**FOR PUBLICATION**

# UNITED STATES COURT OF APPEALS
# FOR THE NINTH CIRCUIT

| | |
|---|---|
| UNITED STATES OF AMERICA,<br><br>*Plaintiff-Appellee*,<br><br>v.<br><br>AARON GORDON HOLMES, Jr.,<br>AKA Aaron Gordon Holmes,<br><br>*Defendant-Appellant*. | No. 22-10266<br><br>D.C. No.<br>2:21-cr-00192-<br>SMB-1<br><br>OPINION |

Appeal from the United States District Court
for the District of Arizona
Susan M. Brnovich, District Judge, Presiding

Argued and Submitted December 5, 2023
San Francisco, California

Filed November 13, 2024

Before: Daniel P. Collins, Danielle J. Forrest, and Jennifer Sung, Circuit Judges.

Opinion by Judge Forrest;
Dissent by Judge Collins

## SUMMARY*

### Criminal Law

Holding: The panel reversed the district court's denial of Aaron Holmes's motion to suppress statements he made to law enforcement and images found on his cellphone, and remanded for further proceedings, in a case concerning a child-pornography investigation of two CyberTipline Reports that the National Center for Missing and Exploited Children (NCMEC) forwarded to the Federal Bureau of Investigation.

Investigating one of the tips, Special Agent Emily Steele viewed two images that NCMEC received from Facebook without a warrant. One of the images matched the digital identification of an image that was previously reported to NCMEC as depicting child exploitation. Viewing the images led Agent Steele to, among other things, obtain a search warrant for Holmes's residence. Holmes was present during the search, he made incriminating statements to law enforcement, and numerous illicit images were found on his cellphone. In his suppression motion, Holmes argued that this evidence was obtained because Agent Steele unlawfully viewed the Facebook images. The Government did not dispute that Agent Steele unlawfully viewed these images, but argued that suppression is unwarranted because two exceptions to the Fourth Amendment's warrant requirement apply: officer good faith and inevitable discovery.

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

The Government argued that suppression was unwarranted because Agent Steele relied in good faith on then-existing precedent when she opened and viewed the image files in the Facebook tip without a warrant. The panel held that the good-faith exception does not apply because the binding appellate precedent that existed when Agent Steele conducted her investigation was contradictory and only plausibly supported her warrantless viewing of the images received from Facebook.

The panel likewise rejected the Government's argument that the inevitable-discovery exception applies. The Government forfeited its arguments (1) that Agent Steele would have sought a warrant for Holmes's Facebook account even if she had not unlawfully viewed the Facebook images, and (2) that even if the reference to the unlawfully viewed Facebook images was excised from Agent Steele's affidavit seeking a warrant to search Holmes's Facebook account, the remaining information that she provided established probable cause to justify the warrant. As to the Government's preserved argument that Special Agent Candace Rose would have separately and lawfully obtained the same evidence through her parallel investigation of one of the tips, the panel concluded (1) whether Agent Rose would have obtained a warrant to search Holmes's residence requires impermissible speculation, and (2) even if Agent Rose inevitably would have obtained a search warrant for Holmes's residence, the Government failed to show that the evidence obtained by Agent Steele inevitably would have been found by Agent Rose.

Dissenting, Judge Collins wrote that the district court's analysis of the good-faith issue was in significant tension with its apparent acceptance of the Government's concession of a Fourth Amendment violation under *United*

*States v. Wilson*, 13 F.4th 961 (9th Cir. 2021). Judge Collins would resolve that tension by rejecting the Government's concession and holding that there was no violation of the Fourth Amendment that would warrant suppression. In his view, the FBI's search of one of the image files was lawful under both *United States v. Jacobsen*, 466 U.S. 109 (1984), as the district court held, and under *Wilson*. Because the warrant affidavit adequately established probable cause based on untainted evidence, he would affirm the denial of Holmes's motion to suppress.

---

## COUNSEL

Caitlin B. Noel (argued), Assistant United States Attorney; Krissa M. Lanham, Appellate Division Chief; Gary M. Restaino, United States Attorney, District of Arizona; United States Department of Justice, Office of the United States Attorney, Phoenix, Arizona; for Plaintiff-Appellee.

Elizabeth J. Kruschek (argued), Assistant Federal Public Defender; Jon M. Sands, Federal Public Defender; Federal Public Defender's Office, Phoenix, Arizona; for Defendant-Appellant.

## OPINION

FORREST, Circuit Judge:

This case concerns a child-pornography investigation of two CyberTipline Reports that the National Center for Missing and Exploited Children (NCMEC) forwarded to the Federal Bureau of Investigation (FBI). An agent investigating one of the tips viewed two images that NCMEC received from Facebook without a warrant. One of the images that the agent viewed matched the digital identification, known as a hash value, of an image that was previously reported to NCMEC as depicting child exploitation. Viewing the images led the agent to, among other things, obtain a search warrant for Defendant Aaron Holmes's residence. Holmes was present during the search, he made incriminating statements to law enforcement, and numerous illicit images were found on his cellphone. Holmes moved to suppress this evidence, arguing that it was obtained because the agent unlawfully viewed the Facebook images. The Government does not dispute that the agent unlawfully viewed these images, but it argues that suppression is unwarranted because two exceptions to the Fourth Amendment's warrant requirement apply: officer good faith and inevitable discovery. Because we conclude that the Government has not proven that either of these exceptions apply, we reverse the district court's denial of Holmes's motion to suppress.

## I. BACKGROUND

### A. Child Pornography Cybertips

Two child-pornography cybertips reported to NCMEC are at issue here. The first tip was made in September 2020

by Kik, an internet messaging provider. The tip reported that the pseudonymous account "mistersir456" sent several images that "match[] the hash value of an uploaded file from a CyberTipline report that was previously viewed and categorized by NCMEC" as "apparent child pornography."[1] Kik employees viewed each of the images included in its tip before sending it to NCMEC. Kik's tip included mistersir456's IP address, which was traced to Laveen, Arizona, and an associated email address: angel.l.espinoza05@gmail.com.

On October 22, 2020, FBI Special Agent Candace Rose began investigating the Kik tip and verified that several images included in the tip were child pornography. In early November, Agent Rose faxed an administrative subpoena to Gila River Telecommunications (Gila River), the internet

[1] Both FBI agents involved in this case testified that a hash-value match reliably establishes that the matched images are identical. The advisory notes to the 2017 amendments to Federal Rules of Evidence 902 explain that a hash value can self-authenticate electronic data:

> [D]ata copied from electronic devices, storage media, and electronic files are ordinarily authenticated by 'hash value.' A hash value is a number that is often represented as a sequence of characters and is produced by an algorithm based upon the digital contents of a drive, medium, or file. If the hash values for the original and copy are different, then the copy is not identical to the original. If the hash values for the original and copy are the same, it is highly improbable that the original and copy are not identical.

Fed. R. Evid. 902(14) advisory committee's note to 2017 amendment. Courts have equated hash-value matches to digital fingerprints or digital DNA. *See United States v. Miller*, 982 F.3d 412, 430 (6th Cir. 2020); *United States v. Ackerman*, 831 F.3d 1292, 1294 (10th Cir. 2016); *United States v. Wellman*, 663 F.3d 224, 226 n.2 (4th Cir. 2011).

service provider associated with the IP address that Kik provided. After the subpoena went unanswered for three months, Agent Rose faxed Gila River a second subpoena on February 3, 2021. Despite Gila River's initial failure to respond, Agent Rose marked the second request as "routine." Again, Gila River failed to respond.

NCMEC received the second tip from Facebook in January 2021. Facebook identified two images suspected of being child pornography that were sent by a user via Facebook Messenger. One of the images matched the hash value of "a previously reported child sexual exploitation image on NCMEC's NGO hash list." The second image did not have a hash-value match, but Facebook included it because it was sent by its user within a minute of the hash-value matched image. Facebook employees did not view the two images before sending the tip to NCMEC.

Facebook's tip included more information than Kik's. Facebook provided the image sender's IP address, the associated Facebook profile photo, the verified email address aaron.holmes93@yahoo.com, the account holder's date of birth and estimated age, the profile name "Aaron Sirsmokalot," and the screen name "aaron.holmes.351." Facebook also provided the same information for the image recipient, who was identified as username "tia.howard.946." Facebook classified the hash-matched image, using an industry classification standard, as A1: the category for depictions of a prepubescent minor engaged in a sex act. *United States v. Wilson*, 13 F.4th 961, 965 (9th Cir. 2021). Facebook also provided the text messages that were sent contemporaneously with the images:

> aaron.holmes.351: "What [if] we can train our daughter to handle that"

tia.howard.946: "Hell NO!"
aaron.holmes.351: "Ok"

Finally, Facebook's tip stated that the IP address used to send the images was located in Laveen, Arizona, and Gila River was identified as the internet service provider.

### B. Agent Steele's Investigation

Special Agent Emily Steele received the Facebook tip on February 3, 2021, and she opened both images that Facebook provided without obtaining a warrant. The images showed a clothed prepubescent girl on her knees with a white liquid substance on and around her mouth. The rest of the girl's face was obscured by a cartoon overlayed on the image. Adult feet were depicted in one of the images.[2] Agent Steele investigated the name Aaron Holmes and found an individual living in Laveen, Arizona with that name who had custody of a young girl who Agent Steele thought resembled the child in the images. With the information provided by Facebook, Agent Steele obtained Holmes's driver's license information and confirmed through school records that his daughter lived with him.

Based on the tip and the images that she viewed, Agent Steele obtained a search warrant for the aaron.holmes.351 Facebook account on February 8, 2021. In her supporting affidavit, Agent Steele included the user information provided by Facebook (*e.g.*, username, IP address, and date of birth), descriptions of the two images that she viewed, the accompanying text messages, and her belief that Holmes's

[2] Although one of the Facebook images matched the hash value of a "previously reported child sexual exploitation image" tracked by NCMEC, neither image was child pornography, as defined in 18 U.S.C. § 2256(2).

daughter resembled the girl in the two images. After executing the Facebook warrant, Agent Steele obtained multiple child pornography files sent by the aaron.holmes.351 account to the tia.howard.946 account.

Agent Steele called Gila River to determine the process for obtaining subpoenaed records "right away" "because of the exigency and the situation of potential child [abuse] and harm." Gila River advised that if Agent Steele sent an agent in person, it would provide information responsive to the subpoena the same day.

Agent Rose learned that Agent Steele was sending an agent to Gila River to deliver a subpoena. Agent Rose asked Agent Steele if this agent could also deliver Agent Rose's subpoena related to her investigation of the Kik tip, which had continued to go unanswered. The FBI received responses to both subpoenas on February 10, 2021, and Agents Steele and Rose discovered that their two investigations involved the same IP address. Agent Rose's investigation of the Kik tip was then reassigned to Agent Steele.

Agent Steele had already started preparing a search-warrant application for Holmes's residence. The residential address provided by Gila River matched the address that Agent Steele had obtained from Holmes's driver's license. Numerous people lived at the residence, including Holmes, his two minor daughters, his mother, his adult brother, his minor brother, his adult sister and her boyfriend, and his sister's two minor children. In her warrant application, Agent Steele identified the images obtained from the Facebook search, the subscriber information obtained from Gila River, and information obtained from police and vehicle records that connected Holmes to the residence. The

warrant was approved the day after the FBI obtained records from Gila River, and it was executed the day after that—February 12, 2021—just nine days after Agent Steele was assigned the Facebook tip.

Holmes was present at the residence when the search warrant was executed. Law enforcement seized numerous phones, computers, and other electronic devices. During the search, Holmes provided the password to his cellphone, on which law enforcement found hundreds of child pornography images—including the images from the Kik tip. Holmes also admitted that the "mistersir456" Kik account was his and that he shared child pornography with his cousin, Tia Howard, via Facebook. The Government charged Holmes on three counts: one count of distribution of child pornography for the Facebook images, one count of distribution of child pornography for the Kik images, and one count of possession of child pornography for the images found on his cellphone.

### C. Holmes's Motion to Suppress

Holmes moved to suppress the evidence obtained from the search of his Facebook account, as well as the evidence and his statements obtained during the search of his residence, which included his admission that the mistersir456 Kik account belonged to him, and the images from the Kik account that were found on his phone. He argued that Agent Steele's warrantless viewing of the images included in Facebook's NCMEC tip violated the Fourth Amendment, which tainted the rest of Agent Steele's investigation. He primarily relied on *Wilson*, 13 F.4th at 961, which was decided several months after Agent Steele viewed the Facebook images. In that case, Google learned that one of its users had attached to an email images that matched the

hash value of images Google had previously categorized as A1. *Id.* at 965. Google included the suspected child-pornography images in a cybertip report transmitted to NCMEC, but neither Google nor NCMEC viewed the images before they were forwarded to law enforcement. *Id.* at 964–66. After receiving the tip report from NCMEC, law enforcement viewed the images without a warrant. *Id.* at 966. We held that the warrantless viewing of the images violated the Fourth Amendment because law enforcement's inspection of the images exceeded the scope of Google's prior inspection. *Id.* at 971–72, 979–80.

The Government opposed Holmes's motion, arguing that the evidence obtained about Holmes should not be suppressed because Agent Steele relied in good faith on pre-*Wilson* precedent when she viewed the Facebook images without a warrant, and, alternatively, that Agent Rose inevitably would have discovered the same evidence that Agent Steele had discovered. Regarding inevitability, Agent Rose testified that absent Agent Steele's investigation, she "would have done the logical investigation into that residence [associated with the IP address] . . . [and] tried to determine who lived there, run criminal histories to try to see if there were any kids in the house, and prepare for and draft a residential search warrant."

The district court denied Holmes's motion to suppress. It concluded that the good-faith exception applied, but only as to Agent Steele's opening of the hash-value matched image received from Facebook. It also found that Agent Rose inevitably would have obtained the challenged evidence by following "routine procedures," such as "surveillance and database checks to identify residents of the home . . . , a search warrant for the residence, interviewing everyone at the home, forensic examination" and seizure of electronic

devices. Holmes pleaded guilty to count two (the Kik images) but reserved his right to appeal the suppression ruling.

## II. DISCUSSION

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. To satisfy the Fourth Amendment's "'ultimate touchstone of . . . reasonableness' . . . , law enforcement must generally obtain a warrant based on probable cause before conducting a search." *United States v. Anderson*, 101 F.4th 586, 591 (2024) (en banc) (quoting *Lange v. California*, 594 U.S. 295, 301 (2014)). But the "warrant requirement is subject to certain exceptions." *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006).

In this case, the Government concedes that Agent Steele's viewing of the Facebook images was a search that triggered the warrant requirement. However, the Government argues on appeal, as it did before the district court, that Agent Steele did not violate the Fourth Amendment because two exceptions to the warrant requirement apply: officer good faith and inevitable discovery. We review de novo the denial of a motion to suppress. *United States v. Vandergroen*, 964 F.3d 876, 879 (9th Cir. 2020). The district court's factual findings are reviewed for clear error. *Id.* Application of the good-faith exception is reviewed de novo. *United States v. Barnes*, 895 F.3d 1194, 1199 (9th Cir. 2018). The inevitable-discovery exception is a "mixed question of law and fact" that is "reviewed under a clearly erroneous standard." *United States v. Lang*, 149 F.3d 1044, 1047 (9th Cir. 1998), *amended by* 157 F.3d 1161 (9th Cir. 1998).

### A. Good-Faith Exception

The Government first argues that suppression of the evidence that Holmes challenges is unwarranted because Agent Steele relied in good faith on then-existing precedent when she opened and viewed the image files in the Facebook tip without a warrant. The good-faith exception excuses unlawful searches that are the "result of nonculpable, innocent police conduct." *Davis v. United States*, 564 U.S. 229, 240 (2011). Such circumstances exist when, for example, officers reasonably rely on the issuance of a warrant that is later held invalid, *United States v. Leon*, 468 U.S. 897, 922 (1984), or when officers rely on law that was binding at the time of their challenged conduct but later overturned, *Davis*, 564 U.S. at 239–40.

When law enforcement asserts that it acted in good faith by relying on then-existing law, it must point to "binding appellate precedent" that authorizes the challenged conduct at issue. *Id.* at 241. The good-faith exception does not require that the existing precedent involve a factual match to the present circumstances, but it does require that the precedent "specifically authorize[]" the conduct at issue. *United States v. Cano*, 934 F.3d 1002, 1021 (9th Cir. 2019) (quoting *United States v. Lara*, 815 F.3d 605, 613 (9th Cir. 2016)). As we explained in *Lara*, the good-faith exception applies "only when 'binding appellate precedent' expressly instruct[s] the officer what to do." 815 F.3d at 613. Good faith is not established where existing precedent is unclear or makes the government's position only "plausibly . . . permissible." *Cano*, 934 F.3d at 1021 (quoting *Lara*, 815 F.3d at 614).

The good-faith exception does not apply here because the existing precedent discussing the private-search doctrine did not specifically authorize Agent Steele to view the

Facebook images without a warrant. Rather, the legal landscape only made plausible the contention that Agent Steele's search fell within the scope of the private-search doctrine.

The Fourth Amendment restrains only government action; it does not apply where "a private party 'freely ma[kes] available' certain information for the government's inspection." *Wilson*, 13 F.4th at 968 (quoting *United States v. Jacobsen*, 466 U.S. 109, 119–20 (1984)). "Once frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now-nonprivate information." *Jacobsen*, 466 U.S. at 117; *see United States v. Tosti*, 733 F.3d 816, 821–22 (9th Cir. 2013). Where the government intrudes into an individual's privacy further than a private actor, the additional government intrusion is "tested by the degree to which [it] exceeded the scope of the private search." *Jacobsen*, 466 U.S. at 115. An additional intrusion that infringes no additional "legitimate expectation of privacy" does not violate the Fourth Amendment. *Id.* at 120.

Here, the Government argues that Agent Steele's warrantless viewing of the hash-matched image in the Facebook tip was specifically authorized by *Jacobsen*. In *Jacobsen*, FedEx employees followed their company policy and opened a damaged package. *Id.* at 111. The employees discovered a white powdery substance in the package. *Id.* They reported the substance to federal agents who reopened the package and tested the powder, discovering it was cocaine. *Id.* at 111–12. The Court upheld the agents' search under the private-search doctrine, recognizing that although the agents exceeded what the FedEx employees did by removing and testing some of the powder from the damaged package, these additional actions did "not compromise any

legitimate interest in privacy." *Id.* at 123, 126. "The field test at issue could disclose only one fact previously unknown to the agent—whether or not a suspicious white powder was cocaine." *Id.* at 122. The Court reasoned that a positive result intruded on no legitimate privacy interest because there is no legitimate "interest in 'privately' possessing cocaine," and a negative "result reveals nothing of special interest." *Id.* at 123.

We agree that *Jacobsen* provides a plausible justification for Agent Steele's actions. Some circuits have held that *Jacobsen* allows warrantless viewing of hash-value matched images. *See United States v. Miller*, 982 F.3d 412, 429–30 (6th Cir. 2020) (concluding that because hash values are "highly reliable" and "*Jacobsen* requires us to apply the p[rivate]-search doctrine if there is a 'virtual certainty'" hash values represent photos that were already viewed by private actors); *United States v. Reddick*, 900 F.3d 636, 639 (5th Cir. 2018) (stating the *Jacobsen* principle "readily applies here—opening the file merely confirmed that the flagged file was indeed child pornography"). But these out-of-circuit cases are not "binding appellate precedent." *Davis*, 564 U.S. at 241.

Moreover, while *Reddick* and *Miller* reached the same conclusion, they did not rely on the same reasoning. *Cano*, 934 F.3d at 1022 (rejecting application of the good-faith doctrine to "a rapidly developing area [that is] not an area of settled law"). *Reddick* first concluded that viewing images that matched the hash value of images previously identified as child pornography goes no further than a prior private search. *Reddick*, 900 F.3d at 639. Second, *Reddick* concluded that the detective's viewing was akin to the drug test analyzed in *Jacobsen* because "opening the file merely confirmed that the flagged file was indeed child

pornography" and law enforcement would learn nothing more than what was revealed in the private search. *Id.* at 639–40. *Miller* agreed with the first rationale but not the second. 982 F.3d at 429. It concluded that viewing a hash-value matched image was permissible because there was a "virtual certainty" that the image matched an image that had already been viewed by a private party—meaning a private actor already frustrated any privacy interest by causing a copy of the image to be hash valued. *Id.* at 429–30. But it concluded that viewing an image that matched the hash value of a previously viewed image *could* reveal significantly more private information than a drug test, which gives only a binary answer to whether the substance is an illegal drug. *Id.* at 429. The disparate reasoning in these out-of-circuit cases does not establish a settled rule on which Agent Steele could rely. *Cano*, 934 F.3d at 1022.

But more problematic to the Government's argument than the non-binding out-of-circuit authority is the Supreme Court's decision in *Walter v. United States*, 447 U.S. 649 (1980). In that case, a package of obscene films was misdelivered to the wrong company. *Id.* at 651. The recipient's employees opened the package and discovered film reels in packaging that suggested the films contained obscene content. *Id.* at 651–52. The employees alerted the FBI without watching the films. *Id.* at 652. FBI agents then watched the films, confirming that they were obscene without first obtaining a warrant or communicating with the package sender. *Id.* The Court held that the private-search doctrine did not apply in this context because viewing the films gave the FBI materially more information than what the private actors learned by looking only at the film packaging. *Id.* at 657. The Court reasoned that the packaging provided only "inferences about what was on the films" and

viewing the films "was a significant expansion of the search that had been conducted previously by a private party and therefore must be characterized as a separate search."[3] *Id.* at 657.

Some material aspects of this case are plausibly analogous to *Jacobsen* and others are plausibly analogous to *Walter*. *Reddick* and *Miller* discussed the analogies to the former. As for the latter, it was plausible to argue that in viewing the Facebook images, Agent Steele expanded on what law enforcement learned from the hash-value match. *See Walter*, 447 U.S. at 657. Before she viewed the images, she knew only that one of them matched the hash value of a "previously reported child sexual exploitation image" that Facebook categorized as depicting a "sex act" involving a prepubescent minor. No one at Facebook had viewed the images to confirm whether the images actually depicted child pornography or were otherwise unlawful (and in fact, neither image provided by Facebook was child pornography, as defined in 18 U.S.C. § 2256(2)). Thus, it is plausible to conclude under *Walter* that Holmes's privacy interest in the images was not extinguished by Facebook's conduct. And we adopted similar reasoning in *Wilson*, 13 F.4th at 976.

As far as we can tell, under our rule that binding appellate precedent must "specifically authorize" law enforcement's conduct, we have not applied the good-faith exception where there are contrasting, potentially dispositive precedents. Instead, we have taken a narrow view of when precedent specifically authorizes an action. *See Lara*, 815

[3] As we have previously noted, there is no clear majority opinion in *Walter*. One "majority of the justices concluded that there had been a violation of the Fourth Amendment, and a different majority of justices agreed on the standard to be applied." *Wilson*, 13 F.4th at 968–69.

F.3d at 613 ("We decline to expand the [good-faith exception] to cases in which the appellate precedent, rather than being binding, is (at best) unclear."). For instance, in *Cano*, notwithstanding precedent authorizing officials to conduct expansive searches at border crossings to locate contraband, we declined to apply the good-faith exception to border searches conducted for a different purpose—"proving [a] case against [a defendant] and finding evidence of future crimes." 934 F.3d at 1022 (emphasis omitted). We reached this conclusion even though law enforcement subjectively "thought that their actions were reasonable" based on the existing border-search precedent. *Id.*; *see also United States v. Lustig*, 830 F.3d 1075, 1080 (9th Cir. 2016) (stating good-faith reliance on precedent must be objectively reasonable).

Because the binding appellate precedent that existed when Agent Steele conducted her investigation was contradictory and only plausibly supported her warrantless viewing of the images received from Facebook, we conclude that the good-faith exception does not apply. When it is ambiguous where an officer's conduct falls on the continuum of what is lawful and what is not, our precedent requires that law enforcement comply with the warrant requirement. *Cano*, 934 F.3d at 1021.

### B. Inevitable-Discovery Exception

The Government also argues that the inevitable-discovery exception applies. The inevitable-discovery exception excuses warrantless searches where the government proves "by a preponderance of the evidence" that unlawfully obtained evidence "would have been discovered inevitably [through] lawful means." *United States v. Andrade*, 784 F.2d 1431, 1433 (9th Cir. 1986).

Inevitability is the key. There can be "no speculative elements" in showing that law enforcement would have obtained the evidence lawfully absent its unlawful actions. *Lang*, 149 F.3d at 1047 (quoting *Nix v. Williams*, 467 U.S. 431, 444 n.5 (1984)). Rather, this inquiry must "focus[] on demonstrated historical facts capable of ready verification or impeachment." *Nix*, 467 U.S. at 444 n.5. We have also explained that "the fact or likelihood that makes the discovery inevitable [must] arise from circumstances other than those disclosed by the illegal search itself." *United States v. Boatwright*, 822 F.2d 862, 864 (9th Cir. 1987).

*Nix* illustrates inevitability. There, the Court considered whether a 200-person search party would have found a body without the evidence obtained from an illegal interrogation that ultimately led law enforcement to the body. *Nix*, 467 U.S. at 441, 448. The specific issue was whether independent "search efforts would have proceeded two and one-half miles into [the adjacent] Polk County." *Id.* at 448. Officers had obtained maps of three counties—Poweshiek, Jasper, and Polk. *Id.* at 448–49. Volunteers were organized into small teams and were instructed to search roads, ditches, and culverts. *Id.* The search started in Poweshiek County, and officers divided the map in a grid fashion, assigning each volunteer team to a specific grid. *Id.* at 449. The search began at 10 a.m., and after several hours, it moved into Jasper County. *Id.* The search, however, was halted around 3:00 p.m. when it became apparent that the suspect would lead the police to the body. *Id.*

The Court held that the inevitable-discovery exception applied because the record demonstrated that searching Polk County was the inevitable next step—officers already had the map of the county—and the search teams would have searched Polk County in the same manner as the two prior

counties. *Id.* at 449–50. The body was also in the search path and near a culvert—where volunteers were "specifically directed to search." *Id.* at 449. And the record showed that the search was "approaching" the area where the body was and would have reached its location within three to five hours. *Id.*

Our decision in *United States v. Martinez-Gallegos*, 807 F.2d 868 (9th Cir. 1987), is also instructive. There, immigration agents unlawfully questioned the defendant about his immigration status. *Id.* at 869. Based on the information they obtained, the agents pulled the defendant's Alien or "A" File, which contained information about his previous deportations, and the defendant was charged under federal law. *Id.* at 869–70. We held that even without the unlawful questioning, the agents inevitably would have consulted the A File. *Id.* at 870. The immigration agents knew the defendant's name because he had previously identified himself to state authorities, and if the immigration agents had not questioned the defendant, their "next step, indeed the only step available to them, would have been to consult his 'A' file." *Id.* Like the body in *Nix*, the A File was not going anywhere, it was "readily retrievable," and its discovery was imminently looming. *Id.*

Contrast these cases with *United States v. Ramirez-Sandoval*, 872 F.2d 1392 (9th Cir. 1989). There, a police officer lawfully stopped a van based on reasonable suspicion that the occupants were involved in illegal narcotic transactions. *Id.* at 1393–95. Seeking evidence of narcotics activity, the officer noticed the sun visor was hanging low on the driver's side. *Id.* at 1394. The officer then, without a lawful basis, touched the sun visor and retrieved a piece of paper with a list of names and numbers on it that fell to the floor. *Id.* The officer read one of the names from the list out

loud and an occupant of the van responded. *Id.* The officer asked the occupant what the number next to his name meant, and the occupant responded that it was the amount of money he had paid to be smuggled into the United States. *Id.* What began as a lawful stop resulted in an illegal search. *Id.* at 1395. The defendant moved to suppress the incriminating statements made after the illegal search, and the government argued the inevitable-discovery exception. *Id.* at 1395–96. We held that this exception did not apply because there were no historical facts to prove that the officer would have asked the same questions and elicited the same information from the van's occupants in the absence of the unlawful search revealing the list of names. *Id.* at 1400. While the officer was "entitled to ask the van's occupants who they were and what they were doing," this did not prove inevitability where the officer "had a great deal of discretion in choosing to ask or not ask certain questions." *Id.*; *see also United States v. Young*, 573 F.3d 711, 723 (9th Cir. 2009) (finding the government did not show inevitable discovery when the evidence relied on speculation and indicated there was more than one plausible outcome).

As the caselaw demonstrates, whether "historical facts" establish that lawful discovery of the evidence was inevitable is a case-specific inquiry. *United States v. Ruckes*, 586 F.3d 713, 719 (9th Cir. 2009). The Government asserts here that the FBI's "routine procedures" prove that the images seized from Holmes's Facebook account, Kik account, and cellphone inevitably would have been found lawfully. In assessing this argument, we must determine what "would have necessarily followed" if Agent Steele had not viewed the Facebook images. *Id. Ruckes* demonstrates the required analysis. There, a state trooper discovered that the defendant was driving without a valid license and then

illegally searched the vehicle. *Id.* at 715–16, 718. Before the search, the trooper explained that the vehicle would be impounded if no one was available to pick it up. *Id.* at 716. Although the trooper had some discretion regarding whether to impound the vehicle, the record established that impoundment was "standard procedure" because no one was available to pick up the defendant's vehicle. *Id.* at 719. Thus, we concluded that an inventory search, which would have uncovered the same evidence that was obtained illegally, was inevitable. *Id.*; *see also Andrade*, 784 F.2d at 1433 (holding the inevitable-discovery exception applied where "routine booking procedure and inventory would have inevitably resulted in discovery of the cocaine").

Where the hypothetical next steps of an investigation are more discretionary and less procedural, inevitability may be lacking. *See United States v. Ramirez-Sandoval*, 872 F.2d 1392, 1400 (9th Cir. 1989). This is logical—the more leeway for decision-making, the harder it is to conclude, without speculation, that law enforcement *inevitably* would reach the same outcome. *See id.* (reversing a district court's inevitability conclusion based on assumptions that did not provide "any certainty" to an officer's discretionary choices). With these principles in mind, we turn to the facts of this case.

**1. Agent Steele**

The Government argues that Agent Steele would have sought a search warrant for Holmes's Facebook account even if she had not unlawfully viewed the Facebook images. It also argues that even if the reference to the unlawfully viewed Facebook images was excised from Agent Steele's affidavit seeking a warrant to search Holmes's Facebook account, the remaining information that she provided

established probable cause to justify the warrant. *See United States v. Nora*, 765 F.3d 1049, 1058 (9th Cir. 2014) ("A search warrant isn't rendered invalid merely because some of the evidence included in the affidavit is tainted."). The problem with these arguments is the Government did not make them to the district court. At no point previously did the Government argue inevitable discovery as it relates to Agent Steele. Therefore, these arguments were forfeited. *See Lara*, 815 F.3d at 613 ("The government did not make this argument in the district court, and consequently it has failed to preserve this argument on appeal.").

**2. Agent Rose**

The Government did preserve an inevitable-discovery argument related to Agent Rose. The Government argues that regardless of Agent Steele's unlawful conduct, Agent Rose would have separately and lawfully obtained the same evidence from Holmes and his cellphone through her parallel investigation of the Kik tip. In other words, Agent Rose would have obtained the same evidence even if "the Facebook [tip] had never have taken place." The district court accepted this argument, concluding that "by following routine procedures, Agent Rose would have inevitably ended up with the same evidence." This was clear error because the Government failed to demonstrate through historical facts that the "routine procedure" it relies on—Agent Rose's investigation process—was sufficiently predictable to establish that she inevitably would have located the same evidence as Agent Steele. This is particularly true because facts material to finding inevitability "were inadequately developed." *Nix*, 467 U.S. at 450.

The district court concluded that Agent Rose would have found the same evidence because she would have conducted

"surveillance and database checks to identify residents of the home . . . , [obtained] a search warrant for the residence, interview[ed] everyone at the home," conducted "forensic examination during the search to preview devices, and seiz[ed] . . . devices for forensic examination back at the FBI." This reasoning is based on two assumptions that are not supported by "demonstrated historical facts capable of ready verification or impeachment." *Id.* at 444 n.5. The first assumption is that Agent Rose's investigation would proceed "in the exact same manner" as Agent Steele's investigation. And the second assumption is that the evidence at issue would have been available to Agent Rose the same as it was to Agent Steele.

**a. Inevitability of Agent Rose's Investigation Process**

The Government argues that Agent Rose inevitably would have obtained a search warrant for Holmes's residence, just as Agent Steele did. The Government has not identified any routine procedure or practice that supports its argument. Rather, it relies on Agent Rose's testimony that she would have sought a search warrant for the residence.

As an initial matter, in determining whether Agent Rose's investigation would have proceeded the same as Agent Steele's, we must consider where Agent Rose began. The Kik tip that she was assigned included significantly less information than the Facebook tip. Even after Agent Rose received information about the IP address that Kik provided, she would not have known Holmes's identity.[4] The only

[4] Agent Steele could identify Holmes from the initial Facebook tip because it included his eponymous username and email address, his Facebook profile photo, and his date of birth.

identifying information that Kik provided was the account username and associated email address, neither of which identified Holmes. Likewise, the subscriber information that Gila River provided identified three customer names and associated email addresses, but none of them were Holmes's. Agent Rose did not seek information from Google about the angel.l.espinoza05@gmail.com account,[5] nor did she request information from Kik about its mistersir456 account.

At the first step of Agent Rose's hypothetical investigation as described by the district court—investigation and surveillance of the residence—nothing establishes that Agent Rose would have linked Holmes to the Kik account through the residence because five adults lived there. And we can only speculate when Agent Rose may have obtained and executed a search warrant for the residence. Even though the FBI received the Kik tip first, Agent Rose seemingly was still in the initial stage of investigation when she passed the case off to Agent Steele. She had reviewed the cybertip, including information about the IP address from which the mistersir456 account was repeatedly accessed, and she had subpoenaed customer information for the IP address from Gila River. But her subpoenas went unanswered for over three months, and she only got a response when Agent Steele had the subpoenas for both investigations presented in person. There is no indication in the record as to when Agent Rose would have received a response had Agent Steele's parallel investigation of the Facebook tip not happened.

[5] Unlike the Facebook email address, the email associated with the Kik account was unverified. When an individual registers an account with Kik, the company sends an email to the email address used to register the account to "verify" it is the individual's email address.

The timing of an asserted hypothetical lawful discovery may inform inevitability. The caselaw demonstrates that shorter periods between the unlawful conduct and the asserted lawful discovery that would have occurred typically increases the likelihood of inevitability. For example, the *Nix* Court noted that inevitable discovery of the body was only "an additional three to five hours" away given the search party's methodology. 467 U.S. at 449. In *United States v. Hylton*, we noted that absent illegal police conduct, officers "would have discovered that [defendant] was a felon [in possession of a gun] only two minutes later." 30 F.4th 842, 848 (9th Cir. 2022), *cert. denied*, 143 S. Ct. 393 (2022). And other examples show that inevitable discovery of the subject evidence would occur on the same day or in other close proximity to the unlawful conduct. *See, e.g.*, *United States v. Ramirez*, 473 F.3d 1026, 1031 (9th Cir. 2007) (discussing the inevitable discovery of narcotics that would have occurred "shortly after" the improper police conduct).

The Government points to Agent Steele's actions to demonstrate how Agent Rose would have conducted her investigation. This comparison is not persuasive because these two agents were not equally positioned or motivated. Agent Steele acted quickly after discovering Holmes's identity, the direct link between him and illicit content, and that he had custody of a young girl that Agent Steele suspected was the girl in the images that she viewed. Agent Rose had none of that troubling information suggesting the possibility of ongoing child endangerment, and we cannot assume she would have conducted her investigation "in the exact same manner" as Agent Steele.

Indeed, the historical facts suggest the opposite. Agent Rose had not acted with urgency before she handed her investigation over to Agent Steele, instead allowing her

"routine" Gila River subpoena to go unanswered for months with minimal, and ineffectual, follow-up. Although there is no precise timing requirement to establish inevitability, we are reluctant to conclude that Agent Rose's passive investigation was destined to yield the same results as Agent Steele's intensive efforts. *Cf. Hylton*, 30 F.4th at 848 (considering timing of subsequent discovery); *United States v. Lundin*, 47 F. Supp. 3d 1003, 1021 (N.D. Cal. 2014), *aff'd* 817 F.3d 1151 (9th Cir. 2016) ("The government has failed to show that, at a minimum, the guns would have been present in the home or backyard *the next day*. . . ." (emphasis added)).

A further problem with the Government's reliance on Agent Rose's assertion that she would have obtained a search warrant for Holmes's residence is Agent Rose's testimony that she does not pursue all the warrants that she can because she has a high caseload. Indeed, *in this case* it seems that Agent Rose did not pursue all the leads and warrants that she could have. Agent Rose explained that she had "seen a couple hundred CyberTips" and had opened "full investigations" into only "maybe 40" of them. The Government did not present any information about what the 40 fully investigated tips involved and why they triggered a thorough inquiry when the others did not; this information might have provided historical facts relevant to assessing whether this case is more like the 40 fully investigated tips or the approximately 160 tips that were not fully investigated.

For these reasons, we conclude that whether Agent Rose would have obtained a warrant to search Holmes's residence requires impermissible speculation.

### b. Inevitability of the Search Results

The next step in the inevitability analysis is even more fatal for the Government. Even if we accept that Agent Rose inevitably would have obtained a search warrant for Holmes's residence, the Government must also show that the evidence unlawfully obtained by Agent Steele inevitably *would have been found* by Agent Rose. The Government failed to make this showing because there are no historical facts to prove with any certainty that this would have happened.

As an initial matter, with no evidence singling out Holmes from the five adults living at the residence, any warrant obtained by Agent Rose necessarily would have been issued on different terms than Agent Steele's warrant. *Cf. Ramirez-Sandoval*, 872 F.2d at 1400 (rejecting inevitability where the officer's investigation—specifically, questioning—would change absent information obtained from an illegal search). Agent Steele had cause to investigate Holmes specifically, and the terms of her warrant included authority to search his "person." Agent Rose would not have had reason to seek search authority specific to Holmes.

Additionally, law enforcement officers discovered the evidence at issue (cellphone images and oral statements) because Holmes was present when the officers executed the warrant. Thus, to prove that Agent Rose would have obtained the same evidence that Agent Steele did, the Government needed to show that Holmes inevitably would have been present during the execution of Agent Rose's hypothetical search warrant. The Government did not make that showing, and it is "most unrealistic" to expect that if Holmes had learned of a search conducted in his absence, he would have passively submitted to investigation.

*Boatwright*, 822 F.2d at 865 (noting that a suspect once alerted to a search "would not have waited patiently beside his [contraband] for an agent to arrive with a warrant"); *see also United States v. Bradford*, 772 F. App'x 554, 555 (9th Cir. 2019) (holding inevitability did not exist where the government presented "no evidence that [defendant] would have remained detained during the entirety of the dog search, such that the weapon would inevitably have been in his possession when a later search incident to arrest occurred").

In some contexts, there is little speculation that evidence unlawfully seized would be found in a subsequent search regardless of whether the defendant was present during the search. *Nix* is a good example because there, the dead body was unlikely to move. 467 U.S. at 446–47. Similarly, in *Ruckes*, police would have maintained control of the impounded vehicle containing the evidence at issue until an inventory search was conducted. 583 F.3d at 719. Access to the vehicle and its contents did not depend on the defendant's presence. *Id.* But inevitability of the fruits of a hypothetical search is less clear where the items at issue are easily moved and law enforcement does not have control over them. For example, in *Lundin*, the district court concluded that the inevitable-discovery exception did not apply where there was a "chance other people could have entered the home and moved the guns prior to any later legal search." 47 F. Supp. 3d at 1021–22; *see also Young*, 573 F.3d at 722 (noting how a gun could easily move in a hypothetical chain of events).

Here, if the illicit images had come from a desktop computer or some other less-mobile device in the residence, the analysis might be different. But where the images at issue

were found on Holmes's cellphone,[6] his presence during the search is necessary because there is no suggestion that Holmes left his cellphone at home rather than carrying it on his person.[7] And while Agent Rose testified that she would have seized and searched any phone "of interest" in the residence, it is not clear that Holmes's phone would have been "of interest" had he not been present given that the investigation did not point to him specifically.

The Government must prove that discovery of the evidence by lawful means was inevitable by a preponderance of the evidence. *Nix*, 467 U.S. at 444. This burden is not met when the Government relies on unsupported assumptions to fill in the gaps of an undeveloped record. And here, the Government's attempt to characterize Agent Rose's investigation as a "routine procedure" that inevitably would have led agents to find the illicit images on Holmes's social media accounts and cellphone simply is not supported by the record. This purported "routine procedure" is also of a different character than other procedures that we have held demonstrate inevitability. *See Nix*, 467 U.S. at 449; *Andrade*, 784 F.2d at 1433; *Hylton*, 30 F.4th at 848. Agents exercise discretion in how they conduct their investigations. This is evident from the differences between Agent Rose's and Agent Steele's investigations and Agent Rose's testimony

[6] Agents found several images on Holmes's cellphone that matched images from the Kik tip and "artifacts" that included screenshots of Facebook messages. But Agent Rose testified that "[t]here was no evidence that Kik was on the phone the day that it was seized."

[7] There were numerous cellphones found in the residence, but Holmes stated during interrogation that "the only electronic devices he has or uses are his cell phone and his Xbox." Cellphone singular, not *cellphones*.

that she did not fully investigate every child-pornography cybertip.

For all these reasons, we conclude that that the good-faith and inevitable-discovery exceptions to the warrant requirement do not apply. The district court's denial of Holmes's motion to suppress is reversed and the case is remanded for further proceedings.

**REVERSED and REMANDED**.

---

COLLINS, Circuit Judge, dissenting:

In ruling on Holmes's motion to suppress, the district court did not directly question the Government's concession that, under this court's decision in *United States v. Wilson*, 13 F.4th 961 (9th Cir. 2021), Agent Steele engaged in an unlawful warrantless search in violation of the Fourth Amendment by examining the two image files forwarded to her by the National Center for Missing and Exploited Children ("NCMEC") from Facebook. The district court instead purported to rely only on the inevitable-discovery doctrine and (partially) on the good-faith exception. However, as I shall explain, the district court's reasoning as to the good-faith exception actually appears to rest on a substantive conclusion that one aspect of the search did *not* violate the Fourth Amendment, but the district court did not explain how that conclusion was consistent with *Wilson*. The court's analysis of the good-faith issue was thus in significant tension with its apparent acceptance of the Government's concession of a Fourth Amendment violation. I would resolve that tension by rejecting the Government's concession and holding that there was no violation of the

Fourth Amendment that would warrant suppression here. I therefore respectfully dissent.

With respect to the issue of good faith, the district court noted that the exception to the exclusionary rule for good-faith reliance on then-existing precedent "applies only when the officials have relied on '*binding* appellate precedent'" that "specifically authorize[s]" the search at issue. *United States v. Cano*, 934 F.3d 1002, 1022 (9th Cir. 2019) (citation omitted); *id*. at 1021–22 (stating that the applicable law must be "settled" and that it is not sufficient that the search was "plausibly permissible" under then-applicable law (simplified)). That high standard traces back to *Davis v. United States*, 564 U.S. 229 (2011), which held that the good-faith exception applies "when the police conduct a search in compliance with binding precedent *that is later overruled*." *Id*. at 232 (emphasis added). That distinctive situation is one in which a search can simultaneously be thought to be unlawful (under current law) but objectively reasonable when conducted (under then-applicable law that has since been abrogated).

Here, however, the district court held that the FBI's search of one of the image files in question was specifically authorized by binding appellate precedent that *remains* binding, namely, *United States v. Jacobsen*, 466 U.S. 109 (1984). Because *Jacobsen* is still controlling precedent, the district court's conclusion that it specifically authorized the examination of one image is merely another way of saying that that search was in fact *lawful*. But that conclusion seems in tension with the district court's implicit assumption that, under our subsequent decision in *Wilson* (which construed and applied *Jacobsen*), the search was unlawful. If one takes the latter assumption seriously, then the district court's ruling would seem unavoidably to rest on the premise that

the good-faith exception should apply here because *Wilson*'s interpretation of *Jacobsen* was wholly unexpected, if not wrong altogether. I am aware of no authority that would allow a district court (or a three-judge panel of this court) to extend the good-faith exception to situations in which it thinks that post-search circuit precedent has misconstrued pre-search Supreme Court precedent.

However, given that the district court effectively held that the relevant search was lawful under *Jacobsen*, I think it is appropriate to address whether that conclusion was correct and whether (despite the Government's concession and the district court's assumption) it was in fact inconsistent with *Wilson*. In my view, the search of the one image in question was lawful under both *Jacobsen* and *Wilson*.

As we explained in *Wilson*, under the "private search doctrine," an "antecedent private search excuses the government from obtaining a warrant to repeat the search but only when the government search does not exceed the scope of the private one." *Wilson*, 13 F.4th at 968. Under this doctrine, "[t]he additional invasions of [the defendant's] privacy by the government agent must be tested by the degree to which they exceeded the scope of the private search." *Id*. (quoting *Jacobsen*, 466 U.S. at 115). "The Fourth Amendment is implicated only if the authorities use information with respect to which the expectation of privacy has not already been frustrated." *Jacobsen*, 466 U.S. at 117. That is, "[o]nce frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now-nonprivate information." *Wilson*, 13 F.4th at 970 (quoting *Jacobsen*, 466 U.S. at 117). Here, any expectation of privacy in the relevant image was already "fully frustrated" when Facebook sent its cybertip to NCMEC, and the Fourth Amendment was therefore not

implicated when Agent Steele examined that file after receiving it from NCMEC. *Id*. at 974.

In its tip to NCMEC, Facebook reproduced the content of the messages between Holmes and another person concerning the image in question, and Facebook uploaded an electronic copy of that image. Facebook also disclosed that, based on its use of "hashing" technology, it had determined that the uploaded image "was identified as a match to a previously reported child sexual exploitation image on NCMEC's NGO hash list." Facebook also supplied the relevant hash value for the file. NCMEC maintains a database that includes both "the actual files that they can run for visual matches" and "the database of hash values for the files." Thus, as soon as NCMEC received Facebook's tip, it objectively had all the information needed to identify *exactly* the actual specific image that Holmes had sent, without the need to examine the uploaded file. To use an analogy, what Facebook did was akin to enclosing a book in a sealed envelope and submitting it to the Library of Congress with a statement that the enclosed book corresponds to a specific Library of Congress classification number; by consulting its own collection, the Library would be able to know exactly what the contents of the book are, even without breaking the seal. Because NCMEC qualifies as a governmental actor for Fourth Amendment purposes, *see United States v. Ackerman*, 831 F.3d 1292, 1296 (10th Cir. 2016); *see also United States v. Rosenow*, 50 F.4th 715, 729 n.3 (9th Cir. 2022) (reserving the issue, but noting that "[t]here is good reason to think that the NCMEC is, on the face of its authorizing statutes, a governmental entity under Fourth Amendment doctrine"), Facebook's submission effectively disclosed the precise contents of the file to the Government, without any need to open the uploaded image

file. Consequently, any "expectation of privacy" in that image had "already been frustrated." *Jacobsen*, 466 U.S. at 117.

We reached a contrary conclusion on the facts in *Wilson*, but those facts are distinguishable in a way that makes a critical difference here. In *Wilson*, Luke Wilson "had uploaded four images . . . to his email account as email attachments," which Google's hashing technology identified as "the same as images other Google employees had earlier viewed and classified as child pornography." 13 F.4th at 964. However, "[n]o one at Google had opened or viewed Wilson's email attachments." *Id*. Moreover, because "Google does not keep a repository of child pornography images, . . . no Google employee could have shown the government the images it believed to match Wilson's." *Id*. at 972. "All Google communicated to NCMEC in its CyberTip was that the four images Wilson uploaded to his email account matched images previously identified by some Google employee at some time in the past as child pornography and classified as depicting a sex act involving a prepubescent minor." *Id*. Thus, when an FBI agent subsequently reviewed the images without a warrant, he "substantively expanded the information available to law enforcement far beyond what the label alone conveyed." *Id*. at 973. That, we concluded, made Wilson's case comparable to *Walter v. United States*, 447 U.S. 649 (1980), in which a majority of the Court held that FBI agents violated the Fourth Amendment by viewing films that had been handed over to them by private citizens to whom the films had been mistakenly delivered. *Wilson*, 13 F.4th at 973. Although the films' packaging had labeling that "suggested that the images on the films were obscene," they did not disclose the actual specific contents of the films. *Id*.; *see also Walter*,

447 U.S. at 657 (plurality) (noting that, "[p]rior to the Government screening, one could only draw inferences about what was on the films"). We therefore concluded in *Wilson* that "the content of the images was no more apparent to Google than the image content was to the private party in *Walter*, as no Google employee had opened and viewed the attachments, and Google does not appear to retain any record of the original images used to generate hash matches." *Wilson*, 13 F.4th at 974 (simplified).

The facts of this case are significantly different. Here, unlike in *Wilson*, the record confirms that NCMEC does retain a database with the actual images that match the hash values for its "hash list." The "information available to law enforcement" from the facts contained in Facebook's tip here thus effectively disclosed the *precise* contents of the image that Holmes had emailed. *Wilson*, 13 F.4th at 973. As a result, the subsequent viewing of the image file that Facebook had uploaded did not "substantively expand[] the information *available* to law enforcement." *Id*. (emphasis added). Regardless of whether NCMEC examined its file copy of the image, the contents of Holmes's image had been fully disclosed by Facebook to NCMEC, as an objective matter, and any expectation of privacy thus had already been "fully frustrated." *Id*. at 974. That is, Facebook's hashing technology had already "searched" the actual contents of the file and learned what the corresponding hash value was, and Facebook then disclosed that to NCMEC with an explicit statement that the hash value was an exact match for an image that was already contained in NCMEC's database. Although the particular *means* by which Agent Steele conducted her search of the contents (visual viewing) differed from the means that Facebook used in its private search of those exact same contents (electronic screening),

the result is that Agent Steele's search did not, in any meaningful respect, "exceed[] the scope of the private search." *Jacobsen*, 466 U.S. at 115. Agent Steele's examination of this image therefore did not "implicate[]" the Fourth Amendment, and the fruits of that examination were properly contained in Agent Steele's search warrant affidavit. *Id*. at 117.

By contrast, as the district court recognized, Agent Steele's examination of the *other* image submitted by Facebook—which did not have an associated hash-value match—violated the Fourth Amendment under *Jacobsen* (and *Wilson*). But given that the second image was so similar to the first, and included *less* information,[1] its inclusion did not add anything to the probable cause already established by the remaining facts in the warrant affidavit. *See United States v. Nora*, 765 F.3d 1049, 1058 (9th Cir. 2014) (stating that a "warrant remains valid if, after excising the tainted evidence, the affidavit's 'remaining untainted evidence would provide a neutral magistrate with probable cause to issue a warrant'" (citation omitted)). Because the warrant affidavit adequately established probable cause

[1] The descriptions in the affidavit state that the two images "are extremely similar in that they appear to have been taken on the same date, with the same background details," and "depict[] the same minor female girl." They both thus apparently disclose the same disturbing evidence of the same incident of child sexual exploitation, even if the images did not themselves fit the actual definition of child pornography under federal law. The only material difference noted in the affidavit between the two images is that the one *without* a hash-value match contained "a cartoon image of hands and a heart" that partially obscured the child's face. The affidavit's description of the child depicted (which formed the basis for the affidavit's assertion that the child resembled an 8-year-old as to whom Holmes had custody) thus came from the image *with* a hash-value match.

based on untainted evidence, suppression of the evidence obtained thereby is unwarranted. On that basis, I would affirm the district court's denial of Holmes's motion to suppress. *See United States v. Holzman*, 871 F.2d 1496, 1512 (9th Cir. 1989) (stating that a denial of a motion to suppress may be affirmed "on any ground finding support in the record" (citation omitted)).

I respectfully dissent.