FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, *Plaintiff - Appellee*, v. DUANE LEE JOHNSEN, AKA Duane Lee Johnson, *Defendant - Appellant*.	No. 24-6689 D.C. No. 4:21-cr-01118-JCH-JR-1 OPINION

Appeal from the United States District Court
for the District of Arizona
John Charles Hinderaker, District Judge, Presiding

Argued and Submitted March 2, 2026
Phoenix, Arizona

Filed May 26, 2026

Before: Richard R. Clifton, Jay S. Bybee, and Eric D. Miller, Circuit Judges.

Opinion by Judge Clifton

SUMMARY*

Criminal Law

The panel affirmed Duane Lee Johnsen's conviction for receiving child pornography, in violation of 18 U.S.C. § 2252, and accessing and possessing child pornography, in violation of 18 U.S.C. § 2252A.

Johnsen argued that the district court erred in denying his motion to suppress evidence obtained from the search of his home and devices.

- Johnsen contended that because officers had not downloaded and viewed any of the suspect files from his computer, it was improper for the magistrate judge who issued the search warrant to find probable cause based in part on evidence that Johnsen possessed files with hash values matching known child pornography. The panel disagreed because a hash match between a suspect's files and known child pornography amply supports the reasonable inference that such material is present on the suspect's devices, even if agents have not downloaded and viewed the suspect file, and the hash matches were bolstered by substantial additional evidence that independently supported the finding of probable cause.
- The panel held that Johnsen's arguments that law enforcement's review of his public files on a peer-to-

* This summary constitutes no part of the opinion of the court. It has been prepared by court staff for the convenience of the reader.

> peer filesharing account violated his Fourth Amendment rights and the Wiretap Act are squarely foreclosed by this court's precedent.

Johnsen argued that the district court erred in denying his motion to dismiss the indictment because he was prejudiced when officers forensically analyzed his devices without his counsel present, and because he was wrongfully targeted for selective prosecution due to his prior conviction for offenses against children. The panel rejected these arguments because Johnsen had no right to an attorney's presence during the forensic analysis, which was not a critical stage of the prosecution, and Johnsen presented no evidence that he received differential treatment or was targeted for prosecution due to an impermissible prosecutorial motive.

Because Johnsen did not pinpoint any element of his conviction as being inadequately supported, nor offer any specific arguments or record citations to support his summary assertion that the Government failed to present sufficient evidence, the panel declined to review the district court's denial of Johnsen's motion for judgment of acquittal.

COUNSEL

Karla H. Delord (argued), Assistant United States Attorney; William G. Vot, Appellate Division Chief; Timothy Courchaine, United States Attorney; Office of the United States Attorney, United States Department of Justice, Phoenix, Arizona; for Plaintiff-Appellee.

Stephanie K. Bond (argued), Law Offices of Stephanie K Bond PC, Tucson, Arizona, for Defendant-Appellant.

OPINION

CLIFTON, Circuit Judge:

Defendant Duane Lee Johnsen was arrested after law enforcement executed a search warrant for his home and discovered copious amounts of child pornography stored on his electronic devices. Johnsen was convicted under 18 U.S.C. § 2252 for receiving child pornography, as well as under 18 U.S.C. § 2252A for accessing and possessing child pornography. On appeal, he challenges the district court's denial of three motions: (1) his motion to suppress evidence seized from his residence; (2) his motion to dismiss the indictment; and (3) his motion for judgment of acquittal. We affirm.

I. Background

During a routine sweep of a peer-to-peer filesharing platform called eMule, law enforcement identified an online profile with the username "Sparky's Engine" that was offering to share at least 19 files of suspected child pornography.

The eMule platform enables its users to offer digital files from their own computers for others to download. Users can search for downloadable content on eMule using keywords; search results then populate with other users' shared files that contain the keywords in their filenames. When a user downloads a file from eMule, he or she causes a digital copy to be saved to his or her computer.

Peer-to-peer filesharing platforms are frequently used as a vehicle for distributing child pornography. Accordingly, law enforcement searches platforms like eMule to identify users who possess child pornography and are offering it for

public download. Officers use special software to locate suspect material by searching for files with the same "hash values" as known child pornography identified in previous investigations.

A hash value is a fixed-length sequence of numbers and letters which is algorithmically derived from the contents of a digital file. It acts as "a sort of digital fingerprint." *United States v. Ackerman*, 831 F.3d 1292, 1294 (10th Cir. 2016). Two identical files—like two copies of the same digital image—will always have the same hash value. *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 541 (2005) (footnote omitted). While distinct files could theoretically have the same hash value, "[t]he chance of two different inputs 'colliding' . . . is astronomically small." Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 Harv. L. Rev. F. 38, 39 (2005). The capacity to identify identically matching files with a high degree of accuracy has made hashing "an important fixture" in law enforcement investigations involving digital media and computer forensics. *Id.* at 38; *see also* Federal Bureau of Investigation, *Privacy Impact Assessment (PIA) Child Victim Identification Program (CVIP) Innocent Images National Initiative (IINI)* (May 9, 2003), https://perma.cc/568D-2UAY (discussing use of hash values in child pornography investigations).

Johnsen's eMule account was flagged by law enforcement software as possessing files with hash values that matched previously identified child pornography. Agents attempted to download the files from "Sparky's

Engine" but were unable to do so.[1] Nonetheless, they could still view certain information about the files, including their hash values and filenames. Agents were able to match the hash values of nine files to those of known child pornography files in law enforcement's library and to view their contents by looking at the library copies. They also observed that the filenames contained terms strongly indicative of child pornography.[2]

The "Sparky's Engine" IP address was registered to Johnsen. Agents conducted a record check on Johnsen and learned that he was a sex offender with prior convictions for offenses involving minors. This led law enforcement to seek a warrant to search Johnsen's property. An agent affidavit in support of the application provided a detailed overview of the process used to match the hash values from Johnsen's eMule account to files in law enforcement's library. It explained that through this process, agents were able to "view the actual files, even though they had not been downloaded from the suspect IP address." The application listed four sample files which law enforcement had been able to view through hash matching and offered narrative descriptions of the sexually explicit content those files contained, as well as their filenames. The magistrate judge

[1] The record indicates various possible explanations for the agents' inability to download the files. For instance, law enforcement could have been placed at the end of a long download queue if multiple users were requesting to download the files.

[2] Agents testified to the commonality of certain terms used to identify and name files containing child pornography. For example, one agent testified that "PTHC" is used to indicate "preteen hardcore," and the use of the abbreviation "Yo" indicates "years old" (as in, "4Yo").

determined that the evidence presented in the application established probable cause and issued the warrant.

The search was executed shortly thereafter. Law enforcement officers seized 59 electronic devices from Johnsen's property, including multiple computers, hard drives, thumb drives, cell phones, and tablets. Before conducting any analysis of Johnsen's devices, agents created forensic copies that duplicated and preserved the devices' contents in the state they were in when seized, in a process known as "imaging." Imaging Johnsen's 59 devices took between one and two months.

Once imaging was complete, the agents used forensic software to process the devices, which involved organizing the stored material into an accessible format. This review encompassed not only saved files, but also any deleted files whose underlying data remained in unallocated space because it had not yet been overwritten. Analysis of the devices and their contents indicated that Johnsen was the sole user, and revealed that Johnsen's "Sparky's Engine" eMule account had been used to download tens of thousands of files containing child pornography. Across all of Johnsen's devices, agents viewed and confirmed the content of more than 140,000 images and over 900 videos depicting child pornography. The forensic examination of the devices took approximately eight months and culminated in a written report. Johnsen was subsequently indicted on one count of possession of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2); three counts of access to child pornography, in violation of 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2); and one count of receipt of child pornography, in violation of 18 U.S.C. §§ 2252(a)(2) and (b)(1).

Johnsen filed pre-trial motions to suppress the evidence obtained pursuant to the search warrant and to dismiss the indictment. The district court held hearings on these motions and ultimately denied both. On the final day of his three-day trial, Johnsen made an oral motion under Federal Rule of Criminal Procedure 29, arguing that the government had not presented sufficient evidence to support the charges. The court denied the motion, and Johnsen's trial concluded with the jury convicting Johnsen of all counts. Johnsen was sentenced to concurrent terms of 168 months' imprisonment on all counts, followed by a lifetime of supervised release.

II. Discussion

On appeal, Johnsen challenges the district court's rulings on all three motions.

A. The Motion to Suppress

Johnsen argues that the district court erred in denying his motion to suppress evidence obtained from the search of his home and devices because the warrant was not supported by probable cause. He further contends that law enforcement violated his Fourth Amendment rights as well as the Wiretap Act, 18 U.S.C. § 2511, by accessing his shared eMule files prior to obtaining the warrant. We review de novo the district court's denial of a motion to suppress. *See United States v. Yang*, 958 F.3d 851, 857 (9th Cir. 2020).

1. Probable Cause

We review for clear error whether the magistrate judge "had a substantial basis to conclude that the warrant was supported by probable cause." *United States v. Celestine*, 324 F.3d 1095, 1100 (9th Cir. 2003). A warrant is supported by probable cause if, based on the totality of the circumstances, the application establishes "a fair probability

that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238 (1983). In the context of child pornography, a "reasonable inference that [a suspect] had received or downloaded [such] images easily meets the 'fair probability' test." *United States v. Gourde*, 440 F.3d 1065, 1071 (9th Cir. 2006) (en banc).

The warrant to search Johnsen's property was issued based in part on evidence that Johnsen possessed files with hash values matching known child pornography. Johnsen contends that because officers had not downloaded and viewed any of the suspect files from his computer, it was improper for the magistrate judge to rely on the hash matches to find probable cause. We disagree. If we were to require visual confirmation of the contents of Johnsen's files to establish probable cause, it would effectively demand certainty that he possessed child pornography, rather than a fair probability.

A hash match between a suspect's files and known child pornography amply supports the reasonable inference that such material is present on the suspect's devices, even if agents have not downloaded and viewed the suspect file. Hash matching is widely viewed as a reliable and scientifically sound means of identifying duplicates of a file. *See* Kerr, *supra*, at 541; Salgado, *supra*, at 39–41. Johnsen does not challenge the reliability of the Government's hashing methodology and offers no rebuttal to the Government's assertion in the warrant application that "hash values are more reliable than DNA evidence." Though a hash match does not guarantee that the file on the suspect's device contains child pornography, the standard for probable cause is a "fair probability," not absolute certainty. *Gourde*, 440 F.3d at 1071. Hash evidence need not be unassailable

in order for a match to be highly probative that a file contains child pornography.[3]

Several other circuits have recognized that a hash match can support a finding of probable cause regardless of whether there was visual confirmation of the file's contents. *See, e.g.*, *United States v. Maher*, 120 F.4th 297, 322 (2d Cir. 2024) (noting that "the hash match of [an unviewed] image to one earlier identified . . . as depicting child pornography provide[s] strong probable cause" for a search warrant to view the file); *United States v. Miknevich*, 638 F.3d 178, 184 (3d Cir. 2011) (holding that the magistrate judge "could have drawn a reasonable inference of the file's contents based on its highly descriptive name and [hash] value"); *United States v. Cartier*, 543 F.3d 442, 446 (8th Cir. 2008) (affirming district court's holding that a search warrant which relied in part on hash matching without a visual inspection of the files did not lack probable cause); *United States v. Tolbert*, 92 F.4th 1265, 1278 (10th Cir. 2024) (observing that law enforcement could have obtained search warrants based on hash matching without visual inspection).

Moreover, the hash matches were bolstered by substantial additional evidence that independently supported the magistrate judge's finding of probable cause. Notably, the warrant application listed the filenames of files Johnsen's

[3] Johnsen also takes issue with the fact that the warrant application "failed to tell the Judge that the hash values were a very small fraction of the total number and size of files being downloaded." An officer presenting a search warrant application has a duty to provide, in good faith, all relevant information to the magistrate judge. *See United States v. Hill*, 459 F.3d 966, 971 n.6 (9th Cir. 2006). Information about Johnsen's legal downloads is wholly irrelevant to the question of whether he was likely to be in possession of child pornography. Accordingly, there was no reason for officers to include it.

eMule account was offering to share, all of which were strongly indicative of explicit sexual content involving minors. "[F]ilenames themselves, apart from their content" can give the magistrate judge "probable cause to issue a search warrant." *United States v. Borowy*, 577 F.Supp. 2d 1133, 1138 (D. Nev. 2008), *aff'd*, 595 F.3d 1045, 1049 (9th Cir. 2010) (affirming district court's holding that probable cause existed where filenames were "explicitly suggestive of child pornography"). Johnsen's filenames referenced the ages of the victims, included abbreviations for "preteen hardcore" or "pedophile," and one expressly referenced the specific sex act contained in the video. *See supra*, n.2. Those highly descriptive filenames were sufficient to support the inference that Johnsen's devices contained child pornography.

Finally, the warrant application also identified Johnsen as a registered sex offender with prior convictions for indecent liberties with a child and contributing to the delinquency of a minor. A suspect's criminal history "can be helpful in establishing probable cause, especially where the previous arrest or conviction involves a crime of the same general nature as the one the warrant is seeking to uncover." *United States v. Nora*, 765 F.3d 1049, 1059 (9th Cir. 2014) (quoting *Greenstreet v. County of San Bernardino*, 41 F.3d 1306, 1309 (9th Cir. 1994)). This cumulative evidence was more than sufficient to support a probable cause finding that Johnsen possessed child pornography.

2. Fourth Amendment and Wiretap Act

Johnsen's remaining two arguments—that law enforcement's review of his public eMule files violated his

Fourth Amendment rights as well as the Wiretap Act—are both squarely foreclosed by our precedents.

"[A] Fourth Amendment search does *not* occur . . . unless 'the individual manifested a subjective expectation of privacy in the object of the challenged search,' and 'society [is] willing to recognize that expectation as reasonable.'" *Kyllo v. United States*, 533 U.S. 27, 33 (2001) (quoting *California v. Ciraolo,* 476 U.S. 207, 211 (1986)). Individuals do not have a reasonable expectation of privacy in electronic files they offer for public download, and accessing files made available on a filesharing platform does not constitute a search. *See United States v. Ganoe*, 538 F.3d 1117, 1127 (9th Cir. 2008). "[W]hen an individual uses a filesharing software, he 'open[s] his computer to anyone else with the same freely available program,' thereby 'open[ing] up his download folder to the world.'" *United States v. Dreyer*, 804 F.3d 1266, 1278 n.6 (9th Cir. 2015) (en banc) (quoting *Ganoe*, 538 F.3d at 1127) (second and third alteration in original).

Law enforcement's pre-warrant review of Johnsen's files was limited to the materials that Johnsen made publicly available for download on the eMule filesharing platform. Their warrantless access to those public files did not violate Johnsen's Fourth Amendment rights.

For this same reason, Johnsen's argument that the "pre-search" violated the Wiretap Act fails. Standing to challenge wiretaps is limited "to persons whose Fourth Amendment rights were violated by the interception." *United States v. Gonzalez, Inc*., 412 F.3d 1102, 1116 (9th Cir. 2005) (citing *Alderman v. United States,* 394 U.S. 165, 175–76 & n.9 (1969)), *amended on denial of reh'g*, 437 F.3d 854 (9th Cir. 2006).

Furthermore, Johnsen's saved files do not fall within the scope of the Wiretap Act. The act bars the unauthorized, intentional "interception" of "electronic communications." 18 U.S.C. § 2511. "[T]o be 'intercepted' in violation of the Wiretap Act, [a communication] must be acquired during transmission, not while it is in electronic storage." *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878 (9th Cir. 2002) (footnote omitted). The Government's pre-search included only files that were described in the warrant application as being "possessed . . . in their entirety" by "[t]he suspect computer." These files were therefore not acquired during the process of transmission; they were fully downloaded and stored on Johnsen's computer.

Accordingly, Johnsen's Fourth Amendment and Wiretap Act arguments both fail.

B. The Motion to Dismiss the Indictment

Johnsen argues that the district court erred in denying his motion to dismiss the indictment because he was prejudiced when officers forensically analyzed his devices without his counsel present, and because he was wrongfully targeted for selective prosecution due to his prior conviction for offenses against children.[4] We review de novo the district court's

[4] Johnsen also argues that he was prejudiced by pre-indictment delay, which prevented him from (1) "tracking the IP addresses of other peer to peer file sharers"; (2) identifying the former owners of the computer equipment he allegedly purchased from his church community; (3) and reviewing footage from his surveillance cameras of agents serving the warrant. Showing actual prejudice from pre-indictment delay requires that the defendant present "definite and non-speculative evidence" that a loss of evidence "meaningfully impaired [his] ability to defend himself." *United States v. Mills*, 280 F.3d 915, 920 (9th Cir. 2002) (citation omitted). Johnsen does not provide "definite and non-speculative" proof that his defense was impaired by a loss of evidence, and his briefing fails

denial of a motion to dismiss an indictment. *See United States v. Haynes*, 216 F.3d 789, 796 (9th Cir. 2000).

1. Right to Counsel

Johnsen claims that his right to counsel was violated and he suffered prejudice when agents did not honor his request for an attorney to be present during the forensic analysis of his devices. But the right to counsel extends only to "critical stages" of the prosecution, and the forensic analysis of Johnsen's devices was not a "critical stage."

The Sixth Amendment ensures defendants "the right to have counsel present for all 'critical stages of the prosecution.'" *Beaty v. Stewart*, 303 F.3d 975, 991 (9th Cir. 2002) (quoting *United States v. Akins,* 276 F.3d 1141, 1146 (9th Cir. 2002)). A "critical stage" is characterized by "the adversary nature of the proceeding, combined with the possibility that a defendant will be prejudiced in some significant way by the absence of counsel." *United States v. Leonti*, 326 F.3d 1111, 1117 (9th Cir. 2003). Forensic analysis of the kind that occurred here does not fit this mold, because the accused is not present during the analysis and because cross-examination of forensic experts about their processes and techniques is available to mitigate any risk of prejudice.

An instructive distinction relating to the presence of the defendant has been drawn by the Supreme Court between police lineups, which are a critical stage, *see United States v. Wade*, 388 U.S. 218, 227–28 (1967), and photographic arrays, which are not, *see United States v. Ash*, 413 U.S. 300, 321 (1973). While the accused is not "confronted . . . with

---

to explain how his legal defense would have been strengthened by the evidence he identifies.

legal questions" during a lineup, the experience "offer[s] opportunities for prosecuting authorities to take advantage of the accused," which the presence of counsel may guard against. *Id.* at 312. In contrast, "the accused himself is not present at the time of the photographic display . . . [so] no possibility arises that [he] might be misled by his lack of familiarity with the law or overpowered by his professional adversary." *Id.* at 317.

Wade recognized the right to counsel during lineups, but it also explicitly differentiated lineups from "mere preparatory step[s] . . . such as systematized or scientific analyzing of the accused's fingerprints, blood sample, clothing, hair, and the like." 388 U.S. at 227. The Court explained that these forensic analyses were not critical steps because "[k]nowledge of the techniques of science and technology is sufficiently available, and the variables in techniques few enough, that the accused has the opportunity for a meaningful confrontation of the Government's case at trial through the ordinary processes of cross-examination of the Government's expert witnesses and the presentation of the evidence of his own experts." *Id* at 227–28.

Agents' forensic examination of Johnsen's devices was carried out through a standardized set of protocols conducted with dedicated software and was later memorialized in a written report. The process, which took approximately eight months, involved cataloguing and organizing files and data contained within the devices and then individually viewing more than 140,900 relevant files. It is unclear what role counsel could have meaningfully played in advising Johnsen during this highly technical analysis for which Johnsen himself was not present. Consistent with the principle expressed in *Wade*—that scientific analysis can be satisfactorily challenged at trial—the record here is replete

with cross-examination testimony from the investigating agents addressing the techniques, tools, and protocols that were used. Because the forensic analysis of Johnsen's devices was not a critical stage of the prosecution, Johnsen had no right to an attorney's presence during it.

2. Selective Prosecution

Johnsen claims that the Government was improperly motivated to prosecute him due to his prior convictions for crimes against children and that it pursued him while ignoring other similarly situated individuals. The standard of review that applies to claims of selective prosecution is unsettled. We have "employed both a de novo standard and a clearly erroneous standard when reviewing a selective prosecution claim." *United States v. Culliton*, 328 F.3d 1074, 1080 (9th Cir. 2003). Johnsen's arguments fail under either standard of review because he presents no evidence whatsoever that he received differential treatment or was targeted for prosecution due to an impermissible prosecutorial motive.

"In our criminal justice system, the Government retains 'broad discretion' as to whom to prosecute," *Wayte v. United States*, 470 U.S. 598, 607 (1985) (citations omitted), and "[m]ere selectivity in prosecution creates no constitutional problem," *United States v. Steele*, 461 F.2d 1148, 1151 (9th Cir. 1972). "To establish a prima facie case of selective prosecution, a defendant must show both (1) that others similarly situated have not been prosecuted, and (2) that the prosecution is based on an impermissible motive . . . ." *United States v. Davis*, 36 F.3d 1424, 1432 (9th Cir. 1994) (citation omitted). An impermissible motive is one in which "the decision whether to prosecute . . . [is] based on an unjustifiable standard such as race, religion, or other

arbitrary classification." *United States v. Armstrong*, 517 U.S. 456, 464 (1996) (quotation and citation omitted).

Johnsen shows neither similarly situated others, nor impermissible prosecutorial motive. He offers nothing more than his asserted belief that the Government has not pursued or prosecuted other eMule users who were involved in either sending or receiving his files. Without more, Johnsen cannot establish that there are similarly situated individuals whom the Government chose to ignore. He also fails to identify an impermissible motive, as "sex offenders do not comprise a suspect class." *Litmon v. Harris*, 768 F.3d 1237, 1244 (9th Cir. 2014). Because Johnsen cannot show either necessary prong to make out a selective prosecution claim, the district court was correct in denying his motion to dismiss his indictment on that basis.

C. The Motion for Judgment of Acquittal

Finally, Johnsen summarily asserts that the Government "failed to present sufficient evidence to sustain a conviction." "We review only issues which are argued specifically and distinctly in a party's opening brief," and "a bare assertion does not preserve a claim, particularly when . . . a host of other issues are presented for review." *Greenwood v. FAA*, 28 F.3d 971, 977 (9th Cir. 1994). Johnsen does not pinpoint any particular element of his conviction as being inadequately supported, nor does he offer any specific arguments or citations to the record to support his contention.

AFFIRMED.