. Clarke*, 979 F.3d 82, 87 (2d Cir. 2020). The name "peer-to-peer" comes from the network created when two or more computers connect directly with each other, without going through a separate server. *See generally Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913, 919–20 (2005). Users of a peer-to-peer file sharing network can search for files that others have made available, browse files that a specific user has made available, and download files directly from other users. *See United States v. Husmann*, 765 F.3d 169, 171 (3d Cir. 2014). Users can also make their own files accessible to others, usually by placing them in a designated folder available to the network's users. *Id.* When one user makes files available to others, however, those files remain local on the user's computer until another user accesses and downloads them. *Id.*

HSI agents here used a proprietary peer-to-peer software program called "eMule" that they engineered to search for specific child pornography files others were making available over a peer-to-peer network. The program combed the network by querying the unique alphanumeric identifiers (known as "hash-IDs"—essentially, the files' digital fingerprints) of already-known child pornography files. Once the program identified a known child pornography file that a network user had made available, it connected to that user's

computer and downloaded the entire file. The program's search and download functions operated without human intervention, and it ran constantly on a secure government computer in a locked room during the yearslong investigation. Law enforcement monitored its activity several times per day.

Using this program, an HSI agent discovered that Warren Siepman made child pornography available to others for download on a peer-to-peer file-sharing network called "Shareaza." Between October 2016 and March 2017, the program identified and then downloaded child pornography from an IP address associated with Siepman on three separate occasions. Forensic examination of hard drives later seized from Siepman revealed over one thousand child pornography files and showed that the computer's user had searched for child pornography on Shareaza. Siepman, in an interview prior to his arrest, also admitted to viewing child pornography on his computer, using Shareaza to view and download child pornography, and knowing that he was sharing files with others on the network.

B. Procedural Background

A grand jury indicted Siepman, charging him with three counts of transportation of child pornography, 18 U.S.C. § 2252A(a)(1), and one count of possession of child pornography, 18 U.S.C. § 2252A(a)(5)(B). The three transportation counts stem from the three specific files the government downloaded from Siepman's computer between October 2016 and March 2017.

The case proceeded to trial, at which the court instructed the jury on the elements of the transportation charge. That instruction directed the jury to return a guilty verdict if it found

beyond a reasonable doubt that (1) Siepman knowingly transported the material identified in the indictment using any means or facility of interstate commerce; (2) the material was child pornography; and (3) Siepman knew that the material depicted one or more actual minors engaged in sexually explicit conduct. *See* Seventh Cir. Pattern Crim. Jury Instructions (2021), 18 U.S.C. § 2252A(a)(1), pg. 914.

In addition to that instruction, the government sought an instruction defining the term "transports" in the peer-to-peer file sharing context. Siepman objected, arguing that it was unnecessary and likely to confuse the jury. The court overruled Siepman's objection and gave the following instruction:

> An individual transports a computer file by computer when he knowingly makes the computer file available for others to download using peer-to-peer file sharing [] and another individual downloads that computer file.

The jury found Siepman guilty on all four counts.

After trial, Siepman moved for a judgment of acquittal notwithstanding the verdict or, alternatively, for a new trial. *See* Fed. R. Crim. P. 29(c), 33(a). The motion primarily concerned the transportation counts. As relevant here, Siepman argued that the district court erred in its jury instruction defining "transports," and that in any event, the evidence was insufficient to prove "another individual" downloaded the files from his computer since the government relied on automated software to conduct its investigation.

The district court denied the motion, finding the instruction legally accurate and the evidence sufficient. As to Siepman's sufficiency argument, the court determined "an

individual" had downloaded the files on the grounds that software "can never operate independent of human design," a human "wrote and initiated the software," and an individual then received the image, reviewed it, and identified it as child pornography.

Siepman now appeals.

II. Analysis

This appeal concerns only Siepman's convictions for transporting child pornography. As below, he contends that the district court erred in its instruction to the jury defining "transports," and that the evidence was insufficient to convict him of that crime. Both arguments really get at a single question: whether Siepman's actions amount to "transportation" within the meaning of § 2252A(a)(1) where, as here, the government employs automated software to download the illicit material from the defendant over a peer-to-peer file sharing network. With that in mind, we take each alleged error in turn.

A. Jury Instruction

We review the legal accuracy of jury instructions de novo, but we evaluate their particular phrasing for abuse of discretion. *United States v. Edwards*, 869 F.3d 490, 496 (7th Cir. 2017). The district court enjoys "substantial discretion" in formulating its instructions. *United States v. Dickerson*, 705 F.3d 683, 688 (7th Cir. 2013) (quoting *United States v. Noel*, 581 F.3d 490, 499 (7th Cir. 2009)). If those instructions accurately reflect the law, we will reverse only if it appears that the instructions both misled the jury and prejudiced the defendant. *United States v. White*, 95 F.4th 1073, 1079 (7th Cir. 2024); *Dickerson*, 705 F.3d at 688. We review the district court's decision to give or refuse

to give a particular instruction for abuse of discretion. *United States v. Campos*, 541 F.3d 735, 744 (7th Cir. 2008).

The district court instructed the jury that an individual satisfies the "transport" element of § 2252A(a)(1) "when he knowingly makes the computer file available for others to download using peer-to-peer file sharing [] and another individual downloads that computer file." That instruction accurately reflects the law and the plain meaning of "transport" in the peer-to-peer network file sharing context.

"Transport" means moving something "from one place to another." Merriam-Webster's Collegiate Dictionary (10th ed. 1994); *see also transport*, Black's Law Dictionary (6th ed. 1990) ("To carry or convey from one place to another."). An internet-connected computer can act as an agent of transportation, just like any car on the road or plane in the air. *See United States v. Chaparro*, 956 F.3d 462, 470 (7th Cir. 2020) ("[T]he images on the hard drive were downloaded from the Internet, so the Internet transported them."). So, when a file moves from one computer to another over the internet, it is "transported" within the meaning of § 2252A(a)(1). *See Clarke*, 979 F.3d at 93 ("The use of the Internet to move video files from [the defendant's] computer to the government agents' computer constituted transportation using a means or facility of interstate commerce within the meaning of § 2252(a)(1)."). We have accordingly affirmed child pornography transportation convictions under § 2252A(a)(1) where the defendant uploaded the illicit materials to a website, *see United States v. Davis*, 859 F.3d 429, 434 (7th Cir. 2017), or sent them over email, *see United States v. Tenuto*, 593 F.3d 695, 697 (7th Cir. 2010).

Nothing about the mechanics of peer-to-peer file sharing changes the basic principle that computer-to-computer movement constitutes transportation. When a defendant makes a file available to a network of others from a computer in one location, and another user then accesses and downloads that file onto his own computer in another location over a peer-to-peer network, the defendant has caused that file to be "transported," just as surely as if he uploaded it to a website or sent it over email. As the Second Circuit explained in reaching the same conclusion in *United States v. Clarke*:

> by knowingly and intentionally joining the file-sharing network, downloading files from the computers of other network users to his own, storing those files in a folder that was shared with other network users, and maintaining his folder's connection to the network, [the defendant] himself perform[s] actions that would constitute the crime of knowing transportation of the files when, as anticipated, another user of the file-sharing network caused the files to be downloaded and sent from his computer to the other user's computer.

979 F.3d at 94. The district court therefore made no error in instructing the jury as it did.

Siepman nevertheless contends the district court erroneously based its instruction on cases dealing with the "distribution" of child pornography under 18 U.S.C. § 2252(a)(2). *See, e.g.*, *United States v. Owens*, 18 F.4th 928, 930–31 (7th Cir. 2021) (holding that "[i]t 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

filesharing network" (citing *United States v. Ryan*, 885 F.3d 449, 453 (7th Cir. 2018))). That was problematic, he argues, because we have previously rejected attempts to equate "distribution" with "transportation." *See United States v. Hyatt*, 28 F.4th 776, 785 (7th Cir. 2022).

But *Hyatt*, on which Siepman relies, does not stand for the idea that "transportation" and "distribution" can never overlap. There we simply rejected the government's proposition that *every* act of transportation "is, *ipso facto*, an act of distribution." *Id.* at 783. We did not hold that the same set of facts could not support both distribution and transportation convictions such that the instructions on their operative verbs cannot resemble each other in some cases. In fact, they can. And in this case, they do.

Although "separate crimes," distribution and transportation offenses are "closely connected." *Tenuto*, 593 F.3d at 697. As we have said before, "a person who has distributed child pornography has likely transported it, and a person who transports it is likely to eventually distribute it." *Id.* Here, Siepman's conduct could have triggered either offense. By making child pornography available over the network to government agents who then downloaded it, Siepman both distributed child pornography (to government agents) and transported it (to another computer). *See, e.g.*, *Owens*, 18 F.4th at 930–31; *United States v. Chiaradio*, 684 F.3d 265, 282 (1st Cir. 2012) ("When an individual consciously makes files available for others to take and those files are in fact taken, distribution has occurred."). That the district court's instruction might have worked equally well for both offenses does not make it wrong.

We find no error in the district court's decision to give the instruction in the first place, either. While Siepman complains that the jury could have gone without the instruction, the district court did not abuse its discretion in opting to explain, in line with our caselaw, the term as it applied to the unique technological context of peer-to-peer file sharing. There is no evidence that the ensuing instruction confused the jury.

B. Sufficiency of the Evidence

We next consider whether there was sufficient evidence to support the transportation convictions. Our review on that front is de novo, but highly deferential. *United States v. White*, 95 F.4th 1073, 1078 (7th Cir. 2024). "[W]e review the evidence presented at trial in the light most favorable to the government and draw all reasonable inferences in its favor." *United States v. Hidalgo-Sanchez*, 29 F.4th 915, 924 (7th Cir. 2022) (quoting *United States v. Anderson*, 988 F.3d 420, 424 (7th Cir. 2021)). "Ultimately, we 'will overturn a conviction only if, after reviewing the record in this light, we determine that no rational trier of fact could have found the essential elements of the offense beyond a reasonable doubt.'" *Id.* (quoting *Anderson*, 988 F.3d at 424).

Siepman fails to meet this burden. Relying on the court's "transports" instruction, Siepman contends there was no evidence that "another individual" downloaded the files because the government's automated software did the downloading. We disagree. A government agent initiated the software, kept tabs on the investigation's progress by checking its results at least twice a day, and then reviewed and maintained logs recording communication between the government's computer and Siepman's. A jury could reasonably find that "an individual" downloaded the files based on this human activity.

That automated software did the heavy lifting of searching for and downloading the illicit material does not remove the government agent from the equation. *See Owens*, 18 F.4th at 931 (acknowledging the government's "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"). The software may be automated, but it is not sentient. It required a government agent to program it, dispatch it, and monitor its progress. We would ignore reality to attribute the program's every act entirely to a computer and thus find it inappropriate to draw parallels between this case and the civil cases involving robocalls and bot activity on which Siepman relies. Viewed in the light most favorable to the government, the level of human involvement here is more than enough to sustain the conviction.

Moreover, requiring a government agent to manually click "download" would do no more than draw an artificial line between human activity and computer activity. We would never say that a defendant has not "transported" child pornography over email on the basis that the email client (Gmail, or its ilk), rather than the defendant, accessed the internet and executed the transfer. *See Tenuto*, 593 F.3d at 697. Nor would that result change if the defendant drafted the email, but then programmed it to send automatically days later. In both scenarios, "an individual" executed the act in question. There is no reason to reach a different conclusion in this case.

In any event, we would sustain Siepman's convictions even if the software was solely responsible for the download activity. Unlike a distribution conviction under § 2252A(a)(2), a transportation conviction under § 2252A(a)(1) does not

require another person to have received the illicit material—the government need only show that the defendant moved child pornography or caused it to be moved. *See Hyatt*, 28 F.4th at 783 ("A person can 'transport' an item without distributing it to anyone."); *United States v. Fall*, 955 F.3d 363, 374 (4th Cir. 2020) ("[Transportation] does not require conveyance to another person."). As applied to the peer-to-peer file sharing context, that movement can occur regardless of who, or what, does the downloading. Here Siepman does not contest that a download occurred. It is therefore irrelevant whether we attribute that download to person or program—either way, the files started on Siepman's computer and ended up on the government's after Siepman made them available. Those facts alone suffice to uphold the convictions.

AFFIRMED