No. _____

IN THE

SUPREME COURT OF THE UNITED STATES

Warren Siepman
_____ — PETITIONER
(Your Name)

VS.

United States of America
_____ — RESPONDENT(S)

MOTION FOR LEAVE TO PROCEED *IN FORMA PAUPERIS*

The petitioner asks leave to file the attached petition for a writ of certiorari without prepayment of costs and to proceed *in forma pauperis.*

Please check the appropriate boxes:

☒ Petitioner has previously been granted leave to proceed *in forma pauperis* in the following court(s):

United States Court of Appeals for the Seventh Circuit

United States District Court, Northern District of Illinois

☐ Petitioner has **not** previously been granted leave to proceed *in forma pauperis* in any other court.

☐ Petitioner's affidavit or declaration in support of this motion is attached hereto.

☒ Petitioner's affidavit or declaration is **not** attached because the court below appointed counsel in the current proceeding, and:

☒ The appointment was made under the following provision of law: 18 U.S. Code § 3006A (c), or

☒ a copy of the order of appointment is appended.

Adam Sheppard
(Signature)

IN THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF ILLINOIS

USA	)	Case No: 18 CR 130
v.	)	Judge: Harry D. Leinenweber
Warren Siepman	)	

ORDER

Defendant's motion for leave to appeal in forma pauperis is granted [140].

Date: 7/6/23

/s/ Judge Harry D. Leinenweber

No. 24-_____

IN THE SUPREME COURT OF THE UNITED STATES

Warren Siepman,

Petitioner

vs.

United States of America,

Respondent.

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SEVENTH CIRCUIT

PETITION FOR A WRIT OF CERTIORARI

Adam Sheppard
Barry Sheppard
Sheppard Law Firm, P.C.
180 N. LaSalle, Suite 2510
Chicago, IL 60601
(312) 443-1233
Adam@Sheppardlaw.com
Barry@Sheppardlaw.com
Attorneys for the
Defendant-Appellant, Warren Siepman

QUESTION PRESENTED

Whether a conviction for transportation of child pornography under 18 U.S.C. § 2252A(a)(1), based on a defendant's use of a peer-to-peer program, requires another person to have downloaded the illicit material or whether the government need only show that the defendant made the material available to be downloaded by another computer?

PARTIES TO THE PROCEEDING

Petitioner is Warren Siepman, the defendant in the proceedings before the district court. Respondent is the United States of America.

CORPORATE DISCLOSURE STATEMENT

There is no parent or publicly held company owning 10% or more of the corporation's stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

DIRECTLY RELATED PROCEEDINGS

United States District Court

United States v. Warren Siepman, 18 CR 1030 (N.D. Ill.)
Judgment entered June 27, 2023

United States Court of Appeals for the Seventh Circuit

United States v. Warren Siepman, No. 23-2207
Judgment entered July 11, 2024

PETITION FOR A WRIT OF CERTIORARI

Petitioner Warren Siepman respectfully requests the issuance of a writ of certiorari to review the judgment of the United States Court of Appeals for the Seventh Circuit.

DECISION BELOW

The decision of the United States Court of Appeals for the Seventh Circuit is published at 107 F.4th 762 (7th Cir. 2024), and is reproduced at Pet. App. 1a.

JURISDICTION

The Seventh Circuit entered judgment on July 11, 2024. See Pet. App. 1a.. This Court's jurisdiction is invoked under 28 U.S.C. § 1254.

STATUTE INVOLVED

18 U.S.C. § 2252A(a)(1): Certain activities relating to material constituting or containing child pornography.

(a) Any person who--

> (1) knowingly mails, or transports or ships using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, any child pornography;
>
> ***
>
> shall be punished as provided in subsection (b).

18 U.S.C.A. § 2252A(A)(1).

STATEMENT OF THE CASE

A four-count indictment charged Mr. Siepman with transporting child pornography, in violation of Title 18, United States Code, Section 2252A(a)(1) (counts one through three) and possessing child pornography, in violation of Title 18, United States Code, Section 2252A(a)(5)(B) (count four). DE 147 [1]at 6, 18, 77. The charges were based on Mr. Siepman's use of a peer-to-peer network, Shareaza. Mr. Siepman did not send any file to any person; however, the settings on his version of Shareaza allowed other computers to access the files that he had downloaded to his computer. Following a jury trial, Mr. Siepman was convicted of each count. DE 149 at 428.

Prior to trial (in pretrial pleadings), in opening statements, and in closing arguments, Mr. Siepman admitted that he possessed child pornography (count four of the indictment); the sole issue at trial – and on appeal – was whether his conduct fit the legal definition of "transportation." DE at 93 at 2; 147 at 83-85; 149 at 381; *U.S. v. Siepman,* 107 F.4th 762 (7th Cir. 2024).

The overarching issue on appeal, which has yet to be resolved by this Court, was 1) whether a conviction for "transportation" required the government to prove that "another individual" actually downloaded the files; and 2) whether "another individual" downloaded the files where a pre-programmed, unmanned, software on the government's computer, that is unavailable to the public, located and downloaded the images. The court of appeals held that 1) the level of human

[1] DE refers to "docket entries" in the District Court which also served as the record on direct appeal.

intervention that the government used in this case – by having an agent program the computer in the first place and monitor its findings – was sufficient to another establish the element of "another individual download[ing]" the files; and 2) the government was not even required to prove that "another individual" downloaded the files; rather,"the government need only show that the defendant moved child pornography or caused it to be moved. *Siepman,* 107 F.4th at 768.

Mr. Siepman petitions for writ on grounds that this case presents an important question of federal law in the digital era that has not be resolved.

I. Trial Testimony Regarding Peer-to-Peer Networks

The testimony of two witnesses at trial relate to the issues in this petition. Detective Rich, associated with an FBI task force, testified as an expert in computer forensics and peer-to-peer file sharing technology. DE 147 at 105-106. Special Agent Michael Ploessl from Homeland Security then testified to the government's use of the peer-to-peer network that it used in this case to locate and download the files from Mr. Siepman's computer. DE 147 at 165.

Detective Rich, through the use of exhibits, walked the jury through the installation process of a generic version (not the defendant's version) of Shareaza and showed the jury how to use Shareaza, which was a program that Mr. Siepman was using. DE 147 at 100-119. Detective Rich testified that when users "seek out the files using a *search term*, they are provided back with a list of files that would be available based upon their connections. They can either choose to do nothing or they can choose to attempt to download the file from those clients making it available."

DE 147 at 98 [Emphasis added].

On cross-examination, Detective Rich clarified "that a user doesn't actually share a file until the file is called for by another user. So the files reside on the user's -- on user A's computer, let's say, until user B decides he wants that file. And then the two computers, the peers connect, communicate with each other and then make -- user A makes that file available to user B." DE 147 at 136. Detective Rich further explained that just because a person uses Shareaza it does not necessarily mean that they are sharing files. DE 147 at 140. Shareaza is not a "network;" it does not "share" files; it is "merely a client [i.e., a program] that enables the communication between the networks . . . Shareaza is just a means to an end. It's a means to share the files but not necessarily sharing the files." DE 147 at 140. A user could set up Shareaza, remove file-sharing folders from Shareaza, and Shareaza would still run on the user's computer. DE 147 at 147.

Detective Rich acknowledged that he never examined Mr. Siepman's computer. DE 147 at 131-132. He strictly reviewed the program network itself; his review was "not case related." DE 147 at 133. He "didn't look at any of the case facts." DE 147 at 141. Detective Rich did not know how Mr. Siepman used the program. DE 147 at 142.

Detective Rich further testified as to the time it takes for one network to upload a file from another network. DE 147 at 144-145. He testified that a picture could take 10 seconds to upload and that if a user does not "X" out the upload in those 10 seconds, then the photo is uploaded. DE 147 at 144-145.

Special Agent Michael Ploessl from Homeland Security then testified. DE 147 at 165. Agent Ploessl had been "using the peer-to-peer network eMule to conduct an investigation looking for clients or individuals sharing child pornography on the internet." DE 147 at 165. Agent Ploessl was trained on the law enforcement version of eMule to conduct such investigations. DE 147 at 165. This type of program was not the type that anyone could download. DE 147 at 165. When asked, on direct examination, what makes the law enforcement software different than other peer-to peer file sharing software another user might have, Agent Ploessl stated, "[i]t would only seek to download files containing child pornography from other individuals." DE 147 at 165.

Agent Ploessl further explained that the program "would look for the child pornography based off of a hash ID, and then once the hash IDs were already known child pornography images, it would download. And then once you receive the file, it identifies the IP address that file is coming from." DE 147 at 165. "A hash ID is a unique alphanumeric identifier for a digital file. So a digital file has -- it's like a fingerprint for that file." DE 147 at 166. The "law enforcement version" of this peer-to peer network "seeks those hash IDs from individuals sharing those IDs, those child pornography images or videos on the peer-to-peer network." DE 147 at 166.

Agent Ploessl reiterated that the software that he used, Roundup eMule version 1.54, is "law enforcement software for the eMule network." DE 147 at 169. The government asked Agent Ploessl whether that "law enforcement-specific" eMule version that he used during this investigation (2016-2017) has since become

publicly available and Agent Ploessl responded, "I don't believe so." DE 147 at 169. Agent Ploessl then demonstrated how the law enforcement program established a connection with Mr. Siepman's computer. DE 147 at 173-177.

The government asked Agent Ploessl whether there was "an actual person to person dialogue between you and the defendant at this point;" and he responded, "[n]o." DE 147 at 173. Rather, the computers were talking to each other, without human intervention. DE 147 at 173, 177, 174 ("the two computers were communicating on the network").

Agent Ploessl then testified regarding an exhibit that showed an instance when the law enforcement program identified and downloaded a file from Mr. Siepman's computer; he explained it as follows: "It's the computers are talking again, and it's sending a request to start downloading the file from the remote client, the defendant's computer." DE 147 at 177.

On cross-examination, Agent Ploessl testified that he was not involved with programing the law enforcement software that was used to search for child pornography. DE 148 at 200. He further testified that the law enforcement software is only available to law enforcement agencies, not the general public. DE 148 at 200. The machine that runs the software sits in a secured room. DE 148 at 201. One reason that the machine is kept in a secured room is to protect it from "human interference." DE 148 at 201. The machine could run "without a person." DE 148 at 201.

When the software found the files in question, the machine was running

automatically; Agent Ploessl was not at the machine. DE 148 at 201. The machine ran automatically for close to three years and was left on for 24 hours a day, seven days a week. DE 148 at 202. As the machine runs, it looks for known hash values; if it identifies hash values, it will attempt to connect to the computer from which those hash values were identified. DE 148 at 202-203. The software then downloads the images. *Id.* This all can occur without a person at the law enforcement computer or defendant's computer. DE 148 at 203.

Agent Ploessl was asked about the time that it took for the law enforcement computer to connect to Mr. Siepman's computer and download the files that were the subject of the indictment. DE 148 at 206-209. As for the image in count one, the connection and download occurred in less than a second. DE 148 at 206. As for the video file in count two, the connection and download occurred in less than four minutes (videos can take longer to download than images). DE 148 at 207-209. As for the image in count three, the connection and download occurred in less than four seconds. DE 148 at 209-210.

II. Jury Instructions

Following the close of testimony, the parties proceeded to a jury instructions conference. DE 148 at 343. Over the defendant's objection, the district court defined the phrase, "transports a computer files," as follows: "[a]n individual transports a computer file when he knowingly makes it available for others to download using peer-to-peer file sharing and another individual downloads the computer file." DE 100 at 19; DE 101; DE 104; DE 149 at 346.

Mr. Siepman was convicted at trial. Mr. Siepman appealed the conviction to the Court of Appeals for the Seventh Circuit. The Seventh Circuit had jurisdiction over this appeal pursuant to 28 U.S.C. § 1291.

On appeal, Mr. Siepman argued that 1) the district court abused its discretion in defining the terms, "transports," when that phrase has an ordinary meaning; and; 2) to prove "transportation," the government was required to prove that "another individual" downloaded the files from defendant's computer and the evidence was insufficient of such in this case. *Siepman*, 104 F.4th 765.

III. The Seventh Circuit's Decision

The Seventh Circuit framed the issue as follows:

> 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.

Id.

The Seventh Circuit held that, "[v]iewed in the light most favorable to the government, the level of human involvement here is more than enough to sustain the conviction." *Id.* at 767. Moreover, the Seventh Circuit stated, "[i]n any event, we would sustain Siepman's convictions even if the software was solely responsible for the download activity." *Id.* at 768. The court explained:

> 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. [inner citations omitted]. 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.

Id.

This petition for writ of certiorari follows

REASON FOR GRANING THE WRIT

This Court Should Grant Certiorari to Define "Transportation;" Many Modern Transportation Cases Involve File Sharing Networks and the Question of What Constitutes "Transportation" in the Digital Era Remains Unsettled

Under Supreme Court Rule 10(c), where, as here, a United States court of appeals has decided an important question of federal law that has not been, but should be, settled by this Court, that may be a basis for granting certiorari. S.Ct.R.10(c). Based on the reasons set forth below, this case satisfies the criteria in Rule 10(c).

"Peer-to-peer file sharing programs attracted hundreds of millions of users in the early 2000s, but have struggled to find legal footing because they often facilitate the unauthorized distribution of copyrighted material." *United States v. Carroll*, 886 F.3d 1347, 1350, fn.1 (11th Cir. 2018) (citing, *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913, 913, 125 S. Ct. 2764, 2766 (2005)). Moreover, in the context of child pornography cases, the offense of "transportation" is often charged in peer-to-peer file sharing networks. *E.g., Siepman,* 107 F.4th at 765-766 (citing other transportation cases in the peer-to-peer context). While other courts of appeals have upheld transportation convictions under similar factual circumstances, no cases from this Court have considered the argument by Siepman: whether a transportation conviction requires proof that "another individual" actually downloaded the images which the defendant allegedly made available on a peer-to-peer network (as opposed to a scenario where a computer program, unavailable to the public, automatically does the downloading). Nor did the Seventh

Circuit in this case cite any precedent from this Court on this issue. *See id.*

Legal research regarding recent transportation cases reveals that litigants and courts alike are seeking a clear definition of "transportation" in the digital era. For example, on September 16, 2024, a defendant in the District of South Dakota "raised the issue of what conduct amounts to 'transportation' of child pornography." *United States v. Echols*, No. 4:24-CR-40019, 2024 WL 4241276, at *2 (D.S.D. Sept. 19, 2024). On January 3, 2024, a district court in the Eastern District of New York noted:

> The Second Circuit has not squarely addressed whether a defendant may be charged with "knowingly transporting" child pornography under 18 U.S.C. § 2252(a)(1) where the defendant has uploaded child pornography to a web-based storage platform to which others did not have access.

United States v. Carver, No. 22-CR-316 (JS), 2024 WL 36988, at *5 (E.D.N.Y. Jan. 3, 2024).

Additionally, pattern jury instructions do not define "transportation" in the context of child pornography cases. *See e.g.*, Seventh Circuit Criminal Jury Instructions 2020 edition at 811;[2] Pattern Criminal Jury Instruction for the District Courts of the First Circuit at 268.[3]

The consequences of a conviction for "transportation" also merit guidance on this issue. "Transportation" carries a mandatory minimum term of imprisonment of

---

[2] Available at https://www.ca7.uscourts.gov/patternjuryinstructions/pattern_criminal_jury_instructions_2020edition.pdf))

[3] Available at https://www.rid.uscourts.gov/sites/rid/files/juryinstructions/criminal/Pattern%20Criminal%20Jury%20Instructions.pdf.

five years, 18 U.S.C. § 2252A(a)(1). In contrast, the charges of "access with the intent to view" and "possession" of child pornography carry no mandatory minimum. *See* §§ 2252A(a)(2)(B), (a)(5)(B), (b)(1), (b)(2). Those charges also carry a lower base offense level than "transportation." *See* USSG §2G2.2(a)("transportation" carries a base offense level of 22 and possessions/accessing-with-the-intent-to-view carry a base offense level of 18).

Based on the foregoing, the issue – whether an individual "transports" child pornography via a file-sharing network even if another individual does not download it – warrants this Court's review.

CONCLUSION

Mr. Siepman respectfully requests that this Court issue a writ of certiorari.

Respectfully submitted:

/s/ Adam J. Sheppard
An Attorney for Defendant

ADAM SHEPPARD
SHEPPARD LAW FIRM, P.C.
180 North LaSalle Street, Suite 2510
Chicago, Illinois 60601
(312) 443-1233
IL. Bar. No. 6287375

APPENDIX

107 F.4th 762
United States Court of Appeals, Seventh Circuit.

UNITED STATES of America, Plaintiff-Appellee,
v.
Warren SIEPMAN, Defendant-Appellant.

No. 23-2207
|
Argued May 13, 2024
|
Decided July 11, 2024

Synopsis

Background: Defendant was convicted in the United States District Court for the Northern District of Illinois, Harry D. Leinenweber, J., of transportation of child pornography and possession of child pornography, and he appealed.

Holdings: The Court of Appeals, St. Eve, Circuit Judge, held that:

defendant satisfied "transport" element of federal statute prohibiting transport of child pornography, and

there was sufficient evidence that another individual downloaded files containing child pornography to support defendant's transportation conviction.

Affirmed.

Procedural Posture(s): Appellate Review; Post-Trial Hearing Motion.

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

Attorneys and Law Firms

Richard Michael Rothblatt, Attorney, Office of the United States Attorney, Chicago, IL, for Plaintiff-Appellee.

Adam J. Sheppard, Attorney, Sheppard Law Firm, P.C., Chicago, IL, for Defendant-Appellant.

Before Scudder, St. Eve, and Pryor, Circuit Judges.

Opinion

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, 125 S.Ct. 2764, 162 L.Ed.2d 781 (2005). Users of a peer-to-peer file sharing network can ***764** 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 ***765** 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 "transpot" 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 ***766** 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 *767 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. *768 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

All Citations

107 F.4th 762

End of Document