

PUBLISHED

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

No. 24-4546

UNITED STATES OF AMERICA,

Plaintiff - Appellee,

v.

NICO AARON LOWERS,

Defendant - Appellant.

Appeal from the United States District Court for the Eastern District of North Carolina, at Raleigh. Richard E. Myers, II, Chief District Judge. (5:22-cr-00178-M-BM-1)

Argued: December 12, 2025

Decided: March 10, 2026

Before KING, THACKER, and BENJAMIN, Circuit Judges.

Affirmed by published opinion. Judge Thacker wrote the opinion in which Judge Benjamin joined. Judge King wrote an opinion concurring in the judgment.

ARGUED: Raymond Curtis Tarlton, TARLTON LAW PLLC, Durham, North Carolina, for Appellant. Lucy Partain Brown, OFFICE OF THE UNITED STATES ATTORNEY, Raleigh, North Carolina, for Appellee. **ON BRIEF:** Daniel P. Bubar, Acting United States Attorney, David A. Bragdon, Assistant United States Attorney, OFFICE OF THE UNITED STATES ATTORNEY, Raleigh, North Carolina, for Appellee.

THACKER, Circuit Judge:

At its core, this case requires us to decide whether the privacy expectations guaranteed by the Fourth Amendment apply with equal force in the digital world.

The district court below held that Nico Lowers (“Appellant”) had no expectation of privacy in the files he uploaded to his private Google Drive account, files that contained child sexual abuse material (“CSAM”).¹ Therefore, the court denied Appellant’s motion to suppress the evidence of conviction that flowed from law enforcement’s warrantless search of those files.

We reject the district court’s proffered reasons for so holding. Just as Americans enjoy a reasonable expectation of privacy in files maintained in a filing cabinet in the physical world, so too, Americans enjoy a reasonable expectation of privacy in the digital files they place in cloud based storage accounts. Law enforcement cannot open and view those private files without first securing a warrant. Because law enforcement here failed

¹ “[T]he current practice among professional organizations that work on behalf of child victims of sexual exploitation is to use the term ‘child sexual abuse material’ and they strongly urge others to do so as well.” *Moretti v. Thorsdottir*, 157 F.4th 352, 365 (4th Cir. 2025) (Thacker, J., concurring) (citing *What Is Child Sexual Abuse Material*, RAINN (Rape, Abuse & Incest National Network) (Aug. 25, 2022), <https://rainn.org/news/what-child-sexual-abuse-material-csam> [<https://perma.cc/N7KW-KHQD>]). The Department of Justice itself has explained that although the term “child pornography” appears in some federal and state statutes, the term “‘child sexual abuse material’ is preferred, as it better reflects the abuse that is depicted in the images and videos and the resulting trauma to the child.” *Child Sexual Abuse Material*, U.S. Dep’t of Just. 1 (June 2023), https://www.justice.gov/d9/2023-06/child_sexual_abuse_material_2.pdf [<https://perma.cc/LM7F-EYNW>].

to secure a warrant before opening Appellant’s files, we hold that this was an unreasonable search in violation of the Fourth Amendment.

That constitutional violation notwithstanding, we nevertheless agree with the district court’s alternative holding that suppression is unwarranted because the causal connection between the illegal search and the later discovered evidence is too strained to trigger the exclusionary rule. The evidence Appellant seeks to suppress came to light months after the illegal search and only because of multiple intervening circumstances. Suppressing the evidence would do little to further the exclusionary rule’s sole purpose of deterring future police misconduct. For that reason, and that reason alone, we affirm.

I.

A.

This case began with a tip from Google to law enforcement based on a process known as “hash-matching.” “A hash value is . . . a short string of characters generated from a much larger string of data . . . using an algorithm.” *United States v. Ackerman*, 831 F.3d 1292, 1294 (10th Cir. 2016). The hashing algorithm “process[es] the contents of a given computer file and assign[s] a sequence of numbers and letters that correspond to the file’s contents.” *United States v. Reddick*, 900 F.3d 636, 637 (5th Cir. 2018). In other words, a hashing algorithm goes “pixel-by-pixel” through a file and assigns a unique identifying serial number to that file, which acts as a “catalogue [of] every pixel,” *United States v. Miller*, 982 F.3d 412, 430 (6th Cir. 2020), or “a sort of digital fingerprint,” *Ackerman*, 831 F.3d at 1294. When done properly, a hashing algorithm can be provided an image, assign it a hash value, and then compare that hash value against a database of

hash values derived from other images. *See United States v. Arce*, 49 F.4th 382, 389 (4th Cir. 2022). When two hash values match, a so called “hash-match,” then their corresponding images likely match, too. *See United States v. Wellman*, 663 F.3d 224, 226 n.2 (4th Cir. 2011).

Google is no stranger to hash-matching. Google, after all, has a strong business interest in keeping its services free of CSAM, as users will likely stop using Google’s services if they become known as a safe haven for such material. So, “Google independently and voluntarily takes steps to monitor and safeguard its platform.” J.A. 140.² This includes hash-matching.

As part of its hash-matching process, Google first trains certain employees and contractors, known as Google Reviewers, on the federal statutory definition of CSAM. Whenever any Google employee comes across a file that they believe contains CSAM, they forward the file to a Google Reviewer, who opens the file, visually inspects its contents, and determines whether or not the file contains “apparent” CSAM.³ If the Google Reviewer believes it does, the file is marked accordingly, given a label that indicates the

² Citations to the “J.A.” refer to the Joint Appendix filed by the parties in this appeal.

³ Although § 2258A requires companies, such as Google, to report “apparent” CSAM to NCMEC, the statute provides no definition for “apparent.” However, because § 2258A casts a wide net and requires companies to make NCMEC aware of even debatable CSAM, *see* 18 U.S.C. § 2258A (requiring covered entities to report “[a]pparent violation[s]” of federal child exploitation laws to NCMEC “[i]n order to reduce the proliferation of online child sexual exploitation and to prevent the online sexual exploitation of children”), we read “apparent” to mean both obvious depictions of CSAM, as well as depictions that may or may not actually depict CSAM but appear to do so. *See Apparent*, Black’s Law Dictionary (12th ed. 2024).

category of CSAM depicted, and assigned a hash value by Google’s proprietary hashing algorithm. Google then places that hash value (but not the file itself)⁴ in “Google’s repository of hashes of apparent CSAM” and reports the file to the National Center for Missing and Exploited Children (“NCMEC”), as required by federal law. J.A. 140; *see also* 18 U.S.C. § 2258A.

Google uses this repository of known hash values to then identify and report files that contain apparent CSAM as they are uploaded to Google’s servers. As Google’s legal investigations support team lead explained in an affidavit submitted to the district court, Google “[c]ompar[es] the hashes in that repository to hashes of content uploaded to Google’s services.” J.A. 140. According to the affidavit, doing so allows Google “to identify exact or very similar CSAM imagery and to prevent them from continuing to circulate on Google products.” *Id.*

As noted above, once Google’s hashing algorithm determines that the hash value of an uploaded file matches a hash in the apparent CSAM repository, Google reports the file to NCMEC as required by federal law. To report the file, Google proceeds in one of two ways. Sometimes -- but not always -- Google will have a Google Reviewer open the file and confirm that the hash-matched file contains apparent CSAM before reporting it to NCMEC. But because a hash-match purportedly indicates that someone at Google has previously seen the same (or very similar) image, Google will sometimes skip the human

⁴ There is no indication in this record that Google retains or otherwise stores the file itself.

review process and report it right away. Either way, Google prepares a written CyberTip report for NCMEC. Each CyberTip report discloses whether someone at Google opened the file and viewed its content, or whether Google sent NCMEC an unopened file.

Beyond that overview, though, the record in this case contains no other evidence on Google's hashing process. The record does not reveal how Google trains Google Reviewers on interpreting and applying the federal CSAM definition. Nor is there any record evidence indicating how accurate or reliable Google Reviewers are at actually identifying apparent CSAM. Similarly, there is no record evidence demonstrating how accurate Google's proprietary hashing algorithm is in practice. The record does not disclose, for example, whether Google's hashing algorithm ever "matches" two non-identical files and, if so, how often that mistake occurs.

The record does, however, indicate that Google warns users of its efforts to identify and report any CSAM uploaded to its platform. The pertinent privacy policy here warned users, "Google may 'analyze your content to help us detect abuse such as spam, malware, and illegal content.'" J.A. 139.

B.

On September 20, 2019, a Google user affiliated with the email address "harvardeperstein@gmail.com" uploaded 156 files to their Google Drive account. Google Drive is a cloud based storage platform offered by Google, where users can upload images, videos, documents, spreadsheets, etc., and share them with other Google users.

Within days, Google's hashing algorithm scanned those 156 files and determined that each file's hash value matched a known hash value in Google's apparent CSAM

repository. Of the 156 files, a Google Reviewer opened 31 and concluded that each opened file contained apparent CSAM. Google then prepared a CyberTip report which identified the approximately 20% of the files it had viewed and the 80% which remained unopened and unviewed. Google sent the CyberTip report and all 156 files to NCMEC on September 23. An employee at NCMEC received that CyberTip and opened and viewed the same 31 images as the Google Reviewer. The NCMEC employee did not open any of the remaining 125 unreviewed files. The NCMEC employee believed the IP address⁵ provided in the CyberTip report corresponded with Bedford County, Virginia. Therefore, the NCMEC employee forwarded the report to law enforcement there on October 29, 2019.

The Bedford County Sheriff's Office received the report not long after but let it sit for half a year. Finally, on April 16, 2020, an investigator in that office reviewed the report and sent an administrative subpoena to the internet service provider affiliated with the IP address found in the report. Once returned, that subpoena revealed that the IP address was linked to a home address located in Chesapeake, Virginia, not Bedford County. As a result, the Bedford County investigator closed out the file on May 13, 2020, and sent the report to the Chesapeake Police Department.

Once the report arrived in Chesapeake, it was downloaded by Detective Jennifer Rider. Without first obtaining a warrant, Detective Rider opened and viewed at least three

⁵ “[A]n Internet protocol or IP address” is “a unique numerical address” used “to identify [a computer] and facilitate the orderly flow of electronic traffic.” *Peterson v. Nat’l Telecomms. & Info. Admin.*, 478 F.3d 626, 629 (4th Cir. 2007). In other words, an IP address is a digital routing number, and every “computer connected to the Internet” has one. *Id.*

files that neither Google nor NCMEC had ever opened or viewed. Each of these three files contained CSAM. So, on May 27, 2020, Detective Rider sought a search warrant for the Google account that uploaded the files. Her warrant application described a single image in detail but just generally described the other two images containing CSAM. The warrant issued and the results were telling: the Google account was created, used to upload the 156 files, and then never used again. The account was active for less than 30 minutes.

Detective Rider proceeded to surveil the Chesapeake address for a four month period from June to September, apparently to no avail. Detective Rider finally decided to obtain a search warrant for the home that fall. Her warrant application again included descriptions of the three files she opened and viewed without a warrant.

That warrant issued, and the Chesapeake Police Department executed it on October 12, 2020. A married couple and their two children, ages 8 and 13, lived in the home. Police seized ten devices and searched each for CSAM but found none. As law enforcement executed the warrant, the couple agreed to a voluntary interview. During the husband's interview, he mentioned that their 21 year old son -- Appellant -- had recently moved out and gone to Raleigh, North Carolina. The husband also provided law enforcement with Appellant's new address along with his phone number.

The Chesapeake Police Department closed out their file and sent all available information to law enforcement in North Carolina. Not long after, Homeland Security Agent Glenn Covington contacted Appellant and asked if he would submit to a voluntary interview. Appellant obliged. Agent Covington and Detective L.E. Faust of the Raleigh Police Department ("RPD") met Appellant at his apartment on November 24, 2020, and

questioned Appellant about the Google Drive account. Appellant professed ignorance. He did, however, consent to a search of his cell phone and laptop.

Detective R.J. Pike of the RPD performed a forensic analysis of Appellant's devices a few days later. Detective Pike located four videos containing CSAM in the deleted files on Appellant's phone.

Once Detective Pike finished searching Appellant's devices, Appellant was contacted again and asked if he would consent to a second interview. Appellant agreed, and he was interviewed on December 8, 2020. However, unlike the first interview at his apartment, the second interview took place at the RPD station with half a dozen officers in the room. Appellant initially stuck to his story, but when confronted with the CSAM found on his phone days earlier, Appellant confessed to downloading CSAM onto a flash drive at his parents' home in Virginia and bringing the flash drive with him to North Carolina. Appellant also told the officers where they could find that flash drive in his apartment.

As it turned out, law enforcement were already searching Appellant's apartment pursuant to a search warrant Detective Faust obtained ahead of time. His supporting warrant affidavit detailed the entire investigation up to that point. The warrant was issued before the second interview began, and officers began executing it while Appellant was being interviewed at the police station. Two officers left Appellant's interview, however, to join the search and retrieve the flash drive. Officers also discovered a hard drive in Appellant's apartment. The flash drive contained 264 images and 17 videos, each depicting CSAM. The hard drive contained 764 images and 11 videos, each of which also depicted CSAM.

C.

Appellant was charged in the Eastern District of North Carolina in a two count indictment. Count One charged Appellant with transporting CSAM in violation of 18 U.S.C. § 2252(a)–(b), beginning on or about June 27, 2020, and ending on or about September 30, 2020. Count Two charged Appellant with possession of CSAM in violation of 18 U.S.C. § 2252(a)(4)(B) on or about December 8, 2020. Neither charge related to the files Appellant uploaded to his Google Drive account on September 20, 2019. The charges instead related to the CSAM discovered by North Carolina law enforcement at Appellant’s apartment.

Appellant later moved to suppress all evidence against him. He argued that Detective Rider’s opening and viewing of his files without a warrant invaded his reasonable expectation of privacy in those files. Appellant further argued that this was an unreasonable search in violation of the Fourth Amendment, and that all evidence derived from that illegal search should be suppressed. After the motion was fully briefed, the Government filed a notice in which it stated that a hearing was unnecessary. Appellant agreed, and the district court decided the motion based on the paper record before it.

The district court denied the motion to suppress. In doing so, the district court found three alternative reasons for holding that no search occurred. First, the district court held that Google’s privacy policy, which warned users that Google may analyze their content to identify “illegal content,” rendered Appellant’s expectation of privacy in his Google Drive objectively unreasonable. Second, the district court held that, even if Appellant had a reasonable expectation of privacy in his Google Drive, he could not have had a reasonable

expectation of privacy in the files he stored there. This was so, the district court explained, because CSAM is a form of contraband, and nobody has an expectation of privacy in contraband. Third, the district court found that Google's proprietary hashing algorithm was "exceedingly reliable," J.A. 255, and that each hash-match proved that Google had previously seen each of the 156 images in Appellant's files. The district court then reasoned that, because Google had previously seen the images in Appellant's files, Appellant's expectation of privacy in those files had been frustrated by a private search.

Alternatively, the district court assumed that there was an unconstitutional search and considered whether the exclusionary rule would apply. The district court determined there were two more reasons to deny suppression. First, the district court held that Detective Rider reasonably relied on the federal statute that required Google to report the CSAM files to law enforcement when she opened and viewed Appellant's files without a warrant. In the district court's view, federal law permitted such warrantless inspection of reported files and, therefore, Detective Rider's reliance on 18 U.S.C. § 2258A triggered the good faith exception to the exclusionary rule. Second, and in the alternative, the district court held that there were "significant intervening events" in the causal chain between the warrantless search and later discovery of evidence, which sufficiently attenuated the connection between the two and rendered suppression unwarranted. J.A. 259.

Ultimately, Appellant entered a conditional guilty plea that preserved his right to appeal the district court's denial of his motion to suppress. Appellant was then sentenced to 96 months of incarceration to be followed by 20 years of supervised release. This timely appeal followed.

II.

“In reviewing a denial of a motion to suppress, we review the district court’s legal conclusions de novo and factual findings for clear error.” *United States v. Ordonez-Zometa*, 141 F.4th 531, 548 (4th Cir. 2025). Clear error exists where, after considering “the entire evidence, we are left with the definite and firm conviction that a mistake has been committed.” *United States v. Henderson*, 159 F.4th 213, 220 (4th Cir. 2025) (quoting *United States v. Manigan*, 592 F.3d 621, 631 (4th Cir. 2010)); *see also Manigan*, 592 F.3d at 631 (explaining that clear error exists where “the findings under review . . . are not supported by substantial evidence” (citation omitted) (alteration in original)). And where, “as here, a suppression motion has been denied, this Court reviews the evidence in the light most favorable to the government.” *Ordonez-Zometa*, 141 F.4th at 548 (quoting *United States v. Bailey*, 74 F.4th 151, 156 (4th Cir. 2023)).

III.

A.

The Fourth Amendment Guarantees a Reasonable Expectation of Privacy

The Fourth Amendment guarantees “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches.” U.S. Const. amend. IV. “A government agent’s search is unreasonable when it infringes on ‘an expectation of privacy that society is prepared to consider reasonable.’” *United States v. Castellanos*, 716 F.3d 828, 832 (4th Cir. 2013) (quoting *United States v. Jacobsen*, 466 U.S. 109, 113 (1984)).

Colloquially known as the *Katz*⁶ test, this standard breaks down into a two step test. *California v. Ciraolo*, 476 U.S. 207, 211 (1986). First, the defendant must have had a subjective expectation of privacy in the place or thing searched. *Id.* Second, the defendant's expectation of privacy must have been objectively reasonable. *Id.* The defendant bears the burden of proving both prongs. *United States v. Rose*, 3 F.4th 722, 727 (4th Cir. 2021).

B.

Appellant's Reasonable Expectation of Privacy in his Google Drive

As a threshold matter, we must decide whether Appellant had a reasonable expectation of privacy in his Google Drive account.

The district court assumed without deciding that Appellant had a subjective expectation of privacy in his Google Drive and skipped straight to the second step of the *Katz* analysis. The Government does not challenge that decision, and we see no reason to address the issue in the first instance. We thus proceed to the second step of the *Katz* test and, in doing so, decide whether it was objectively reasonable for Appellant to have had an expectation of privacy in his Google Drive.

⁶ *Katz v. United States*, 389 U.S. 347 (1967).

1.

Google's Privacy Policy did not Defeat Appellant's Expectation of Privacy in his Google Drive

Here, Google's privacy policy warned users that Google "may 'analyze [their] content to help [Google] detect abuse such as spam, malware, and illegal content.'" J.A. 139, 142. The district court held that these boilerplate terms "limit[ed] [Appellant's] objectively reasonable expectation of privacy" to the point that he lost all right to challenge warrantless government intrusions into his Google Drive account. *Id.* at 249. We disagree.

To be sure, Google's warning that it may monitor user's content for illegal activity reduced Appellant's expectation of privacy to some degree. But, as the Supreme Court has acknowledged, the mere fact that someone has a "diminished privacy interest[]" does not mean that the Fourth Amendment falls out of the picture entirely." *Riley v. California*, 573 U.S. 373, 392 (2014). Relevant here, courts have long held that a service provider's ability to monitor how its customers use the provided services does not negate a customer's reasonable expectation of privacy against the government. *See, e.g., United States v. Warshak*, 631 F.3d 266, 286–87 (6th Cir. 2010) (explaining that "that the mere ability of a third-party intermediary to access the contents of a communication cannot be sufficient to extinguish a reasonable expectation of privacy" (emphasis omitted)).

For proof, we need look no further than *Katz* itself. There, federal agents placed a listening device atop a telephone booth and recorded Mr. Katz's private telephone conversation. *Katz*, 389 U.S. at 348–49. The Supreme Court held that Mr. Katz had a reasonable expectation of privacy in his phone call -- and that the Government's

warrantless eavesdropping invaded that expectation of privacy -- even though telephone companies retained the right to monitor calls for illegal conduct. *Id.* at 352; *see also Smith v. Maryland*, 442 U.S. 735, 746–47 (1979) (Stewart, J., dissenting) (observing that even though “telephone conversation[s]” “may be recorded or overheard by the use of [telephone] company equipment [the Court] squarely held [in *Katz*] that the user of even a public telephone is entitled ‘to assume that the words he utters into the mouthpiece will not be broadcast to the world.’” (quoting *Katz*, 389 U.S. at 352)). So even though Mr. Katz knew the operator could eavesdrop and hear every word said, he maintained a reasonable expectation that government agents would not.

The same is true here. Every Google Drive user knows that Google may scan their files to see if those files contain anything illegal. But a user’s knowledge that Google might occasionally sift through their files does not mean that he expects the Government to have equally unfettered access to those same files.

An offline example helps solidify the point: hotel rooms. Hotel guests have a reasonable, yet diminished, expectation of privacy in their hotel room,⁷ as they know housekeeping shares a key to their room, and they know that housekeeping will use that key from time to time to come in, tidy up, and do their job. Mindful of that, reasonable hotel guests keep any contraband they have out of sight because they know housekeeping

⁷ *United States v. Kitchens*, 114 F.3d 29, 31 (4th Cir. 1997) (“A guest in a hotel room has a reasonable expectation of privacy.”); *see also United States v. Stokes*, 733 F.3d 438, 443 n.7 (2d Cir. 2013) (“Hotel guests retain a legitimate expectation of privacy in the hotel room and in any articles located in their hotel room for the duration of their rental period.”).

may report them to hotel management, and maybe even to the police, if that contraband is discovered. But a hotel guest would never expect the police to barge in uninvited without a warrant, turn their room upside down, and search for that same contraband. That, of course, would violate the Fourth Amendment. *See United States v. Stevenson*, 396 F.3d 538, 546 (4th Cir. 2005) (explaining that the Fourth Amendment’s protections “extend[] to apartments, rented rooms within a house, and hotel rooms so that a landlord may not give the police consent to a warrantless search of a rented apartment or room”).

A Google Drive account is no different merely because it exists in the cyberworld. The privacy rights implicated are the same.

2.

The Government’s Cases Do Not Support a Different Conclusion

The Government sees things differently. In defending the district court’s holding, the Government contends that “[a] legitimate expectation of privacy can be reduced by notice,” Appellee Br. at 20, and further argues that Google’s privacy policy served to minimize Appellant’s expectation of privacy. The Government relies on two cases to support this view, but neither case can bear the weight the Government places on it.

The first is *United States v. Simons*, 206 F.3d 392 (4th Cir. 2000). There, a subdivision of the CIA implemented a new internet usage policy for its employees. *Simons*, 206 F.3d at 395. The policy warned employees that their government employer “shall . . . implement[]” “[e]lectronic auditing” to detect unauthorized internet activity at the office. *Id.* The policy further warned that the government employer would “periodically audit, inspect, and/or monitor the user’s Internet access as deemed appropriate.” *Id.* at 396. The

government employer later checked an employee's internet history and found that he had downloaded files containing CSAM. *Id.*

The employee sought to suppress that evidence, but we held that the internet policy defeated his expectation of privacy in his internet activity. As we explained, “[t]he policy clearly stated that [the government employer] would ‘audit, inspect, and/or monitor’ employees’ use of the Internet, including all file transfers, all websites visited, and all e-mail messages.” *Simons*, 206 F.3d at 398. That policy, we held, “placed employees on notice that they could not reasonably expect that their Internet activity would be private.” *Id.*

At first blush, *Simons* might seem controlling here, but there is a key difference: in *Simons*, the party that provided the warning was the government, not a private third-party service provider. As a result, the *Simons* defendant could not claim an expectation of privacy against the government, notwithstanding the service provider's warning, because it was the government *itself* that warned the defendant that it would monitor how he used the provided service. Not so here. In the case at hand, the Government never issued such a warning. Thus, whereas the Government had no right to monitor Appellant's Google Drive account, Appellant had every right to expect the Government would stay out of his account.

The Government's second case is *United States v. Young*, 350 F.3d 1302 (11th Cir. 2003). In *Young*, Federal Express⁸ used shipping labels that warned customers that Federal

⁸ Federal Express, of course, is a private shipping company, not a government entity.

Express “may, at [its] option, open and inspect your packages prior to or after you give them to us to deliver.” *Young*, 350 F.3d at 1307. Federal Express’s envelopes also explicitly advised its customers “DO NOT SEND CASH.” *Id.* Despite those warnings, the defendant had several packages containing cash shipped to him via Federal Express. *Id.* at 1304. Federal agents investigating the defendant asked Federal Express if it would turn over packages bearing the defendant’s name. *Id.* Federal Express agreed and turned the packages over to the federal agents, who then opened them and found the cash. *Id.* The Eleventh Circuit held that these searches did not intrude on any expectation of privacy. In reaching this conclusion, the court explained, in full:

No reasonable person would expect to retain his or her privacy interest in a packaged shipment after signing a[] [shipping label] containing an explicit, written warning that the carrier is authorized to act in direct contravention to that interest. Federal Express told its customers two things: (1) do not ship cash, and (2) we may open and inspect your packages at our option. As a matter of law, this simply eliminates any expectation of privacy.

Id. at 1308.

With due respect to our sister circuit, we find this analysis unpersuasive. As we explained above, a private party’s warning that it may monitor how someone uses its provided services to prevent misuse does not eliminate Fourth Amendment protections entirely. *United States v. Maher*, 120 F.4th 297, 307–09 (2d Cir. 2024) (holding that Google’s terms of service, which “repeatedly qualif[ied] the content review that the company ‘may’ conduct,” did not negate the defendant’s expectation of privacy against the Government); *Warshak*, 631 F.3d at 286 (“[T]he mere *ability* of a third-party intermediary

to access the contents of a communication cannot be sufficient to extinguish a reasonable expectation of privacy.” (emphasis in original)).

We, therefore, hold that Appellant had a reasonable expectation of privacy in his Google Drive account, and that Google’s warning that it may analyze Appellant’s files did not extinguish that expectation of privacy.

C.

Appellant’s Reasonable Expectation of Privacy in his Digital Files

We next turn to the district court’s second holding: even if Appellant had a reasonable expectation of privacy in his Google Drive generally, he did not have a reasonable expectation of privacy in the 156 files he stored there.

In reaching this conclusion, the district court first found that Google’s proprietary hashing algorithm was “exceedingly reliable,” and then further found that each hash-match demonstrated Appellant’s files contained “obvious” CSAM. J.A. 250–51, 254. From there, the district court reasoned that, because Appellant’s files contained CSAM, a form of contraband, Detective Rider was free to open and view each file. This was allowed, the district court said, because “governmental conduct that only reveals the possession of contraband compromises no legitimate privacy interest.” *Id.* at 251 (quoting *Illinois v. Caballes*, 543 U.S. 405, 408 (2005)). On this issue, the district court erred across the board.

1.

No Record Evidence Supports the Reliability of Google’s Hashing Algorithm

First, the district court committed clear error when it found Google’s proprietary hash-matching technology “exceedingly reliable,” despite there being no record evidence

to support that finding. As noted above, the Government affirmatively waived its opportunity to hold an evidentiary hearing on the motion to suppress, where it could have put on evidence demonstrating the reliability of Google's proprietary algorithm. J.A. 234 ("The United States of America, by and through the United States Attorney for the Eastern District of North Carolina, hereby notifies the Court that the Government does not believe a hearing [on the motion to suppress] is necessary.").

That left the district court with only the briefs and accompanying exhibits to consider when deciding the motion. But those papers contained zero evidence demonstrating that Google's hashing algorithm is "exceedingly reliable." To the contrary, the record evidence indicated that Google's hashing algorithm is fallible inasmuch as it may sometimes "match" two non-identical images. J.A. 140 (affidavit submitted by Google employee that indicated Google's hashing algorithm may match "very similar," but non-identical, images). But, as even the Government conceded at oral argument, the district court ignored that evidence and, instead, simply looked to what other courts had said about Google's hash-matching technology and adopted those findings as its own:

Court: How accurate is the algorithm?

Government: My understanding from the, that hash-matching itself is more than 1 in 9.2 quintillion . . .

Court: And your understanding comes from what, what expert in the record?

Government: There is not [one], Your Honor.

Court: Where did you, how did it get in this record?

Government: [The district court] in [its] order relied on secondary sources in other cases that discussed the reliability of hash-matching, of which there are many.

Oral Argument at 36:37–37:03, *United States v. Lowers*, No. 24-4546 (4th Cir. Dec. 12, 2025), <http://www.ca4.uscourts.gov/oral-argument/listen-to-oral-arguments> (hereinafter “Oral Argument”).

In other words, absent any supporting record evidence in the case at hand, the district court simply took judicial notice of facts adjudicated in other cases. That was error. As we have explained, Federal Rule of Evidence 201(b) allows courts to take judicial notice of adjudicative facts only when “they are ‘generally known within the trial court’s territorial jurisdiction’ or they ‘can be accurately and readily determined from sources whose accuracy cannot be reasonably questioned.’” *United States v. Zayyad*, 741 F.3d 452, 463–64 (4th Cir. 2014) (quoting Fed. R. Evid. 201(b)). Significantly, “[f]acts adjudicated in a prior case . . . do not meet either test of indisputability contained in Rule 201(b).” *Id.* at 464 (internal quotation marks omitted) (first alteration in original) (quoting *Int’l Star Class Yacht Racing Ass’n v. Tommy Hilfiger U.S.A., Inc.*, 146 F.3d 66, 70 (2d Cir. 1998)). The district court therefore erred when it ignored the record before it and borrowed factual findings made in other cases to conclude that Google’s hashing technology can reliably identify previously flagged CSAM.

2.

The Warrant Requirement Applies to Digital Files

The district court further erred in holding that the Government can open and view files containing suspected CSAM without a warrant. In the district court’s view, a hash-

match is no different from a dog sniff “hit,” which the Supreme Court has said provides probable cause that contraband is present. And because dog sniffs provide probable cause to search automobiles without a warrant, the district court reasoned that “it logically follow[ed] that a positive ‘hit’ by Google’s hashing technology on an individual file justifies government inspection of that same file.” J.A. 252. Not so. The district court’s logic does not readily translate to the digital world.

Digital files are containers,⁹ and the Fourth Amendment rules governing container searches are well established. The Supreme Court has held that when officers have probable cause to believe that a container holds contraband, they may seize the container without a warrant. *United States v. Jacobsen*, 466 U.S. 109, 114 (1984). But police must still get a warrant before they can open the container and confirm its contents. *Id.* (“Even when government agents may lawfully seize such a package to prevent loss or destruction of suspected contraband, the Fourth Amendment requires that they obtain a warrant before examining the contents of such a package.”); *see also United States v. Buster*, 26 F.4th 627, 633 (4th Cir. 2022) (“If officers have probable cause to believe a particular place or item contains contraband or evidence of a crime, they can get a warrant to search it”). That holds true no matter how strong a hunch officers have that the container holds contraband.

⁹ A digital file is best thought of as a sealed manila envelope in that both can be used to store all sorts of private documents and photographs, legal and illegal alike. We recognize that this may not be a perfect analogy but just like a sealed manila envelope, law enforcement has no way of determining the precise contents of a digital file unless and until they open it and examine those contents. *See United States v. Galpin*, 720 F.3d 436, 447 (2d Cir. 2013) (explaining that “there is currently no way to ascertain the content of a [digital] file without opening it”).

Horton v. California, 496 U.S. 128, 137 n.7 (1990) (recognizing as a “familiar principle” that “no amount of probable cause can justify a warrantless search or seizure absent ‘exigent circumstances’” (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 468 (1971)). Absent some exception to the warrant requirement, officers cannot open the container without a warrant. See *United States v. Place*, 462 U.S. 696, 701 (1983). Finally, to the extent the district court suggested that a warrantless search of a secured container can nevertheless be reasonable if the search reveals contraband, we reject that means-end methodology -- as has the Supreme Court. *Jacobsen*, 466 U.S. at 114 (explaining that “a warrantless search [of a container holding suspected contraband] could not be characterized as reasonable simply because, after the official invasion of privacy occurred, contraband is discovered”).

But, oddly, the district court nonetheless analogized digital files to vehicles and applied the automobile exception. J.A. 252 (“If a positive ‘hit’ by a drug-detecting canine justifies government inspection of an item as cavernous (and likely to also hold noncontraband) as a vehicle, it logically follows that a positive ‘hit’ by Google’s hashing technology on an individual file justifies government inspection of that same file.” (internal citations omitted)). We need not spend much time debunking this line of reasoning, as even a cursory analysis demonstrates why the district court’s application of that exception was misguided.

The Supreme Court has carved out the so-called “automobile exception” from the warrant requirement, allowing officers to search a vehicle when there is probable cause that the vehicle contains contraband. *United States v. Brookins*, 345 F.3d 231, 235 (4th

Cir. 2003) (“Under the ‘automobile exception,’ “[i]f a car is readily mobile and probable cause exists to believe it contains contraband, the Fourth Amendment . . . permits police to search the vehicle without more.” (alterations in original) (quoting *Maryland v. Dyson*, 527 U.S. 465, 466 (1999) (per curiam))). The Court has identified two rationales for that exception. First, vehicles can flee the scene on a moment’s notice, meaning criminals could easily move, hide, or even destroy their contraband if police had to leave the scene and obtain a warrant before searching the vehicle. *See Collins v. Virginia*, 584 U.S. 586, 591 (2018). Second, vehicles are placed in the public space and subject to “pervasive schemes of regulation,” such as inspections and traffic stops, which “significantly” diminishes the driver’s expectation of privacy in the contents of his vehicle. *California v. Carney*, 471 U.S. 386, 391, 392 (1985).

But those rationales are unique to automobiles, and neither apply here. For one thing, Appellant’s files were not in jeopardy of being lost or destroyed. Far from it. Google had copied each of the 156 files and sent them to NCMEC, which then forwarded them to law enforcement. Law enforcement could have easily obtained a warrant before opening the files, and any delay would not have hampered the investigation -- the files were not going anywhere. Indeed, the files were maintained for over seven months before Detective Rider even looked at them. Nor is there any indication that the files in Appellant’s Google Drive were ever made public or subject to government regulation. They were instead hidden in a cloud based storage system, a digital file cabinet of sorts, inaccessible to law enforcement.

At the risk of stating the obvious, digital files are not automobiles. The two things are poles apart, and the Fourth Amendment treats them differently. The district court erred in concluding otherwise.

D.

Private Search Exception

We now take up the district court's third reason for holding that no search occurred here: the private search doctrine. The district court found that Google's hash-matching of each file in Appellant's Google Drive proved that someone at Google had already viewed the images in those files. And because someone at Google had previously seen each image in Appellant's files, the district court reasoned that Google's private hashing algorithm had frustrated Appellant's expectation of privacy in those files. The district court thus applied the private search doctrine and held that Detective Rider could open and view the three yet unopened files that she did without a warrant, because Appellant had no remaining expectation of privacy in them.

This issue -- whether a defendant's expectation of privacy in his digital files can be defeated by a hash-match -- has divided our sister circuits. *Compare United States v. Maher*, 120 F.4th 297 (2d Cir. 2024) (holding that a hash-match alone does not defeat a reasonable expectation of privacy in an unopened digital file), and *United States v. Wilson*, 13 F.4th 961 (9th Cir. 2021) (same), with *United States v. Miller*, 982 F.3d 412 (6th Cir. 2020) (holding that a hash-match to apparent CSAM defeats a reasonable expectation of privacy in an unopened file), and *United States v. Reddick*, 900 F.3d 636 (5th Cir. 2018) (similar).

The Limits of the Private Search Exception

In staking out our position, we begin with the basic principle that “[w]arrantless searches are *per se* unreasonable unless they fall within one of the few specifically established and well-delineated exceptions to the Fourth Amendment’s warrant requirement.” *United States v. Taylor*, 54 F.4th 795, 803 (4th Cir. 2022) (internal quotation marks omitted) (quoting *United States v. Davis*, 690 F.3d 226, 241–42 (4th Cir. 2012)).

The private search doctrine is one of those exceptions. *United States v. Fall*, 955 F.3d 363, 370–71 (4th Cir. 2020). The Fourth Amendment, after all, prevents only unreasonable searches by the government, not private actors. *United States v. Richardson*, 607 F.3d 357, 364 (4th Cir. 2010). That means a search conducted by a private party, “no matter how unreasonable,” does not implicate the Fourth Amendment. *Id.* And should a private party conduct their own search and discover evidence, they can turn that evidence over to the police, who need not “avert their eyes” from what the private party has put in plain view. *Coolidge*, 403 U.S. at 489; *Fall*, 955 F.3d at 370 (“[W]hen a third party provides the police with evidence that she obtained in the course of her own search, the police need not stop her or avert their eyes.” (internal quotation marks and citation omitted)).

The private search doctrine may seem simple, but it can sometimes lead to thorny questions. Suppose, for instance, that a private party searches someone else’s container, say, a backpack, and they find incriminating evidence within. Now further suppose that, instead of taking the evidence straight to the police, the private party puts it back in the

backpack as they found it and they take the entire backpack to the police. Can the police open the backpack on the spot and retrieve the previously discovered evidence? Or must they first secure a warrant? The answer depends on whether the police's subsequent search will "exceed the scope of the private search" and reveal any additional information in which the defendant's "expectation of privacy has not already been frustrated." *Jacobsen*, 466 U.S. at 116, 117 (citation omitted).

The Supreme Court has handed down a pair of opinions illustrating this concept, starting with *Walter v. United States*, 447 U.S. 649 (1980) (plurality). In *Walter*, a shipment of obscene films was mailed to the wrong recipient. *Walter*, 447 U.S. at 651. The unintended recipient opened the packages and found film boxes with "suggestive drawings" on one side and "explicit descriptions of the contents" on the other side. *Id.* at 652. The unintended recipient also opened an individual film box and held the film up to the light, trying to determine the film's contents. *Id.* But that proved fruitless, so they called the FBI, who seized the films. *Id.* Without first obtaining a warrant, FBI agents then viewed the films with a projector and confirmed that they showed obscenity. *Id.*

The Supreme Court held that this was a search. In doing so, the Court explained that the Fourth Amendment's private search exception allowed the Government to "examin[e] [the packages'] contents to the extent that they had already been examined by third parties." *Walter*, 447 U.S. at 656. But the Court further explained, "the Government may not exceed the scope of th[at] private search unless it has the right to make an independent search." *Id.* at 657. The Court then held that the FBI's "projection of the films was a significant expansion of the [private party's] search" that revealed information

previously unknown -- such as confirming the films' suspected contents -- and therefore exceeded the scope of the private search. *Id.*

The Court revisited the private search doctrine a few years later in *United States v. Jacobsen*, 466 U.S. 109 (1984). In *Jacobsen*, Federal Express workers opened a damaged package in order to assess the damage. *Jacobsen*, 466 U.S. at 111. Inside they found a tube that contained several baggies, which themselves contained a white powder. *Id.* The workers stuffed the baggies back in the tube, the tube back in the box, and then called the Drug Enforcement Administration ("DEA"). *Id.* The DEA then reopened the package and conducted a chemical field test using a trace amount of the powder. *Id.* at 111–12. The field test confirmed the powder to be cocaine. *Id.* at 112.

The Court said this was not an unreasonable search. The Court first explained that the Federal Express workers' opening of the box was private action that did not implicate the Fourth Amendment. *Jacobsen*, 466 U.S. at 115. The DEA agent, the Court said, was entitled to repeat that process and reopen the package because "there was a virtual certainty that nothing else of significance was in the package[,] [meaning] a manual inspection of the tube and its contents would not tell him anything more than he already had been told." *Id.* at 119. As for the field test, that did not violate the Fourth Amendment, the Court said, because it "could disclose only one fact previously unknown to the agent—whether or not a suspicious white powder was cocaine." *Id.* at 122. And because binary "test[s] that merely disclose[] whether or not a particular substance is cocaine does not compromise any legitimate interest in privacy," the Court held that this additional intrusion implicated no additional privacy interest and was therefore permissible. *Id.* at 123.

2.

The Government's Search Exceeded the Scope of the Private Search

That brings us back to the case at hand. As noted above, the district court found that Google's hash-matches proved that each image in Appellant's digital files had already been viewed by someone at Google. In the district court's view, this meant that law enforcement could open and view Appellant's files without a warrant because, like in *Jacobsen*, doing so (1) would reveal nothing that had not been previously seen by a private actor and (2) would only confirm that each file contained contraband. Again, we disagree.

a.

To start, the district court had no evidentiary basis to conclude that someone at Google had previously viewed the images in Appellant's files. As discussed above, there is no evidence in the record that demonstrates the reliability of Google's proprietary hashing technology, and the district court was not permitted to borrow factual findings made by other courts to fill that gap. The district court thus had no way of assuring itself that Google had actually seen the images in Appellant's files before. That evidentiary shortcoming alone should have foreclosed the private search doctrine's application from the start.

The district court compounded that error when it saddled Appellant with the burden of disproving the reliability of Google's proprietary technology. J.A. at 255 (faulting Appellant for "not contest[ing] the reliability of Google's hashing technology," despite there being no evidence of its reliability in the record). But it is fundamental that Appellant

did not carry that burden. Rather, the Government carried the burden of *establishing* the technology's reliability in the first instance.

The private search doctrine, after all, is an exception to the warrant requirement. *Fall*, 955 F.3d at 370. So once Appellant satisfied his initial burden of establishing an expectation of privacy in his Google Drive, the burden shifted to the Government to prove that Appellant's expectation of privacy had been frustrated. *See United States v. Aigbekaen*, 943 F.3d 713, 719 (4th Cir. 2019) (explaining that where "the Government conduct[s] the challenged searches without warrants, it bears the burden of proving, by a preponderance of the evidence, that an exception to the warrant requirement applies."); *see also United States v. Maher*, 120 F.4th 297, 316 n.18 (2d Cir. 2024) ("[W]here the government relies on hash matching or other technology to carry that burden, it assumes the obligation of demonstrating the technology's reliability."); *United States v. Wilson*, 13 F.4th 961, 979 (9th Cir. 2021) (similar); *but see United States v. Miller*, 982 F.3d 412, 430 (6th Cir. 2020) (relying on Sixth Circuit precedent when placing on the defendant the burden of disproving the reliability of hash-matching technology). Yet, as the Government acknowledged, it made no effort to meet its burden here. Oral Argument at 37:42–38:00.

Appellant therefore had no obligation to try and disprove the reliability of technology that the Government failed to establish as reliable in the first instance, and the district court erred in concluding otherwise.

b.

Beyond the evidentiary issues, the district court's approach on the merits ignored the basic truth that Fourth Amendment rights are personal. *Rakas v. Illinois*, 439 U.S. 128,

133–34 (1978). In other words, “a defendant can mount a Fourth Amendment challenge only if he has his own cognizable Fourth Amendment privacy interest in the invaded place.” *United States v. Green*, 106 F.4th 368, 375 (4th Cir. 2024). If the defendant cannot make that showing, he cannot complain about the search. *United States v. Ferebee*, 957 F.3d 406, 412 (4th Cir. 2020).

Here, the district court did not find -- and the Government does not contend -- that Google had previously opened and viewed **any** of the three files belonging to Appellant that Detective Rider opened and viewed. *See* Oral Argument at 38:38–58 (Government conceding that Google had not opened any of the same files as Detective Rider). Instead, Google purportedly opened and viewed files belonging to some unknown third party, which purportedly contained the same images as those three files belonging to Appellant - - which Google did not open and view.¹⁰ Appellant, no doubt, would have lacked standing to challenge a government search of the files belonging to the third party, as he could not have had a reasonable expectation of privacy in files belonging to a stranger. *See United States v. Daniels*, 41 F.4th 412, 415 (4th Cir. 2022) (explaining that courts “look to ‘concepts of real or personal property law or to understandings that are recognized and permitted by society’” when “determin[ing] whether a legitimate expectation of privacy exists” (quoting *Byrd v. United States*, 584 U.S. 395, 405 (2018))).

¹⁰ We say purportedly because, as explained above, there is no basis to conclude that Google had actually seen the images in Appellant’s files on a prior occasion.

The inverse must also be true. If Appellant could not challenge a government search of someone else's files because that search did not implicate his privacy interests, then Google's visual examination of a third-party's files could not affect, much less frustrate, Appellant's expectation of privacy in his own unopened files. *Maher*, 120 F.4th at 319 (“[J]ust as Maher cannot claim any expectation of privacy in Google's earlier visual examination of the original image, which did not belong to him . . . the government cannot claim that Google's visual search of that third-party file somehow defeated Maher's expectation of privacy in the contents of his own unopened, unreviewed file as against the government.”); *Wilson*, 13 F.4th at 975 (“[W]hether Google had previously reviewed, at some earlier time, other individuals' files is not pertinent to whether a private search eroded Wilson's expectation of privacy.” (emphasis omitted)). It does not matter that the images contained in the third party's files were purportedly identical to those in Appellant's files. They were found in *different files, belonging to a different person*. Google's inspection of those third party files did not -- indeed, could not -- affect Appellant's expectation of privacy in his own files.

c.

The district court's private search analysis suffered from another fatal flaw: the district court was under the impression that Detective Rider could open and view Appellant's files without a warrant because doing so would expose “nothing of significance that Google had not already identified.” J.A. 255. We disagree.

At the outset, the district court misunderstood the extent and nature of Google's private search. As explained above, no one at Google had ever opened and laid eyes on

the contents of the three files that Detective Rider viewed. The Government and Google have both conceded as much. Oral Argument at 38:38–58; *see also* J.A. 95–130 (CyberTip report made by Google explicitly stating which files Google had opened and which files remained unopened).

Google had instead run those three files through a computer algorithm, which spit out an indecipherable serial number for each image that, in isolation, provides no useful information.¹¹ *See United States v. Arce*, 49 F.4th 382, 392 (4th Cir. 2022) (“The hash value of a file standing alone [tells] little; it . . . is just raw data.”). True, Google’s algorithm produced each hash value by performing a pixel-by-pixel analysis of each image. But that analysis revealed nothing else about the image itself, and it could not -- as Detective Rider later did -- describe the contents of the image. *Wilson*, 13 F.4th at 972 (detailing the “gulf” of information revealed between a computer hash-match and an officer’s actual inspection of an image). Because Detective Rider’s visual examination revealed information that the algorithm could not, the district court erred in concluding that her search did not exceed Google’s private search. It clearly did.

¹¹ By way of example, here are just a few of the hash values contained in the CyberTip report that Google extracted from Appellant’s unopened files:

- 9d9df8fb41373b15a734ace17db2a6ab
- 5f5c89bc795c09ac66c831bb92b4e674
- 1db4dd93cefd862311c39bd645481738

J.A. 134.

Google itself acknowledges that the purpose of Google Reviewers actually opening and viewing the files is to *confirm* what the files are. J.A. 140 (affidavit of Google employee explaining that Google Reviewers will examine hash-matched files to “confirm[] the previously viewed file contained Reportable CSAM”). As explained above, the algorithm alone cannot do that.

Walter confirms the conclusion that Detective Rider exceeded the scope of Google’s private search. There, just like here, law enforcement were given containers, each of which contained suspected contraband. *Walter*, 447 U.S. at 652. And there, just like here, a private party had previously examined the containers’ contents to try and confirm or dispel that belief, but to no avail. *Id.* And here, just like there, law enforcement had to use different means of inspection that revealed information previously unknown. *Id.* So here, just like there, law enforcement exceeded the scope of the private party’s search.

However, the district court thought this case hewed closer to *Jacobsen*. The district court was of the view that Google’s hash-match confirmed that each of Appellant’s files contained only contraband, which meant that Detective Rider was free to rifle through each file without any risk of exposing private, non-contraband information. In other words, the district court thought that Detective Rider’s inspection of the files was no different than the field test in *Jacobsen* because, much like the chemical field test, her “inspection would only confirm that the image contained [CSAM].” J.A. 256.

This, too, was error. Putting aside that there was no evidentiary basis to rely on Google’s hash-match (as we have detailed throughout this opinion), the district court

erroneously equated physical inspection of an apparent CSAM image with a chemical field test of suspected narcotics.

The Supreme Court has long held that binary tests, such as dog sniffs and chemical field tests, do not implicate the Fourth Amendment. This is because those binary tests “disclose[] only the presence or absence of narcotics, a contraband item,” and nobody has a reasonable expectation of privacy in possessing contraband. *United States v. Place*, 462 U.S. 696, 707 (1983); *see also United States v. Johnson*, 148 F.4th 287, 292 (4th Cir. 2025) (explaining that dog sniffs and chemical field tests “cannot violate any reasonable expectation of privacy” because they “expose[] only the presence or absence of narcotics” (internal quotation marks and citation omitted)). But those binary tests are *sui generis*. *Place*, 462 U.S. at 707. They tell law enforcement nothing but a yes-or-no, a thumbs-up or thumbs-down, about whether the substance is contraband.

Opening and viewing a digital file, by contrast, risks exposing much more. Every time law enforcement opens and views a file that contains apparent CSAM, there is a non-trivial, and unavoidable, possibility that they will view non-contraband material. *Cf. Riley v. California*, 573 U.S. 373, 395 (2014) (recognizing that the immense storage capacity of modern cell phones make them “a cache of sensitive personal information”).

Every hashing process, after all, carries with it a certain amount of error -- both human and computer. Indeed, even if the hashing algorithm is 100% accurate, there remains the possibility that the human reviewer (who viewed the image previously) misjudged it and erroneously labeled non-CSAM images (protected by the Fourth

Amendment) as CSAM (contraband).¹² *Arce*, 49 F.4th at 393 (explaining that the determination of whether “a given image is [CSAM]” depends on human judgment, and therefore the labeling as such for future hashing purposes does as well); *see also United States v. Holmes*, 121 F.4th 727, 732 n.2 (9th Cir. 2024) (finding a Fourth Amendment violation where Facebook reported a hash-match of apparent CSAM that did not meet the federal statutory definition, and the FBI agent who received the tip opened and viewed the two provided images without a warrant). Thus, unlike a binary drug field test, the Government cannot open and view a hash-matched file without running the risk of exposing private, non-contraband material. This is not a risk the Fourth Amendment allows.

* * *

An officer’s decision to search an unopened digital file that a hash-matching algorithm flagged as containing apparent CSAM implicates serious privacy concerns, and the district court erred in whisking away those concerns. Today we hold that a hashing algorithm, which reveals nothing about a given file but a non-descriptive serial number, does not frustrate a defendant’s expectation of privacy in his unopened files. We further hold that, unless someone visually inspects the contents of a file containing apparent CSAM prior to law enforcement doing the same, the defendant maintains a reasonable expectation of privacy in the file and the private search doctrine is inapplicable. In reaching

¹² The federal CSAM reporting statute implicitly recognizes this reality: it requires internet service providers to report “apparent” CSAM, thus recognizing the difference between suspected and adjudicated CSAM. *See* 18 U.S.C. § 2258(A).

this holding, we align ourselves with the Second and Ninth Circuits, which have reached the same conclusion. *United States v. Maher*, 120 F.4th 297 (2d Cir. 2024); *United States v. Wilson*, 13 F.4th 961 (9th Cir. 2021).

We recognize that our holding puts us at odds with the Fifth and Sixth Circuits. In *Reddick*, the Fifth Circuit, like the district court below, held that a hash-match suggested that a file contains CSAM, and further held that law enforcement can, consistent with the Fourth Amendment, open a hash-matched file without a warrant because doing so only confirms that the file contains suspected contraband. *Reddick*, 900 F.3d at 639. But, as we explained above, the Supreme Court has held that no amount of probable cause can justify a warrantless search of a container absent exigent circumstances, *Horton v. California*, 496 U.S. at 137 n.7, and the results of a warrantless search cannot cure the search's illegality, *Jacobsen*, 466 U.S. at 114. The end does not justify the means.

The Sixth Circuit, in *Miller*, held that a private party's hash-matching algorithm defeated the defendant's reasonable expectation of privacy in his files. *Miller*, 982 F.3d at 429–31. In doing so, the Sixth Circuit equated a human's inspection of unknown third parties' files with the defendant's files, and held that the prior inspection frustrated the defendant's reasonable expectation of privacy in his identical files. *Id.* at 430. Critically, however, the court never considered the personal nature of Fourth Amendment rights, and that analytical oversight is fatal to the analysis. Searching a stranger's files does not impact a defendant's expectation of privacy in his own files.

Because we conclude that the Fifth and Sixth Circuit's contrary decisions each rest on faulty reasoning, we decline to follow either decision.

Despite these analytical shortcomings, our concurring colleague would have us join the Fifth and Sixth Circuits. In articulating this position, the concurring opinion describes the private search exception as “stand[ing] for the well-founded and sensible proposition” that the Fourth Amendment does not bar law enforcement from “merely review[ing] the same information that was discovered during the private search.” *Post* at 47. We do not quarrel with our colleague’s description of the private search doctrine, but those are not the facts of this case. As we explain above, Detective Rider did not merely review the hash values derived from Google’s private search. Detective Rider went beyond the extent of the private search when she opened and viewed Appellant’s private files -- an act that even the Government concedes Google had not done. And because Detective Rider’s visual examination of Appellant’s files revealed information previously unknown, the private search exception -- as articulated by our concurring colleague -- does not apply here.

E.

Attenuation Doctrine

Having established that Detective Rider violated the Fourth Amendment when she opened and viewed Appellant’s three files without a warrant, we next consider whether the district court was correct in ruling that the exclusionary rule’s attenuation exception applied.

1.

The Limits of the Exclusionary Rule

The Fourth Amendment prohibits unreasonable searches. U.S. Const. amend. IV. But it says nothing about what to do when one occurs. *Davis v. United States*, 564 U.S.

229, 236 (2011). However, to “compel respect for th[is] constitutional guaranty,” *Elkins v. United States*, 364 U.S. 206, 217 (1960), the Supreme Court has created the exclusionary rule, which “provides that evidence obtained in violation of the Fourth Amendment cannot be used in a criminal proceeding against the victim of the illegal search and seizure.” *United States v. Ray*, 141 F.4th 129, 134 (4th Cir. 2025). The exclusionary rule applies to “evidence obtained as a direct result of an illegal search,” as well as “evidence later discovered and found to be derivative of an illegal[] [search],” known as the “fruit of the poisonous tree.” *Utah v. Strieff*, 579 U.S. 232, 237 (2016) (internal quotation marks omitted) (quoting *Segura v. United States*, 468 U.S. 796, 804 (1984)).

Importantly, the exclusionary rule is not an individual right, and it is not intended to remedy every Fourth Amendment violation. *Herring v. United States*, 555 U.S. 135, 141 (2009). The exclusionary rule is instead a deterrent measure designed to reduce future police misconduct. *United States v. Leon*, 468 U.S. 897, 906 (1984) (“The rule thus operates as ‘a judicially created remedy designed to safeguard Fourth Amendment rights generally through its deterrent effect, rather than a personal constitutional right of the party aggrieved.’” (quoting *United States v. Calandra*, 414 U.S. 338, 348 (1974))). As a result, the exclusionary rule does not apply as a matter of course for each and every Fourth Amendment violation. *Arizona v. Evans*, 514 U.S. 1, 13 (1995) (explaining that the Supreme Court has come to “reject[] [a] reflexive application of the exclusionary rule”).

For these reasons, the Supreme Court has “limited the [exclusionary] rule’s operation to [only those] situations in which [its deterrent] purpose is ‘thought most efficaciously served.’” *Davis*, 564 U.S. at 237 (quoting *Calandra*, 414 U.S. at 348). In

other words, exclusion is a “last resort, not [a] first impulse,” *Hudson v. Michigan*, 547 U.S. 586, 591 (2006), and courts should refuse to apply the exclusionary rule where its application would yield no real “appreciable deterrence,” *Herring*, 555 U.S. at 141 (quoting *Leon*, 468 U.S. at 909).

The Supreme Court has, over the years, identified several scenarios where it would make little sense to apply the exclusionary rule because doing so would not deter future police misconduct. *Strieff*, 579 U.S. at 238. Relevant here, the Supreme Court has said suppression is unwarranted where “the [causal] connection between [the] unconstitutional police conduct and the evidence is remote or has been interrupted by some intervening circumstance.” *Id.* This is so, the Court has said, because suppressing evidence seized too far downstream from a prior illegal search, or evidence that is the product of an intervening act that broke the causal chain, would do little to vindicate “the interest protected by the constitutional guarantee that has been violated.” *Id.* (quoting *Hudson*, 547 U.S. at 593).

Known as the attenuation doctrine, this analysis “evaluates the causal link between the government’s unlawful act and the discovery of evidence.” *Strieff*, 579 U.S. at 238. We have said that “a direct, unbroken chain of causation is necessary, but not sufficient[,] to render derivative evidence inadmiss[i]ble.” *United States v. Najjar*, 300 F.3d 466, 477 (4th Cir. 2002). “Rather, the more apt question” in the attenuation analysis is this: was the evidence of conviction obtained “by exploitation of” the illegal search, or was it instead discovered “by means sufficiently distinguishable [from the illegal search so as] to be purged of the primary taint”? *Wong Sun v. United States*, 371 U.S. 471, 488 (1963) (citation omitted).

We use a three-part test when “determin[ing] whether the fruit [of an illegal search] is no longer poisonous,” that is, whether it is sufficiently attenuated from the illegal search. *Najjar*, 300 F.3d at 477. First, we consider “the amount of time between the illegal action and the acquisition of the evidence.” *Id.* Second, we look for “the presence of intervening circumstances.” *Id.* Third, and finally, we scrutinize “the purpose and flagrancy of the official misconduct.” *Id.* And “[w]hat suffices to dissipate the taint from derivative evidence depends on the specific facts and circumstances of each case.” *Id.* Because we analyze factors, not elements, “[n]o single fact is dispositive.” *Brown v. Illinois*, 422 U.S. 590, 603 (1975).

2.

The Attenuation Exception Applies Here

Here, Appellant does not seek suppression of the three files that Detective Rider opened and viewed without a warrant because he was not charged with possessing those files. Appellant instead seeks suppression of the later discovered evidence that flowed from that search, i.e., his hard drive, flash drive, and confession.¹³ The district court conducted the three factor analysis outlined above and concluded that each factor counseled against suppression. We agree.

First, the amount of time that elapsed between the illegal search and the later discovered evidence in North Carolina -- seven months -- is significant. We and the

¹³ Appellant’s briefing does not specifically indicate whether he is seeking to suppress the four CSAM images found on his cell phone, and the record is unclear as to whether that was evidence used to convict him. However, to the extent Appellant seeks
(Continued)

Supreme Court have found far smaller stints of time sufficient to purge the taint of an illegal search. *Wong Sun*, 371 U.S. at 491 (several days passed between illegal arrest and subsequent voluntary confession); *United States v. Seidman*, 156 F.3d 542, 549 (4th Cir. 1998) (moments passed between a warrantless entry into the defendant's home and his striking up an incriminating conversation with a government informant); *United States v. Hooker*, 54 F.3d 774 (Table), at *2 (4th Cir. 1995) (one hour passed between an illegal seizure and later consensual search that revealed evidence). Appellant makes no effort to explain why this case is any different, and we see none.

The second factor -- the presence of intervening circumstances -- also cuts the Government's way. We and the Supreme Court have long recognized that voluntary acts of a defendant are "the quintessential act[s] of free will" that "sever the connection between an unlawful act and the acquisition of additional evidence." *Seidman*, 156 F.3d at 549 n.10. In *Wong Sun*, for instance, the defendant was illegally arrested, arraigned the next day, and then released on his own recognizance. *Wong Sun*, 371 U.S. at 491. He voluntarily returned to the police station later that week and confessed. *Id.* The Supreme Court held that the defendant's decision to return to the police station made the causal chain "so attenuated as to dissipate the taint." *Id.* Similarly, in *Seidman*, we held that a defendant's decision to begin a 45 minute long incriminating conversation with a government

suppression of those four files, we find suppression unwarranted because Appellant consented to a search of his phone, and that voluntary act broke the causal chain, rendering suppression unnecessary.

informant that had just illegally entered into his house was an “intervening circumstance[]” that purged “any taint arising from” the illegal entry. *Seidman*, 156 F.3d at 549.

Here, Appellant’s intervening voluntary acts attenuated the causal chain, thus purging any taint that flowed from Detective Rider’s illegal search. First, Appellant voluntarily submitted to not one, but two consensual interviews with authorities. Second, and relatedly, he allowed law enforcement to search his phone and laptop, a decision that revealed new CSAM and further fueled the investigation against him. Third, Appellant voluntarily confessed to downloading CSAM and transporting it across state lines, and he also told law enforcement where they could find his flash drive, which stored a portion of the evidence he now seeks to suppress. Each of these intervening voluntary acts significantly attenuated the causal chain.

That leaves the third factor -- the purpose and flagrancy of the officer’s misconduct. “Flagrancy,” in this context, means more than a “‘technical’ Fourth Amendment violation[.]” *Brown*, 422 U.S. at 610 (Powell, J., concurring in the judgment). It means an “*abusive* violation of [the] Fourth Amendment.” *Id.* (emphasis supplied); *see also Strieff*, 579 U.S. at 241 (“The third factor of the attenuation doctrine reflects [the exclusionary rule’s deterrence] rationale by favoring exclusion only when the police misconduct is most in need of deterrence—that is, when it is purposeful or flagrant.”). And here, Detective Rider’s misconduct was anything but flagrant. Make no mistake, she violated the Fourth Amendment when she opened and viewed Appellant’s files without a warrant. But there is no evidence in this record to suggest that Detective Rider opened and viewed Appellant’s files intending to circumvent the Fourth Amendment’s warrant requirement. And, any

“mistake [due to] ignorance of the law” is a far cry from flagrancy. *United States v. Terry*, 909 F.3d 716, 722 (4th Cir. 2018). Therefore, the third factor also counsels against suppression.

Because all three factors tip toward attenuation, we agree with the district court and conclude that the attenuation exception applies here.

3.

Appellant’s Arguments to the Contrary are Unpersuasive

Appellant attempts to rebut this conclusion, but none of his arguments are persuasive. Appellant first emphasizes the “cascading” series of events that led to his arrest, many of which followed Detective Rider’s Fourth Amendment violation, and he suggests that the causal connection alone requires suppression. Appellant’s Br. at 41–44. But, in doing so, Appellant ignores the fact that although a Fourth Amendment violation is a necessary condition for suppression, it is not always sufficient. *Najjar*, 300 F.3d at 477 (“[A] direct, unbroken chain of causation is necessary, but not sufficient to render derivative evidence inadmiss[i]ble.”). And where, as here, law enforcement’s investigative efforts are subsequently aided through a series of independent acts of free will on the part the defendant, the causal chain becomes too attenuated to warrant suppression. *Strieff*, 579 U.S. at 238.

Perhaps realizing that his first argument goes nowhere, Appellant takes a slightly different tack in his next. He points out that each search warrant issued in this case -- including the final search warrant for his apartment -- included the results of Detective Rider’s illegal search. He then argues that, because each warrant was issued, at least in

part, on account of the illegal search, the eventual seizure of his hard drive and flash drive, along with his confession, “c[a]me a[bout] by the exploitation of that illegality.” Appellant’s Br. at 40 (quoting *Wong Sun*, 371 U.S. at 471).

While we certainly do not condone police practices such as this, we do not find much merit in Appellant’s position. As detailed above, Detective Rider’s unconstitutional search led police to Appellant’s parents’ house, but that was a dead end. If Appellant’s parents had not voluntarily consented to an interview, the investigation would have ended there. Further, each subsequent search warrant application (including the final one) included all the mounting additional evidence gathered once the investigation was redirected toward Appellant. That, in our view, demonstrates that the evidence here -- Appellant’s flash drive, hard drive, and confession -- were discovered “by means sufficiently distinguishable to be purged of the primary taint.” *Wong Sun*, 371 U.S. at 488.

Finally, Appellant contends that his consent to search his devices could not attenuate the causal chain because that consent was influenced by his knowledge of the illegal search. However, there is no record evidence bearing out this assertion, and our standard of review precludes us from drawing such an inference. *United States v. Bailey*, 74 F.4th 151, 156 (4th Cir. 2023) (explaining that when “a suppression motion has been denied, this Court reviews the evidence in the light most favorable to the government” (quoting *United States v. Abdallah*, 911 F.3d 201, 209 (4th Cir. 2018))).

For these reasons, we agree with the district court and hold that the attenuation doctrine applies here, making suppression unwarranted.¹⁴

IV.

Although the district court erred in holding that there was no Fourth Amendment violation, it correctly determined that the attenuation doctrine precluded suppression. For that reason, the judgment is

AFFIRMED.

¹⁴ Because we conclude that the attenuation exception applies, we decline to address the district court's ruling on the good faith exception.

KING, Circuit Judge, concurring in the judgment:

I am pleased to concur in the panel majority’s judgment in this criminal appeal from the Eastern District of North Carolina. Put simply, the majority is entirely correct in its bottom-line conclusion that the district court properly denied defendant Nico Lowers’s motion to suppress evidence of child pornography. In my view, however, there is no need to reach or address whether the evidence utilized by the prosecutors to convict Lowers was sufficiently attenuated from what the majority rules was an “illegal search” by law enforcement in opening and viewing electronic images of apparent child pornography identified by Google. *See ante*, at 3. Rather, I would simply join with the Fifth and Sixth Circuits and rule that the “private search doctrine” — which stands for the well-founded and sensible proposition that “the Fourth Amendment is not implicated by a private search,” when law enforcement “merely review[s] the same information that was discovered during the private search” by a private party (i.e., Google), *see United States v. Fall*, 955 F.3d 363, 370 (4th Cir. 2020) — inoculates against any Fourth Amendment violation being attributable to Lowers. *See, e.g., United States v. Reddick*, 900 F.3d 636 (5th Cir. 2018); *United States v. Miller*, 982 F.3d 412 (6th Cir. 2020).

On that basis, I am satisfied to affirm the judgment of conviction and sentence entered by the district court.