United States Court of Appeals

FOR THE DISTRICT OF COLUMBIA CIRCUIT

Argued October 24, 2025 Decided July 31, 2026

No. 24-3162

UNITED STATES OF AMERICA,
APPELLEE

v.

STEPHEN JOHNSON,
APPELLANT

Appeal from the United States District Court
for the District of Columbia
(No. 1:22-cr-00176-1)

Courtney R. Forrest argued the cause for appellant.

William C. Winn, Attorney, U.S. Department of Justice, argued the cause for appellee. With him on the brief were *Jeanine F. Pirro*, U.S. Attorney, and *Chrisellen R. Kolb*, Assistant U.S. Attorney.

Before: WILKINS and PAN, *Circuit Judges*, and RANDOLPH, *Senior Circuit Judge*.

Opinion for the Court filed by *Circuit Judge* PAN.

Concurring opinion filed by *Senior Circuit Judge* RANDOLPH.

PAN, *Circuit Judge*: Technology makes it easy to disseminate and store child pornography. In this case, for example, defendant Stephen Johnson used filesharing sites to access hundreds of videos depicting children engaged in sexual acts, uploaded the videos to his Google Drive account, and then saved them on his computer.

But technology also has facilitated detection. Google now uses automated software to identify child sexual abuse material ("CSAM") stored by its users.[1] In 2020, Google submitted 547,875 "CyberTips" concerning CSAM to the National Center for Missing & Exploited Children ("NCMEC"), a

[1] Our concurring colleague prefers to call this material "child pornography." Concurrence at 1. We decline to use that terminology because the terms "child sexual abuse material" and "CSAM" are preferred by victims' rights organizations, law enforcement authorities, and technology companies that screen for such materials. For example, the National Center for Missing & Exploited Children uses the term "child sexual abuse material" to "most accurately reflect what is depicted — the sexual abuse and exploitation of children." *Child Sexual Abuse Material*, Nat'l Ctr. for Missing & Exploited Children, https://perma.cc/L22N-KS85. The Department of Justice agrees. Off. of Just. Programs, U.S. Dep't of Just., *Child Sexual Abuse Material*, https://perma.cc/44AS-2DVA ("'child sexual abuse material' is preferred, as it better reflects the abuse that is depicted"). And Google, the industry actor in this case, also refers to it as "CSAM." *Google's Efforts to Combat Online Child Sexual Abuse Material*, Google Transparency Report Help Center, https://perma.cc/M2A5-YLSW ("Google is committed to fighting CSAM online.").

watchdog organization, which relays such tips to law-enforcement officers.

Here, when Johnson uploaded CSAM files to his Google Drive account, Google's automated system flagged some of the files as likely CSAM and sent them to NCMEC. NCMEC automatically passed those CyberTips to law enforcement, and the files ended up in the possession of Detective Thomas Sullivan of the D.C. Metropolitan Police Department. Detective Sullivan initiated an investigation that ultimately led to Johnson's prosecution and conviction on charges of possessing and transporting CSAM.

On appeal, Johnson argues that Sullivan violated the Fourth Amendment when he failed to secure a warrant before initially viewing some of the CSAM files that were forwarded to him through the CyberTips system. According to Johnson, the lack of a warrant at that stage of the investigation necessitates suppression of the CSAM files that Sullivan viewed and all other downstream evidence. Johnson also claims that the government exceeded the bounds of a search warrant that was executed at his residence and that the district court erred in calculating his Guidelines sentencing range.

We disagree on all counts. Even if we assume that a warrant was necessary for Sullivan to lawfully view the CSAM files when he first received them, the government gained lawful access to the files via an independent source — a magistrate judge who later authorized the government to open the files — and the government was entitled to rely on the magistrate judge's advice in good faith. Moreover, Johnson misreads the residential search warrant and misunderstands the Guidelines provision for possessing and soliciting CSAM. We therefore affirm the judgment of the district court.

I.

A.

Google operates a proprietary digital tool that identifies CSAM stored in Google Drive accounts. The tool is known as Child Sexual Abuse Imagery ("CSAI") Match technology. It monitors and analyzes user content, identifying any videos or images that potentially "match" known CSAM. When Google determines that a user's file contains offending content, it removes the file and sends a report to law-enforcement authorities.

Google keeps a database of known CSAM that it uses to detect other CSAM on its servers. The process starts with a trained Google employee or contractor viewing and classifying known content as containing CSAM. Google then translates the known CSAM content into a digital "hash value" (a digital fingerprint), which is a unique string of numbers and letters. The hash value — but not the underlying image or video itself — is entered into Google's database of CSAM content, where it can be checked against user-uploaded content to identify any recurrence of the same CSAM.

To identify CSAM in user accounts, Google routinely makes digital fingerprints of images and videos that are uploaded to its servers by its users. Google then searches for hash values that match the digital fingerprints in its CSAM database. When Google's CSAI Match software "detects a video containing CSAM, it is a match to any part of the [relevant] portion of a previously fingerprinted video" and can include "exact matches, matches intermingled with non-offending content, and slightly modified versions of the previously fingerprinted video." J.A. 119. In other words, CSAI Match will flag a video for potential CSAM if any portion of the video contains a match to known CSAM, and the

match may not be identical to the known CSAM. Sometimes a Google employee or contractor confirms that a digital fingerprint match contains CSAM before tipping off the authorities. At other times, CSAI Match automatically sends a report without any human review or confirmation.

Google undertakes its CSAM-identification process voluntarily — no law requires it to "affirmatively search, screen, or scan" for CSAM. 18 U.S.C. § 2258A(f). But once Google discovers CSAM, it may not keep that information to itself. It is subject to a mandatory reporting requirement in the Protect Our Children Act of 2008. *Id.* § 2258A(a)(1) (mandatory reporting required of any provider with "actual knowledge" of CSAM on its platform); *see also United States v. Maher*, 120 F.4th 297, 302 n.5 (2d Cir. 2024) (explaining § 2258A's reporting requirement).

The Protect Our Children Act requires Google to send a "CyberTip" about any suspected CSAM that it discovers to NCMEC, a nonprofit organization that operates a "CyberTipline." 34 U.S.C. § 11293; 18 U.S.C. § 2258A(a)(1). "A 'CyberTip' is an alert submitted by an electronic service provider under 18 U.S.C. § 2258A indicating that the service provider believes that there has been a violation of federal statutes involving the production or distribution of child pornography." *United States v. Sykes*, 65 F.4th 867, 873 n.1 (6th Cir. 2023). NCMEC makes each CyberTip report "available to the appropriate law enforcement agency for its review and potential investigation." 34 U.S.C. § 11293(b)(1)(K)(i)(II); *see also* 18 U.S.C. § 2258A(c). The CyberTip reports typically include the digital files that are suspected of containing CSAM.

B.

In 2020, defendant Stephen Johnson watched hundreds of videos containing CSAM on the internet and then saved the videos to his computer. Johnson used an encrypted filesharing site called Mega to gain access to CSAM, which was stored on files with labels such as "Children," "9y 10y 11y 12y black preteen" (meaning 9-, 10-, 11-, and 12-year-olds), and "11Yo Black Girl Showing Off Her [Genitalia]." J.A. 1829. The videos depicted nude children being forced to perform sexual acts. Johnson uploaded over two hundred of the videos, totaling nearly a gigabyte of data, to his personal Google Drive account. He then saved the files on his computer in folders with names like "blkkidd2." J.A. 1135.

In October 2020, CSAI Match flagged some of Johnson's Google Drive files as containing CSAM. The automated system sent nineteen CyberTip reports containing the suspect files to NCMEC, without additional human review. NCMEC's computer system conducted an automated preliminary investigation — also without any human input — and then forwarded the results (along with the CyberTip files) to a joint law-enforcement task force called the Northern Virginia Internet Crimes Against Children Task Force. The Task Force then referred the case to the D.C. Metropolitan Police Department ("MPD"), where it landed on the desk of Detective Thomas Sullivan, a member of the Child Exploitation and Human Trafficking Task Force administered by MPD and the FBI's Washington Field Office.

Detective Sullivan first reviewed the forwarded CyberTip reports in December 2020. The nineteen reports included Johnson's email address and account information, the names of about 220 files of suspected CSAM, and Google's notation that no Google employee had viewed Johnson's files. The video

files that had been flagged as CSAM accompanied the CyberTip reports. Sullivan opened three or four of the hundreds of video files and confirmed that they contained CSAM. He decided to seek a warrant to search Johnson's Google Drive account for more CSAM and drafted an affidavit establishing probable cause for that search.

When Sullivan submitted his affidavit to the U.S. Attorney's Office for approval, an Assistant U.S. Attorney ("AUSA") asked him about Google's procedures for reviewing, digitally fingerprinting, and reporting suspected CSAM. The AUSA noted certain ambiguities in the law surrounding CyberTips, hash-matching, and whether a search warrant is necessary to view reported files.

At the AUSA's direction, Sullivan set aside the warrant application for Johnson's Google Drive account and instead drafted a new affidavit. The new affidavit supported a request for a warrant to review the video files from Johnson's Google Drive account that were included in the CyberTip reports. The new affidavit acknowledged that Sullivan had already viewed some of the CyberTip video files, but it included none of the information he obtained from watching the videos.

Sullivan brought the warrant application to a magistrate judge for approval. The magistrate judge denied the application on the ground that no warrant was needed. He reasoned that (1) a Google employee or contractor reviews CSAM content before adding its digital fingerprint to the known-CSAM database, and Google's review is a private search; and (2) when a law-enforcement officer reviews user files that match the digital fingerprints in Google's database, that review does not exceed the scope of Google's private search, and therefore does not invade any reasonable expectation of privacy. The magistrate judge noted that the

warrant affidavit prepared by Sullivan established probable cause to view the CyberTip video files, but he nevertheless declined to sign the warrant because he believed it was unnecessary.

Relying on the magistrate judge's determination that the government would not "exceed the scope of the prior private search" by viewing the CyberTip video files, J.A. 258, Sullivan proceeded to open and review all of the files. He then used information from those files to obtain a warrant to search Johnson's Google Drive. Execution of that warrant yielded additional evidence of CSAM searches, downloads, and saved files on Johnson's Google Drive account. Sullivan then used evidence from the Drive account to obtain a warrant to search Johnson's home for CSAM "in whatever form." J.A. 297. The residential search warrant allowed officers to seize digital devices, as well as "[i]nformation, correspondence, records, and documents constituting evidence of the possession, receipt, distribution, or production of child pornography." J.A. 298. It also authorized obtaining Johnson's biometrics "for the purpose of attempting to unlock the Device(s)'s security features in order to search the contents as authorized by this warrant." J.A. 300.

Law-enforcement officers arrested Johnson and executed the residential search warrant in October 2021. Digital devices recovered during the residential search contained additional evidence of CSAM searches and downloads.

C.

Johnson was indicted on fifteen counts of transporting CSAM, *see* 18 U.S.C. § 2252(a)(1), as well as one count of possessing material depicting "a minor engaging in sexually explicit conduct," *id.* § 2252(a)(4)(B).

Before trial, Johnson filed a motion to suppress the CyberTip video files and their fruits, arguing that Sullivan's warrantless initial review of the files violated the Fourth Amendment. Johnson also moved to suppress the contents of the digital devices seized from his residence on the ground that the residential search warrant authorized only the seizure — not the search — of those devices.

The district court denied both motions. The district court agreed that Sullivan's initial warrantless viewing of the CyberTip videos may have violated Johnson's Fourth Amendment rights, but it determined that suppression was unwarranted under the good-faith exception. And the court held that the plain text of the residential search warrant authorized both the seizure and search of electronic devices.

After an eight-day trial, a jury convicted Johnson on one count of possession of material depicting a minor engaging in sexually explicit conduct and five counts of transportation of CSAM. Before sentencing, the district court denied Johnson's request that it reduce his Guidelines offense level by two points because his conduct was "limited to the receipt or solicitation" of CSAM. U.S.S.G. § 2G2.2(b)(1)(B). The district court reasoned that Johnson was not entitled to that reduction because his conduct included transportation and therefore was not "limited to the receipt or solicitation" of CSAM. The district court sentenced Johnson to ninety months' imprisonment, followed by ten years of supervised release.

Johnson timely appealed. We have jurisdiction under 28 U.S.C. § 1291. In reviewing the district court's rulings on Johnson's motions to suppress, we review its factual findings for clear error and its legal conclusions *de novo*. *United States v. Glover*, 144 F.4th 336, 339 (D.C. Cir. 2025). We review the district court's interpretation of the U.S. Sentencing Guidelines

de novo. *United States v. Webster*, 102 F.4th 471, 478 (D.C. Cir. 2024).

II.

A.

Johnson's primary argument on appeal is that Detective Sullivan violated the Fourth Amendment when he failed to secure a warrant before he first viewed some of the CSAM files from Johnson's Google Drive that were included in the CyberTip reports. Whether a warrant was necessary at that point turns on whether the files that Sullivan viewed fell within the scope of Google's "private search" of known CSAM with matching hash values. The answer to that question is unclear, and we need not resolve it. Instead, we exercise our discretion to decide that suppression of evidence is unwarranted here, even assuming that a Fourth Amendment violation occurred. *See United States v. Leon*, 468 U.S. 897, 925 (1984) (permitting courts to "exercise an informed discretion in making this choice"). Because the government later obtained authorization to view the CSAM files in question from an independent source — a magistrate judge — and Sullivan thereafter acted in good-faith reliance on the magistrate judge's legal determination, suppression is not an appropriate remedy for the alleged violation. *See Murray v. United States*, 487 U.S. 533, 542–43 (1988) (applying the independent-source doctrine to prevent suppression); *Leon*, 468 U.S. at 926 ("[S]uppression is appropriate only if the officers were dishonest or reckless . . . ."). We therefore affirm the district court's denial of Johnson's motion to suppress the CyberTip video files and their fruits.

1.

The Fourth Amendment generally requires law-enforcement officers to seek a warrant before conducting a search. *See Franks v. Delaware*, 438 U.S. 154, 164 (1978) ("The bulwark of Fourth Amendment protection, of course, is the Warrant Clause, requiring that, absent certain exceptions, police obtain a warrant from a neutral and disinterested magistrate before embarking upon a search."); U.S. Const. amend. IV. And a "search" occurs when officers intrude upon a defendant's "reasonable expectation of privacy." *Terry v. Ohio*, 392 U.S. 1, 9 (1968) (cleaned up); *accord Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); *New York v. Class*, 475 U.S. 106, 112 (1986).

A violation of the warrant requirement generally calls for the suppression of the evidence obtained during the illegal search and any other "fruits" that can be traced to the violation — *i.e.*, evidence "that is otherwise acquired as an indirect result of the unlawful search, up to the point at which the connection with the unlawful search becomes so attenuated as to dissipate the taint." *Murray*, 487 U.S. at 536–37 (cleaned up); *see also Leon*, 468 U.S. at 905–06.

Here, Johnson argues that the CyberTip video files and their fruits must be suppressed because Sullivan failed to secure a warrant before he first viewed some of those files. The government responds that no warrant was required because the government did not impinge on any reasonable expectation of privacy. According to the government, the videos viewed by Sullivan did not exceed the scope of Google's "private search" of known CSAM.

The private-search doctrine recognizes that the Fourth Amendment constrains government actors and generally does not reach the conduct of private parties. *See United States v.*

Jacobsen, 466 U.S. 109, 113 (1984). Thus, a private party's unauthorized search does not violate the Fourth Amendment. And once a private party has conducted a search, "the Fourth Amendment does not prohibit governmental use of the now nonprivate information." *Id.* at 117.

The Supreme Court explained this principle in *Jacobsen*. There, law-enforcement officers reexamined a package that private individuals — FedEx employees — had already opened. *Jacobsen*, 466 U.S. at 111, 119. The government's actions did not violate the Fourth Amendment because the FedEx employees had already seen the contents and "there was a virtual certainty that nothing else of significance was in the package." *Id.* at 118–19. After the private search by FedEx, the owners of the package no longer had a reasonable expectation of privacy in that package, and the Fourth Amendment therefore did not bar the government from seeing its contents without a warrant. *Id.* at 119. After all, the *Jacobsen* Court held, "it hardly infringed respondents' privacy for the agents to reexamine the contents of the open package." *Id.* "The agent's viewing of what a private party had freely made available for his inspection did not violate the Fourth Amendment." *Id.* Because the agents' examination of the package permitted them "to learn nothing that had not previously been learned during the private search," it "infringed no legitimate expectation of privacy and hence was not a 'search.'" *Id.* at 120.

Relying on *Jacobsen*, the government argues that Sullivan did not need a warrant to view the CSAM files that Google forwarded to law-enforcement authorities. It theorizes that Johnson had no reasonable expectation of privacy in CSAM that "matched" videos that Google had already viewed in a private search. We have some doubts about whether *Jacobsen* is analogous and ultimately decline to resolve the issue.

Recall that no Google employee or contractor viewed the CSAM files on Johnson's Google Drive. Rather, CSAI Match identified the CSAM in Johnson's files without any human involvement, by matching hash values in Johnson's files with the hash values of known CSAM in Google's database. It is true that Google employees and contractors have reviewed and identified all the known CSAM files in Google's database. But in this case, no one at Google took the extra step of reviewing Johnson's Google Drive files to confirm that they contained CSAM after a hash-value match was detected. Thus, application of the private-search doctrine here depends entirely on the match between Johnson's files and the known CSAM that Google has viewed and placed in its database.

Five of our sister circuits have considered whether the private-search doctrine applies under similar circumstances. The Fifth and Sixth Circuits have held that no warrant is necessary where the user files at issue exactly match the files that a private party previously reviewed. *United States v. Reddick*, 900 F.3d 636, 639–40 (5th Cir. 2018); *United States v. Miller*, 982 F.3d 412, 429–31 (6th Cir. 2020). By contrast, the Second, Fourth, and Ninth Circuits have held that even an exact match is not enough — the government always must obtain a warrant before examining user files, even if those files match known, privately viewed files. *Maher*, 120 F.4th at 314; *United States v. Lowers*, 170 F.4th 134, 154, 156–57 (4th Cir. 2026); *United States v. Wilson*, 13 F.4th 961, 971–72, 978–79 (9th Cir. 2021).

All of those previously decided cases differ from this one in an important respect: Each of them addressed exact matches between privately viewed files and the user files that the government sought to access without a warrant. Here, by contrast, Google's CSAI Match technology identifies matches "to any part of the [relevant] portion of a previously

fingerprinted video," including "exact matches, matches intermingled with non-offending content, and slightly modified versions of the previously fingerprinted video." J.A. 191. Thus, it is unclear whether any of Johnson's files were identical matches to known CSAM in Google's database. Instead, Johnson's files might have been flagged because they contained "intermingled" or "slightly modified" versions of previously viewed CSAM.

We are aware of no court that has held that an *inexact* file match satisfies the private-search doctrine, and we decline to break new legal ground here. Instead, we assume without deciding that a warrant was necessary and thus a Fourth Amendment violation occurred, and we proceed to determine whether suppression of evidence is the proper remedy. *See Leon*, 468 U.S. at 924–25 ("[C]ourts have considerable discretion in conforming their decisionmaking processes to the exigencies of particular cases . . . ."); *see also Herring v. United States*, 555 U.S. 135, 139 (2009) (same); *Hudson v. Michigan*, 547 U.S. 586, 592 (2006) ("Whether the exclusionary sanction is appropriately imposed in a particular case . . . is an issue separate from the question whether the Fourth Amendment rights of the party seeking to invoke the rule were violated by police conduct." (cleaned up)).[2]

2.

When the government violates the Fourth Amendment, exclusion of evidence is the default rule, but there are a number of exceptions to that rule. *Davis v. United States*, 564 U.S. 229,

[2] Johnson also presses a trespass theory. We need not decide whether Sullivan's viewing of the files separately violated Johnson's property rights because we assume a Fourth Amendment violation occurred.

244 (2011). We consider two of those exceptions in evaluating whether suppression is an appropriate remedy here: the independent-source doctrine, and the good-faith exception to the warrant requirement.

The Supreme Court's independent-source doctrine sets forth the following principle: When unlawfully obtained evidence is rediscovered in a second search that is both lawful and "genuinely independent" of the initial violation, suppression is unwarranted. *Murray*, 487 U.S. at 542.

In *Murray*, police officers illegally entered a warehouse and discovered bales of marijuana. 487 U.S. at 535. The officers then left and obtained a warrant to search the warehouse. *Id.* Their warrant application "did not mention the prior entry, and did not rely on any observations made during that entry." *Id.* at 535–36. With the warrant in hand, the officers reentered the warehouse and seized the marijuana. *Id.* at 536. The Supreme Court held that, because the warrant provided an independent source of lawful authority for the search and seizure, the marijuana did not need to be suppressed: "So long as a later, lawful seizure is genuinely independent of an earlier, tainted one (which may well be difficult to establish where the seized goods are kept in the police's possession) there is no reason why the independent source doctrine should not apply." *Id.* at 542.

Under the "independent source" doctrine, the second search is "genuinely independent" only if (1) the officers' "decision to seek the warrant was [not] prompted by what they had seen during the initial" unlawful search, and (2) no information obtained during that first search "was presented to the Magistrate and affected his decision to issue the warrant." *Murray*, 487 U.S. at 542; *see also United States v. Halliman*, 923 F.2d 873, 880 (D.C. Cir. 1991) (applying the independent-

source doctrine where "overwhelming independent grounds for probable cause" existed (citation omitted)); *United States v. Glover*, 681 F.3d 411, 418 (D.C. Cir. 2012) (similar).

The second exception to the exclusionary rule that is relevant here is the good-faith exception. In *United States v. Leon*, the Supreme Court held that suppression of evidence is not required when a police officer relies in good faith on a facially valid warrant that was issued in error by a judicial officer. 468 U.S. at 920–21, 923. The Court explained that the exclusionary rule is a "judicially created remedy designed to safeguard Fourth Amendment rights generally through its deterrent effect" on law-enforcement officers. *Id.* at 906 (citation omitted); *see also Davis*, 564 U.S. at 246 ("[T]he *sole* purpose of the exclusionary rule is to deter misconduct by law enforcement." (emphasis in original)). Thus, where police officers sought a warrant, were not "dishonest or reckless in preparing their affidavit," and reasonably believed that there was probable cause, suppression is not warranted because it would not "deter police misconduct" and instead would have the unintended effect of "punish[ing] the errors of judges and magistrates." *Leon*, 468 U.S. at 916, 926.

In subsequent cases, the Court has emphasized that suppression "has always been our last resort, not our first impulse." *Hudson*, 547 U.S. at 591. The exclusionary rule thus applies "only where its deterrence benefits outweigh its substantial social costs." *Utah v. Strieff*, 579 U.S. 232, 237 (2016) (cleaned up). "The principal cost of applying the rule is, of course, letting guilty and possibly dangerous defendants go free — something that 'offends basic concepts of the criminal justice system.'" *Herring*, 555 U.S. at 141 (quoting *Leon*, 468 U.S. at 908); *see also Hudson*, 547 U.S. at 591.

Accordingly, "[t]he extent to which the exclusionary rule is justified by these deterrence principles varies with the culpability of the law enforcement conduct." *Herring*, 555 U.S. at 143. "To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Id.* at 144. At bottom, "the exclusionary rule serves to deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence." *Id.* Where the violation instead reflects only "simple, isolated negligence," "exclusion cannot pay its way." *Davis*, 564 U.S. at 238 (cleaned up).

Here, the Fourth Amendment violation identified by Johnson occurred when Sullivan first opened the CyberTip video files, soon after they were initially forwarded to him. At that time, Sullivan believed that a search warrant was not necessary, and he therefore did not seek one. As a remedy for that warrantless search, Johnson argues that we must suppress not only the files that Sullivan initially viewed, but also the many fruits of that search. The CyberTip video files formed the basis for obtaining a warrant to search Johnson's Google Drive, which then led to a warrant to search Johnson's residence. According to Johnson, all the CSAM evidence in this case was tainted by the initial Fourth Amendment violation. In our view, however, both the independent-source doctrine and good-faith exception preclude suppression.

We assume that Sullivan violated the Fourth Amendment when he first reviewed CyberTip video files without a warrant. But what happened next is critical: Sullivan consulted with an AUSA who advised him to obtain a warrant to open and view those files, and Sullivan attempted to do just that. He went to a magistrate judge with a warrant affidavit that established probable cause to search the CyberTip files, without relying on

the contents of the files that he had already seen. But the magistrate judge advised Sullivan that no warrant was necessary because, the judge reasoned, the video files from Johnson's Google Drive fell within the scope of Google's private search of other, matching CSAM videos. Sullivan relied on the magistrate judge's determination that he could access the CyberTip files without a warrant when he subsequently viewed all the files and made investigative use of them.

Similar to the officers in *Murray*, 487 U.S. at 543, Sullivan sought a warrant after an initial search that was unlawful, without relying on any information gleaned from the initial search. Also like in *Murray*, Sullivan received authorization from a judicial officer to independently and lawfully repeat the search. Thus, when Sullivan reviewed the CyberTip video files for the second time, in reliance on the magistrate judge's advice that it was permissible to do so, the search was lawful under *Murray*, and all the investigative steps that flowed from there were also lawful. The magistrate judge's legal determination broke the causal chain between the initial (assumedly) unlawful viewing and everything that came afterward. *See id.* at 537 (holding that suppression was unwarranted where the post-warrant search was "so attenuated as to dissipate the taint" of the original violation (cleaned up)); *see also Nardone v. United States*, 308 U.S. 338, 341 (1939) (similar).[3]

[3] Although the government does not rely on the independent-source doctrine in its briefing on appeal, it made this argument to the district court. And we may "affirm the judgment of the district court if any reasonable view of the record supports its denial of the motion to suppress." *United States v. Hutchings*, 99 F.4th 604, 607 (D.C. Cir. 2024) (cleaned up).

It is of no moment that the officers in *Murray* obtained a warrant after their initial illegal search, while Sullivan instead received advice from a magistrate judge that no warrant was needed. Sullivan acted in good-faith reliance on the magistrate judge's legal determination, and suppression of the evidence therefore would not advance the exclusionary rule's purpose of deterring "deliberate, reckless, or grossly negligent" police misconduct. *Herring*, 555 U.S. at 144. Just like in *Leon*, the mistake of a judicial officer in evaluating a warrant application should not lead us to punish the law-enforcement officer who acted properly by requesting the warrant. *See* 468 U.S. at 916. Indeed, if the police may reasonably rely on a judicial officer's erroneous *issuance* of a warrant, *see id.* at 913, it naturally follows that law-enforcement officers may rely on a judge's erroneous *failure* to issue a warrant despite the existence of probable cause, based on a legal judgment that no warrant is necessary.

We also note that Sullivan's decision to seek a warrant was not "prompted" by his initial review of the CyberTip video files — that is, the warrant "would have been sought even if what actually happened had not occurred." *Murray*, 487 U.S. at 542 & n.3. Sullivan did not "decide[] to obtain the . . . warrant *on the basis* of what [he] had seen" during his initial search of several CyberTip video files. *Halliman*, 923 F.2d at 880 (emphasis added). Instead, it is undisputed that he sought a warrant to view the CyberTip files after consulting with an AUSA, and the AUSA's advice would have been the same whether Sullivan had already viewed the files or not. *See Murray*, 487 U.S. at 542; *see also United States v. Johnson*, 994 F.2d 980, 987 (2d Cir. 1993) (applying the independent-source doctrine where agents got a warrant on the advice of an AUSA, and the "only reason" they failed to do so initially "was their mistaken belief that they were entitled to" listen without a warrant to tapes seized from the defendant).

In sum, the magistrate judge's determination that the government could open and view the CyberTip video files without a warrant was an independent source of authority that dissipated any potential taint from Sullivan's initial search. Sullivan was entitled to rely on the magistrate judge's legal analysis in good faith, and he therefore was free to view the CyberTip files again and to use them in his investigation of Johnson. Under the independent-source doctrine and good-faith exception, suppression of the CSAM evidence in this case is not appropriate. Sullivan's actions were not deliberately unlawful, reckless, or grossly negligent, and imposing the harsh remedy of suppression therefore would serve no valid deterrent purpose.

B.

Johnson next argues that the government violated the Fourth Amendment by accessing the contents of the digital devices that it recovered during the residential search. He asserts that the residential search warrant permitted only the *seizure* of his digital devices, not a search of their contents. For that, he says, law enforcement should have obtained a separate warrant.

We disagree. The plain language of the residential search warrant defeats Johnson's claim. *See United States v. Dale*, 991 F.2d 819, 845 (D.C. Cir. 1993) (affirming that warrants "must be tested and interpreted . . . in a commonsense and realistic fashion[.]") (quoting *United States v. Ventresca*, 380 U.S. 102, 108 (1965)). The warrant authorized seizure of "[i]nformation, correspondence, records, and documents constituting evidence of the possession, receipt, distribution, or production of child pornography" from "any digital device." J.A. 298. Permitting the seizure of materials *from any digital device* is best read as allowing a search of the devices.

That reading is reinforced by another provision in the warrant, which authorized the government to secure biometric data from Johnson "for the purpose of attempting to unlock the Device(s)'s security features *in order to search the contents as authorized by this warrant*." J.A. 300 (emphasis added). *See also* Fed. R. Crim. P. 41(e)(2)(B) (permitting law enforcement to seize or copy data during the execution of a warrant and review it later). Thus, the warrant plainly stated that the devices could be searched.

Johnson notes only that the warrant listed "digital devices" under "property to be seized," not "property to be searched." J.A. 296–98 (cleaned up). To him, that means the government should have obtained a separate warrant to authorize a *search* of the digital devices. That argument ignores other parts of the warrant that explicitly allowed the government to search the devices, as discussed *supra*. And the cases Johnson cites are both factually inapposite and nonbinding on this court. *See United States v. Wilkins*, 538 F. Supp. 3d 49, 90–91 (D.D.C. 2021) (device seized without a warrant); *In re Search of Twenty-Six (26) Digit. Devices & Mobile Device Extractions that Are Currently in the Possession of L. Enf't in Wash. D.C.*, No. 21-sw-233, 2022 WL 998896, at *1 (D.D.C. Mar. 14, 2022) (devices seized pursuant to previous warrants from other investigations).

We thus have no trouble rejecting Johnson's unsupportable reading of the residential search warrant.

C.

Lastly, Johnson argues that the district court erred by declining to apply U.S. Sentencing Guideline § 2G2.2(b)(1) when calculating his sentencing range. That Guideline provides for a two-level reduction in a defendant's offense level if (1) "the defendant's conduct was limited to the receipt

or solicitation of material involving the sexual exploitation of a minor; *and*" (2) "the defendant did not intend to traffic in, or distribute, such material." U.S.S.G. § 2G2.2(b)(1) (emphasis added). Johnson argues that he met that Guideline's requirements.

Johnson's argument is contradicted by the jury's verdict. The jury convicted Johnson on five counts of *transporting* CSAM in violation of 18 U.S.C. § 2252(a)(1). Thus, his conduct was not "limited to the receipt or solicitation of" CSAM.

Indeed, a comment that accompanies the Guideline explains that "transportation" is a form of "distribution." U.S.S.G. § 2G2.2 cmt. n.1. The definition of "distribution" is "any act, including . . . transportation, related to the transfer of material involving the sexual exploitation of a minor." *Id.* Thus, Johnson's convictions for "transportation" of CSAM preclude application of a Guideline premised on a lack of intent to "distribute" CSAM. The district court correctly declined to apply § 2G2.2(b)(1).

* * *

For the reasons explained, we affirm the judgment of the district court.

So ordered.

RANDOLPH, *Senior Circuit Judge*, concurring:

This case presents the question whether Johnson had the requisite "expectation of privacy"—and thus Fourth Amendment protection—in the files containing child pornography that he stored on his Google account.

My colleagues do not resolve that question. They assume, without deciding, that Johnson's Fourth Amendment rights were violated but conclude that suppression is unwarranted given the independent source doctrine and the good faith exception.

I take no issue with my colleagues' analysis of either doctrine or with their conclusion that suppression is unwarranted. I would, however, resolve the constitutional question directly. Google expressly informed Johnson that it reserved the right to monitor the content in his account; that it would remove any child pornography it detected; and that it would report that material as federal law requires. Johnson therefore lacked a reasonable expectation of privacy in the files, and no Fourth Amendment violation occurred.

Before further explaining my position, I must object to the majority's terminology. The majority opinion refers nearly seventy times to "CSAM," an acronym for "child sexual abuse material." Neither the acronym nor the phrase it abbreviates appears in the governing statutes. Congress instead repeatedly referred to the material we confront here as "child pornography." *See, e.g.*, 18 U.S.C. §§ 2251(e), 2252A(a)(2)(A), (a)(3)(A), (a)(4)(B), (a)(5)(B), (a)(7), 2256(8); 2258A(a)(2)(A), (b)(4).

I recognize that other circuits have adopted "CSAM" as their preferred terminology. *But see United States v. Reddick*, 900 F.3d 636 (5th Cir. 2018); *United States v. Long*, 92 F.4th 481 (3d Cir. 2024). No matter why the acronym has taken

hold elsewhere, we should follow Congress's lead. "Child pornography" is the statutory term, and its meaning is direct and unmistakable. The shorthand CSAM tends to obscure the vile nature of this material. No one would think that serial killer should be "SK" – so "Ted Bundy was an SK." Or that the mass slaughter of Jews should be "MSJ" – as in "Hitler was responsible for MSJ." Or that gang rape should be "GR" – as in "The invading soldiers committed GR."

As to the Fourth Amendment, Google customers must anticipate that storing child pornography on their accounts exposes it to detection. Google regards eliminating child pornography from its services as "critically important to protecting [its] users, [its] product, [its] brand, and [its] business interests." Google Product Manager Decl. ¶ 4. Consistent with that policy, Google requires each user to accept its Terms of Service and its Privacy Policy. *Id.* ¶¶ 2-3.[1] Those documents inform its customers that Google may "take down" any "child pornography" it finds on a user's account and will "analyze [the user's] content to help [Google] detect abuse such as . . . illegal content." *Id.*

When Google discovers what appears to be child pornography on a customer's account, a federal criminal law—analogous to the ancient crime of misprision of a felony[2]—requires Google to report this ostensible criminal offense. *See* 18 U.S.C. § 2258A. Google must—and did in Johnson's case—send copies of its customer's material to the National Center for Missing and Exploited Children, a

---

[1] This was Google's voluntary choice. Federal law disclaims any duty on the part of such companies to monitor their customers' postings for child pornography. *See* 18 U.S.C. § 2258A(f).

[2] The modern version is 18 U.S.C. § 4.

clearing house, which then forwards a report to law enforcement in the suspect's venue.

My colleagues describe Google's detection system and explain its operation through hash-value matching. *See* Maj. Op. at 3-4. Their opinion notes that no human viewed Johnson's files before copies were transmitted to the National Center and then to law enforcement. Maj. Op. at 12. This is interesting but it is of no Fourth Amendment consequence. Law enforcement relies on sniffer dogs to detect illicit drugs in closed containers. Google relies on algorithms to detect child pornography. Dogs are not human and neither are algorithms. Humans train dogs to detect cocaine. And humans devise—train—algorithms to detect child pornography.[3]

The Supreme Court has described the expectation of privacy the Fourth Amendment protects as "one that society is prepared to recognize as 'reasonable.'" *Smith v. Maryland*, 442 U.S. 735, 743 (1979) (quoting *Katz v. United States*, 389 U.S. 347, 360 (1967) (Harlan, J., concurring)). If "society" is to determine what is "reasonable" then the people, through their elected representatives, must be consulted. *See Gregg v. Georgia*, 428 U.S. 153, 175 (1976).[4] With respect to child

---

[3] Narrowly targeted, nonhuman detection may implicate fewer Fourth Amendment concerns than direct human inspection. *See United States v. Place*, 462 U.S. 696, 707 (1983).

[4] Justice Alito: "In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way." *United States v. Jones*, 565 U.S. 400, 429-430 (2012) (concurring opinion); *see also Carpenter v. United States*, 585 U.S. 296, 386 (2018) (Alito, J., dissenting); *United States v. Davis*, 785 F.3d 498, 520 (11th Cir. 2015) (Pryor, J.,

pornography and the internet, Congress has spoken. In the interest of privacy, Congress has generally prohibited internet service providers from divulging their customers' communications and records. *See* 18 U.S.C. § 2702. But Congress has specifically excluded child pornography from that protection. *See* 18 U.S.C. § 2702(b)(6), (c)(5). And as mentioned above, Congress has required internet providers to report instances in which they acquire actual knowledge that a customer's account contains child pornography. *See* 18 U.S.C. § 2258A.

The chain of disclosure here—Google's discovery of child pornography in Johnson's account and its reporting of that discovery to law enforcement through the National Center—falls within the rule announced in *United States v. Miller*, 425 U.S. 435, 443 (1976): "[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *Hoffa v. United States*, 385 U.S. 293, 302 (1966), reflects the same principle, rejecting the view that "the Fourth Amendment protects a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it."

The Supreme Court distinguished *Miller* in *Chatrie v. United States*, No. 25-112, 609 U.S. __, 2026 WL 1855568, at *14-15 (June 29, 2026); and *Carpenter v. United States*,

---

concurring); *In re Askin*, 47 F.3d 100, 105-06 (4th Cir. 1995) (Wilkinson, J.); William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 HARV. L. REV. 1821, 1827-29, 1874-76 (2016).

585 U.S. 296, 308-10 (2018). Both cases dealt with the Fourth Amendment's application to cellphone-location data generated through ordinary use and disclosed by technology providers to law enforcement. The Court's distinctions of *Miller* do not apply here. A user's storing of child pornography on his Google account is by no means what the Court in *Chatrie* called "the automatic price of conventional cell usage," 609 U.S. at __. And it is not true that in using Google's services "a person can hardly help but generate 'a trail of [child pornography]," *id*. at __.[5] As for *Carpenter*, child pornography is not "a pervasive and insistent part of daily life." 585 U.S. at 315 (quoting *Riley v. California*, 573 U.S. 373, 385 (2014)). In short, unlike location data generated incidentally through routine cellphone use, child pornography does not appear in a Google account as a passive byproduct of ordinary digital activity—it results from a user's decision to place it there.[6]

For these reasons, when thumbnails of the files copied from Johnson's account appeared on Detective Sullivan's computer screen, the Fourth Amendment did not require him to avert his eyes, close the files, and prepare a

---

[5] The concurring opinion of Justice Gorsuch in *Chatrie* states that "the government enlisted Google to search" the defendant's location data. 609 U.S. at __. No such enlisting of a search occurred in this or similar cases. *See supra* note 1.

[6] Whatever broader implications *Carpenter* and *Chatrie* might have, those decisions do not permit us to disregard *Miller* when, as here, it directly applies. "If a precedent of this Court has direct application in a case, yet appears to rest on reasons rejected in some other line of decisions, the Court of Appeals should follow the case which directly controls, leaving to this Court the prerogative of overruling its own decisions." *Rodriguez de Quijas v. Shearson/American Express, Inc.*, 490 U.S. 477, 484 (1989).

search-warrant affidavit to obtain a magistrate's authorization to open them. The consequences of a contrary regime on enforcing the laws against possession and distribution of child pornography are ominous. In 2020, Google alone submitted 547,875 reports to the National Center encompassing more than 4.4 million images of child pornography. Google Product Manager Decl. ¶ 5. By 2025, those figures had risen to 1,457,204 reports and more than 8.8 million items. *Google's Efforts to Combat Online Child Sexual Abuse Material*, GOOGLE: TRANSPARENCY REP., https://transparencyreport.google.com/child-sexual-abuse-material/reporting**.** And Google is but one provider. Online service providers collectively submitted 21.1 million reports to the National Center during 2025. *2025 CyberTipline Reports by Electronic Service Providers (ESPs)*, NAT'L CTR. FOR MISSING & EXPLOITED CHILD., https://www.missingkids.org/content/dam/missingkids/pdfs/2025-reports-by-esp.pdf. Requiring officers to obtain search warrants before examining the files accompanying such reports would unnecessarily threaten to overwhelm both investigators and judges.