# UNITED STATES COURT OF APPEALS
# FOR THE SECOND CIRCUIT

# SUMMARY ORDER

**RULINGS BY SUMMARY ORDER DO NOT HAVE PRECEDENTIAL EFFECT. CITATION TO A SUMMARY ORDER FILED ON OR AFTER JANUARY 1, 2007 IS PERMITTED AND IS GOVERNED BY FEDERAL RULE OF APPELLATE PROCEDURE 32.1 AND THIS COURT'S LOCAL RULE 32.1.1. WHEN CITING A SUMMARY ORDER IN A DOCUMENT FILED WITH THIS COURT, A PARTY MUST CITE EITHER THE FEDERAL APPENDIX OR AN ELECTRONIC DATABASE (WITH THE NOTATION "SUMMARY ORDER"). A PARTY CITING TO A SUMMARY ORDER MUST SERVE A COPY OF IT ON ANY PARTY NOT REPRESENTED BY COUNSEL.**

**At a stated term of the United States Court of Appeals for the Second Circuit, held at the Thurgood Marshall United States Courthouse, 40 Foley Square, in the City of New York, on the 26th day of December, two thousand twenty-four.**

PRESENT:

SUSAN L. CARNEY,
JOSEPH F. BIANCO,
WILLIAM J. NARDINI,
*Circuit Judges*.

---

UNITED STATES OF AMERICA,

*Appellee*,

v. 23-7374-cr

CHAD SROGI,

*Defendant-Appellant*.

---

FOR APPELLEE: Michael D. Gadarian, Assistant United States Attorney, *for* Carla B. Freedman, United States Attorney for the Northern District of New York, Syracuse, New York.

FOR DEFENDANT-APPELLANT: Melissa A. Tuohey, Assistant Federal Public Defender, Office of the Federal Public Defender, Syracuse, New York.

Appeal from a judgment of the United States District Court for the Northern District of New York (Glenn T. Suddaby, *Judge*).

**UPON DUE CONSIDERATION, IT IS HEREBY ORDERED, ADJUDGED, AND DECREED** that the judgment of the district court, entered on October 11, 2023, is **AFFIRMED**.

Defendant-Appellant Chad Srogi appeals from the district court's judgment of conviction following his conditional guilty plea to: (1) five counts of distribution of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(2)(A) and 2252A(b)(1); (2) one count of transportation of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(1) and 2252A(b)(1); and (3) one count of possession of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(5)(B) and 2252A(b)(2). The district court sentenced Srogi principally to 300 months' imprisonment, to be followed by 25 years' supervised release. His conditional plea reserved the right to challenge the district court's denial of his motion to suppress evidence seized in connection with two search warrants issued based, in part, on files uploaded to Facebook, Dropbox, and Tumblr that were suspected of containing child pornography. These electronic service providers ("ESPs") attached the files to CyberTipline Reports ("CyperTip Reports") and submitted them to the National Center for Missing and Exploited Children ("NCMEC"). After reviewing the CyberTip Reports, NCMEC provided this information to law enforcement officials. On appeal, Srogi challenges the denial of his suppression motion, arguing, *inter alia*, that the search warrant affidavits included evidence seized in violation of the Fourth Amendment, and that, when that tainted evidence is excised from the affidavits, the warrants lacked probable cause. More specifically, Srogi asserts that the evidence in the affidavits—consisting, *inter alia*, of descriptions of certain files and chat logs

reported in the associated CyberTip Reports—was tainted because there was insufficient record evidence to support a finding that the ESPs had first reviewed the material. Consequently, Srogi argues the government investigators exceeded the scope of any private search performed by the ESPs when they reviewed that information without a warrant.

Srogi maintains that the government illegally searched image files found in each of four CyberTip Reports submitted by the ESPs. We need not address Srogi's specific arguments as to each of the CyberTip Reports, however, because we find that: (1) the private search doctrine permitted government investigators to search the image files identified in the June 2018 Facebook CyberTip Report without a warrant, *see United States v. Maher*, 120 F.4th 297 (2d Cir. 2024); and (2) the evidence identified in the June 2018 Facebook CyberTip Report—along with other evidence collected by law enforcement in its investigation and whose use Srogi does not challenge—was sufficient to support a finding of probable cause, even after excising all other CyberTip Report evidence from the warrant applications.[1]

In analyzing these issues, we assume the parties' familiarity with the underlying facts, procedural history, and issues on appeal, to which we refer only as necessary to explain our decision to affirm.

[1] Because we affirm the district court's decision on this ground, we need not address the alternative grounds provided by the district court for denying the suppression motion or the government's threshold argument that Srogi had no protectable Fourth Amendment interest in the child pornography files he received from or shared with third parties using these ESPs' platforms.

## BACKGROUND

Between February 2017 and June 2018, Facebook, Dropbox, and Tumblr each submitted CyberTip Reports to NCMEC stating that a user, later identified as Srogi, had uploaded files suspected of containing child pornography to their platforms.[2] After its own review, NCMEC provided these reports to the New York State Police. As relevant here, one of those reports, a June 2018 report submitted by Facebook, provided NCMEC with three files containing suspected child pornography that Srogi shared with another user. This CyberTip Report indicated that a Facebook employee or contractor "view[ed] [the] entire contents of [the] uploaded file[s]" before sending them to NCMEC. App'x at 118–19; *see id.* at 191. The CyberTip Report also disclosed certain identifying information, including the user's name and date of birth, as well as the username associated with the account and the IP address from which the files were uploaded.

On October 1, 2019, New York State Police applied for, and were issued, a warrant by an Oneida County Court Judge to search Srogi's residence for evidence of child pornography, based, in part, on the information they reviewed in the CyberTip Reports, including Facebook's June 2018 report. The affidavit submitted in support of the warrant application explained that a New York State Police investigator had reviewed, *inter alia*, the June 2018 Facebook CyberTip Report and determined that at least two of the files described therein contained child pornography. The affidavit further stated that the investigator linked the IP address provided in the report to an address in Durhamville, New York. Although they determined that Srogi did not reside there, investigators learned that the address was in "close proximity to other homes and offices," and that

[2] Facebook submitted two CyberTip Reports to NCMEC—one in February 2018 and another in June 2018.

the internet connection at the location was not password-protected, meaning members of the public could access it "from the public street." App'x at 93. An investigator also learned that, based on a search of sex offender registry records, Srogi had lived within approximately 100 yards of the location associated with this IP address. The registry also disclosed to the investigator that Srogi's first and middle names and date of birth were consistent with information in the Facebook CyberTip Report, and that Srogi was a sex offender who was previously arrested in Florida in 2006 for promoting a sexual performance by a child.

On October 2, 2019, New York State Police executed the warrant to search Srogi's residence, where they seized his cell phone, which contained a memory card storing 128 video files of children engaged in sexually explicit conduct. Srogi admitted in an interview with law enforcement, following the execution of the search warrant at his residence, that he used Facebook, Dropbox, and Tumblr to view and share images and/or videos of child pornography.[3] On July 16, 2020, Special Agent Brad Brechler, from the United States Department of Homeland Security, also obtained a warrant from the United States District Court for the Northern District of New York to search Srogi's Facebook, Dropbox, and Tumblr accounts. The federal warrant application contained information that mirrored the overview of the New York State Police investigation set forth in the Oneida County search warrant application and, like the state investigator, Special Agent Brechler reviewed all images referenced in the Facebook and Tumblr CyberTip Reports. The federal search warrant application also described the incriminating statements made by Srogi

[3] Srogi was subsequently charged and convicted in Oneida County Court for promoting a sexual performance by a child less than seventeen years of age and, on October 6, 2020, was sentenced to a term of imprisonment of two to six years.

at the time of the execution of the state court warrant at his residence in October 2019. The evidence obtained through these searches was used in federal court to charge Srogi, in May 2021, in a seven-count indictment. In his motion to suppress, Srogi argued that all the evidence seized from the searches of his internet accounts and residence, and additional evidence that flowed therefrom (including his statements to law enforcement), was obtained in violation of his Fourth Amendment rights. The district court denied the motion in its entirety. This appeal followed.

**DISCUSSION**

"On an appeal from a ruling on a motion to suppress, we review a district court's findings of historical fact for clear error, but analyze *de novo* the ultimate determination of such legal issues as probable cause . . . ." *United States v. Gagnon*, 373 F.3d 230, 235 (2d Cir. 2004) (internal quotation marks and citation omitted).

Srogi argues that the state and federal warrant applications contained tainted evidence—namely, information included in the Dropbox, Facebook, and Tumblr CyberTip Reports—that, when removed, left the applications without sufficient evidence to establish probable cause. We disagree. First, we find that the evidence in the June 2018 Facebook CyberTip Report was not tainted: the record evidence clearly establishes that a Facebook employee reviewed each of the image files before Facebook submitted the CyberTip Report to law enforcement. Thus, the private search exception to the warrant requirement applied and permitted the government's search. Second, as set forth below, even assuming *arguendo* that information in the other three CyberTip Reports was tainted, we conclude that Facebook's June 2018 CyberTip Report and the remaining evidence in the search warrant affidavits was sufficient to establish probable cause for those warrants.

To determine whether a warrant is properly supported by probable cause, a court must "make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before [it] . . . , there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238 (1983). We "generally accord[] substantial deference to the finding of an issuing judicial officer that probable cause exists . . . ." *United States v. Raymonda*, 780 F.3d 105, 113 (2d Cir. 2015) (internal quotation marks and citation omitted). However, when a warrant is issued based on an affidavit that contains tainted evidence, "[the] reviewing court should excise [that] evidence and determine whether the remaining, untainted evidence would provide a neutral magistrate with probable cause to issue a warrant." *United States v. Trzaska*, 111 F.3d 1019, 1026 (2d Cir. 1997) (internal quotation marks and citation omitted). Ultimately, we review a probable cause determination "simply to ensure that the [issuing judge] had a substantial basis for concluding . . . that probable cause existed." *United States v. Smith*, 9 F.3d 1007, 1012 (2d Cir. 1993) (alteration adopted) (internal quotation marks and citation omitted).

## I. The Evidence in the June 2018 Facebook CyberTip Report Was Untainted.

As a preliminary matter, we find that law enforcement did not violate Srogi's Fourth Amendment rights when it searched the image files associated with the June 2018 Facebook CyberTip Report without a warrant. We agree with the district court that the private search exception to the warrant requirement permitted the government to search those image files. Further, we are not persuaded by Srogi's claim that the district court abused its discretion by failing to hold an evidentiary hearing on this issue.

If the government "seeks to intrude upon an individual's legitimate expectations of privacy, it must either obtain a warrant from a neutral magistrate or bring its search within one of the few jealously and carefully drawn exceptions to the warrant requirement." *United States v. Buettner-Janusch*, 646 F.2d 759, 764 (2d Cir. 1981) (internal quotation marks and citation omitted). We do not resolve whether Srogi had a reasonable expectation of privacy in the images he shared over Facebook. *See* note 1, *supra*. But, assuming that he did, the government then bore "the burden of showing that [its] search [of those files] fell within one of the exceptions to the warrant requirement." *United States v. Kiyuyung,* 171 F.3d 78, 83 (2d Cir. 1999). One such exception is reflected in the private search doctrine, which "authorizes government officials to conduct a warrantless search . . . insofar as they effectively duplicate the search conducted by a private party, thereby frustrating no greater expectation of privacy and learning nothing more than what had been learned during the private search." *Maher*, 120 F.4th at 315.

In the context of CyberTip Reports submitted to NCMEC, this Court has held that when an ESP has visually inspected an image file before submitting it to NCMEC, the private search doctrine applies, and "no warrant [is] required for the government to [subsequently] review [the same file]." *United States v. Wilbert*, 818 F. App'x 113, 114 (2d Cir. 2020). When law enforcement "conduct[s] a warrantless visual search of a digital file . . . that no [ESP] employee or contractor ha[s] ever opened or visually examined," however, the private search doctrine does not apply and the search may be unlawful. *Maher*, 120 F.4th at 317.

Here, the record establishes that a Facebook employee visually inspected the image files submitted with the June 2018 CyberTip Report before any member of law enforcement examined those files. The government presented a declaration from Tyler Harmon, an employee of Meta

Platforms, Inc., which operates Facebook. Harmon explained that Meta has "various ways" to "identif[y] content that might violate its Community Standards" regarding child pornography, so that it can submit a CyberTip Report. App'x at 190. Once content has been flagged, a Meta employee or contractor will sometimes "view[] an image concurrently or immediately [before] making a report to NCMEC"; when an individual does so, the CyberTip Report will "show an answer 'Yes' to the question 'Did Reporting ESP view entire contents of the uploaded file?'" *Id.* In other instances, Meta "automatically detects content previously identified as child pornography." *Id.* at 191. If it does so, the CyberTip Report will be modified to include, "via automation," several "supplemental lines" containing the three text or image messages the user sent immediately before and after the child pornography.[4] *Id.* These "are not reviewed by a person before the report is submitted to NCMEC." *Id.*

The June 2018 CyberTip Report showed Facebook's response of "Yes" to the question "Did Reporting ESP view entire contents of uploaded file?" with respect to each of the three image files included with the report. *Id.* at 117–19. Harmon described these responses as meaning that "a Meta employee or contractor viewed the image in question before it was reported to NCMEC in the CyberTip[] [R]eport." *Id.* at 191. In addition, Facebook described the contents of two of the files in the CyberTip Report, explaining that one file contained an image of a prepubescent minor engaged in a "[s]ex [a]ct," and another contained an image of a prepubescent minor engaged

[4] For example, the February 2018 Facebook CyberTip Report includes messages Srogi and another Facebook user sent "immediately preceding and following" the upload of two image files. App'x at 104. Harmon explained that the "supplemental text or image information was not viewed by a Meta employee or contractor." App'x at 191.

in a "[l]ascivious [e]xhibition."[5] *Id.* at 120. The June 2018 Facebook CyberTip Report did not bear any automatically generated "supplemental lines," described above, which would have contained text or images messages—not reviewed by any Facebook employee— that Srogi sent immediately before or after he sent the child pornography. The record thus supports the conclusion that the files were viewed by the reporting individuals before law enforcement viewed them.

Srogi nevertheless maintains that the record evidence did not support application of the private search doctrine and that an evidentiary hearing was needed to resolve disputes of fact. He characterizes as disputed material facts the absence of evidence about "how the images described in the warrant applications were first obtained and observed," Appellant's Br. at 36, and about what Facebook "specifically did and observed with respect to each of Srogi's files before [it] reported the activity to NCMEC," *id.* at 38.

We are unpersuaded by these arguments. The record evidence was sufficient to answer the single key question here: whether the government "effectively duplicate[d]" the visual inspection already conducted by Facebook, or did more. *Maher*, 120 F.4th at 315. Srogi offers no reason to believe that the government's visual inspection was in some manner more invasive or revealed anything "that had not previously been learned" in Facebook's search. *Id.* at 311 (quoting *United States v. Jacobsen*, 466 U.S. 109, 120 (1984)). Contrary to what Srogi argues, the government need not produce a specific description of what the Facebook employee did and observed when reviewing each image. The government need only show by a preponderance of the evidence that a Facebook employee visually inspected each of the images before the government did so. Any

[5] Facebook's description of these two images is consistent with the government's more detailed description of the images, which it included in the warrant affidavits.

evidence of further steps Facebook took to obtain or examine the images cannot help Srogi's case: such evidence, if relevant at all, would only provide further proof that the government's search was no more invasive than Facebook's.

Nor did the district court err by declining to hold an evidentiary hearing as to the evidence in the June 2018 Facebook CyberTip Report. In the motion to suppress context, we review a district court's decision not to hold an evidentiary hearing for abuse of discretion. *United States v. Finley*, 245 F.3d 199, 203 (2d Cir. 2001). We ordinarily will require an evidentiary hearing only "if the moving papers are sufficiently definite, specific, detailed, and nonconjectural to enable the court to conclude that contested issues of fact going to the validity of the search are in question." *United States v. Pena*, 961 F.2d 333, 339 (2d Cir. 1992) (internal quotation marks and citation omitted). Here, Srogi does not identify a "contested issue[] of fact going to the validity of the search." *Id.* As explained, the only contested issues that Srogi has identified do not affect the validity of the search.

Thus, we agree with the district court's conclusion that the private search doctrine applied to law enforcement's search of the image files in the June 2018 Facebook CyberTip Report. We reject Srogi's claim that the descriptions of those image files were tainted and required exclusion from the warrant applications.

## II. The Untainted Evidence Supported a Finding of Probable Cause.

Having found that the evidence collected from the June 2018 Facebook CyberTip Report was untainted, we need not consider the Fourth Amendment arguments Srogi raises regarding the other CyberTip Reports. The evidence that law enforcement collected through its investigation, described below, in combination with the June 2018 Facebook CyberTip Report evidence,

supported a finding of probable cause. Here, the search warrant affidavits identified as child pornography at least two of the files contained in Facebook's June 2018 CyberTip Report. The affidavits then explained that, through a review of internet service provider and sex offender registry records, investigators linked the IP address identified in Facebook's June 2018 CyberTip Report to a location with a publicly accessible internet connection that was within approximately 100 yards of a residence associated with Srogi. It also stated that Srogi's first and middle names and date of birth matched information provided in that CyberTip Report, and that Srogi was a registered sex offender arising from his arrest in Florida, on May 16, 2006, for promoting a sexual performance by a child. Even excising from the warrant applications the information related to the other three CyberTip Reports, the remaining evidence is sufficient to support a finding of probable cause. *See, e.g.*, *United States v. Thomas*, 788 F.3d 345, 348–49 (2d Cir. 2018) (finding probable cause existed where law enforcement's warrant application provided a description of files suspected of containing child pornography, identified an IP address that had offered to share those files, and linked the IP address to a physical location).

Srogi's principal argument is that the evidence described above did not establish probable cause because the information in the affidavits from Facebook's June 2018 CyberTip Report was stale, having been provided to law enforcement over a year before the warrants were issued. We are unpersuaded.

A warrant may lack probable cause when "the evidence supporting it is not sufficiently close in time to the issuance of the warrant that probable cause can be said to exist *as of the time of the search*—that is, where the facts supporting criminal activity have grown stale by the time that the warrant issues." *Raymonda*, 780 F.3d at 114 (emphasis in original) (internal quotation

marks and citation omitted). There is "no bright-line rule for staleness," *Walczyk v. Rio*, 496 F.3d 139, 162 (2d Cir. 2007), and "the passage of time is not controlling and is but one factor to be considered, along with the kind of property sought and the nature of the criminal activity," *United States v. Singh*, 390 F.3d 168, 181 (2d Cir. 2004). In child pornography investigations, because "it is well known that images of child pornography are likely to be hoarded by persons interested in those materials in the privacy of their homes," *United States v. Irving*, 452 F.3d 110, 125 (2d Cir. 2006) (internal quotation marks and citation omitted), evidence is not stale if there is a showing, based on probable cause, that a suspect is a "collector" of that contraband, *Raymonda*, 780 F.3d at 114. Facts that could support such a finding include evidence identifying the suspect as a pedophile, or a history of possessing or receiving pornographic images. *Id.* at 114–15.

The affidavits contained facts sufficient to establish that Srogi was a "collector" of child pornography, and thus the June 2018 CyberTip Report information in the affidavits was not stale. In particular, as discussed above, the affidavits noted that Srogi was a registered sex offender, in connection with his 2006 arrest in Florida for promoting a sexual performance by a child. *See, e.g.*, *Irving*, 452 F.3d at 115, 125 (finding no staleness where suspect was a convicted pedophile). Further, the affidavits explained that, in June 2018, Srogi accessed, and shared with others, multiple files on Facebook identified as containing child pornography. *See Raymonda*, 780 F.3d at 115 (noting that a suspect could be a collector where he "accessed a single file of child pornography" and "subsequently redistributed that file to other users"). Taken together, this evidence—his arrest for a sex offense in 2006 and the fact that he shared files containing child pornography in 2018—was sufficient to establish that Srogi is a collector of child pornography, and thus the information in the affidavits was not stale. *See United States v. Boles*, 914 F.3d 95,

105 n.3 (2d Cir. 2019) (noting that factors weighing against staleness included the defendant's previous conviction for possession of child pornography and his membership in chat rooms used for posting and trading child pornography).

In sum, we conclude that, even excising from consideration some of the information in the search warrant affidavits that Srogi asserts was obtained in violation of his Fourth Amendment rights, the warrants were supported by probable cause, and the district court properly denied the motion to suppress.

* * *

We have considered Srogi's remaining arguments and find them to be without merit. Accordingly, we **AFFIRM** the judgment of the district court.

FOR THE COURT:
Catherine O'Hagan Wolfe, Clerk of Court