United States Court of Appeals
For the Eighth Circuit

No. 20-2570

United States of America

Plaintiff - Appellee

v.

Christopher Allen Shipton

Defendant - Appellant

Appeal from United States District Court
for the District of Minnesota

Submitted: June 16, 2021
Filed: July 23, 2021

Before GRUENDER, ARNOLD, and STRAS, Circuit Judges.

ARNOLD, Circuit Judge.

After a police officer downloaded part of a computer file containing child pornography on a peer-to-peer network from an IP address connected to Christopher Shipton, investigators searched his home and digital devices and uncovered additional illicit files, and so the government charged him with two counts of possessing child pornography. *See* 18 U.S.C. § 2252(a)(4)(B), (b)(2). Shipton moved

to suppress the evidence gathered during the search on the ground that the officer who downloaded the file had conducted a warrantless search in violation of the Fourth Amendment. He also requested that the software the officer used to facilitate the sharing be tested to ensure it was reliable and that it did not gain access to private areas of Shipton's computer. The district court[1] denied Shipton's motion and request, and he appeals. We affirm.

As many of our cases on the subject have shown, peer-to-peer networks provide common forums for those who trade child pornography on the internet. Users may connect to a peer-to-peer network and share files on their computer with others. Law enforcement agencies have developed programs that mimic ordinary users of peer-to-peer networks that are designed to help identify child-pornography purveyors. Like ordinary participants in the network, officers can search for and obtain child pornography from other users. But they can also compare a retrieved file's "hash value," which is essentially a particular file's digital signature, with the hash values of files known to contain child pornography. When the values match, investigators can pretty much be assured that the file at issue contains child pornography.

In this case, a Minneapolis police officer used a program called RoundUp eMule to search for users on a peer-to-peer network who were sharing child pornography. The officer downloaded part of a file—a video that played for twenty to thirty seconds—from an IP address in or around St. Paul, Minnesota. Using the file's hash value, the officer was able to obtain the complete file and determined that it contained child pornography. After subpoenaing the relevant internet service provider, the officer learned that Shipton was the person associated with the IP address. According to the search warrant application, investigators also learned that

[1]The Honorable Patrick J. Schiltz, United States District Judge for the District of Minnesota, adopting the report and recommendation of the Honorable Katherine Menendez, United States Magistrate Judge for the District of Minnesota.

Shipton was a registered sex offender who was convicted in June 2015 of possessing child pornography. Further, a search of the Child Protection System database, which, the magistrate judge explained, "compiles hash values of previously identified child pornography and documents hits that have occurred for certain IP addresses," revealed that Shipton had advertised 92 known or suspected child pornography files near the time the officer here was investigating Shipton. These 92 files were uncovered by programs similar to RoundUp eMule known as G2Scanner and Nordic Mule. With this information in hand, a Minnesota state court issued a search warrant for Shipton's home, where officers found additional digital files containing child pornography, two of which served as the bases of the charges filed against Shipton.

Shipton maintains that the officer who used the RoundUp eMule program to facilitate the sharing of child pornography performed a "search" under the Fourth Amendment and therefore should've first obtained a warrant. A search can include a government official's physical intrusion or trespass, *see United States v. DE L'Isle*, 825 F.3d 426, 431 (8th Cir. 2016), but that's not what Shipton contends happened here. He maintains instead that the officer violated his reasonable expectation of privacy in the anonymous communications he made on the network. To demonstrate that the officer had conducted a search, Shipton must show that he had an actual, subjective expectation of privacy in those communications and that the expectation is "one that society is prepared to recognize as reasonable." *See id.*

Setting aside the question of whether Shipton had a subjective expectation of privacy, we have held numerous times that 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. *See, e.g.*, *United States v. Stults*, 575 F.3d 834, 843 (8th Cir. 2009). These decisions bind us unless an intervening decision of the Supreme Court casts them into doubt. *See United States v. Anderson*, 771 F.3d 1064, 1066–67 (8th Cir. 2014). Shipton purports to identify three such Supreme Court decisions from the last decade. *See Carpenter v. United States*, 138

S. Ct. 2206 (2018); *Riley v. California*, 573 U.S. 373 (2014); *United States v. Jones*, 565 U.S. 400 (2012).

The difficulty for Shipton is that we held, after *Carpenter*, *Riley*, and *Jones*, were decided that "[a] defendant has no legitimate expectation of privacy in files made available to the public through peer-to-peer file-sharing networks." *See United States v. Hoeffener*, 950 F.3d 1037, 1044 (8th Cir. 2020). Though our opinion in *Hoeffener* did not explicitly confront this trio of cases, the panel was certainly mindful of them as the defendant there raised contentions similar to Shipton's. *See* Br. of Appellant Hoeffener at 48–51, 53–54, No. 19-1192, 2019 WL 2488953. We now hold explicitly what was implicit in *Hoeffener*: That nothing in *Carpenter*, *Riley*, or *Jones* calls into question our oft-repeated observation that a defendant has no reasonable expectation of privacy in materials he shares on a public peer-to-peer network. Our sister circuits have rejected similar attempts by online traders in child pornography to use *Carpenter*, *Riley*, and *Jones* to demonstrate a reasonable expectation of privacy in things such as a user's IP address and other subscriber information. *See, e.g.*, *United States v. Trader*, 981 F.3d 961, 967–68 (11th Cir. 2020) (collecting cases from the First, Fourth, Fifth, and Ninth Circuits).

Shipton decries what he calls the government's "dragnet surveillance" through programs like RoundUp eMule and the CRC's maintenance of vast databases of hash values connecting known or suspected child pornography to IP addresses where those files were offered for sharing, invoking images of an Orwellian dystopia. His concerns are overstated. These programs and databases contain only information that users of peer-to-peer networks have deliberately chosen not to keep private. And as the magistrate judge here explained in an admirably thorough opinion, though this "surveillance" may certainly cast a wide net, most of the information gathered pertains to people other than Shipton. Unlike *Jones,* where officers tracked a person's car for nearly a month with the help of a GPS device, the information gathered here was relatively minimal. In *Carpenter*, the Court was similarly concerned about the

detailed information that a week's worth of cell-site location information generated from a mobile phone revealed about a particular person's everyday movements. Likewise, the concern in *Riley* was about the depth of detail that a person's mobile phone could reveal about him. In sum, we reject Shipton's contention that he had a reasonable expectation of privacy here.

Shipton also maintains that the district court should have ordered independent testing of RoundUp eMule and G2 Scanner to ensure that they were reliable programs and did not access private spaces on Shipton's computer. We rejected a similar request in *Hoeffener* based on a record much more favorable to the defendant than the current one, noting that Hoeffener offered only speculation about the relevant program's operation and simply wanted to go on "a fishing expedition." 950 F.3d at 1043–44. The same is true here. Shipton, moreover, has expressly disclaimed any reliance on his own expert's unsupported suggestion that the programs were faulty. The evidence in the record, which the magistrate judge expressly found credible, is that the programs operated reliably and did not access private areas of Shipton's computer. Shipton has offered no reason to conclude otherwise.

Affirmed.
