CRIMINAL PROCEDURE — FOURTH AMENDMENT — NINTH CIRCUIT HOLDS THAT OFFICER'S WARRANTLESS REVIEW OF IMAGES FLAGGED BY GOOGLE AS APPARENT CHILD SEXUAL ABUSE MATERIAL VIOLATED FOURTH AMENDMENT. — *United States v. Wilson*, 13 F.4th 961 (9th Cir. 2021).

The rise of digital media has unleashed a flood of Child Sexual Abuse Material (CSAM) across the internet, and with it, the horrible shame and vulnerability that haunt survivors of such abuse.[1] In 2008, President Bush signed the PROTECT Our Children Act of 2008[2] (PROTECT Act) to enlist large technology companies in the fight against CSAM.[3] The law requires "electronic communication service provider[s and] remote computing service providers"[4] to notify the National Center for Missing and Exploited Children (NCMEC) when they discover "apparent violation[s]" of laws prohibiting CSAM.[5] Some electronic communication service providers have responded by actively screening content on their platforms for CSAM.[6] But as service providers have started to help law enforcement search for CSAM, courts have struggled to apply Fourth Amendment doctrines that were developed in physical search cases to digital contexts.[7] Recently, in *United States v. Wilson*,[8] the Ninth Circuit held that the government violated the defendant's Fourth Amendment rights when it viewed — without a warrant — images he had attached to an email that Google flagged as "apparent child pornography."[9] The Ninth Circuit correctly applied precedent in this case, but only because the government did not provide adequate evidence to demonstrate the accuracy of Google's CSAM screening process.[10] The fact that the government can easily provide such information in future cases, nullifying the Ninth Circuit's analysis in this one, reveals that current Fourth Amendment jurisprudence does not provide meaningful protection against the government's ever-increasing power to conduct digital surveillance and that Congress shoulders the responsibility of protecting citizens' digital privacy rights.

---

[1] *See generally* Ateret Gewirtz-Meydan et al., *The Complex Experience of Child Pornography Survivors*, 80 CHILD ABUSE & NEGLECT 238 (2018).

[2] Pub. L. No. 110-401, 122 Stat. 4229 (codified as amended in scattered sections of 18 and 34 U.S.C.).

[3] *See Summary: S.1738 — 110th Congress (2007–2008)*, CONGRESS, https://www.congress.gov/bill/110th-congress/senate-bill/1738 [https://perma.cc/CW95-DNM9].

[4] 18 U.S.C. § 2258E(6).

[5] *Id.* §§ 2258A(a)(1)(A), (2)(A).

[6] *See* United States v. Wilson, 13 F.4th 961, 964 (9th Cir. 2021).

[7] *See, e.g.*, United States v. Miller, 982 F.3d 412, 421–34 (6th Cir. 2020); United States v. Ackerman, 831 F.3d 1292, 1304–08 (10th Cir. 2016).

[8] 13 F.4th 961 (9th Cir. 2021).

[9] *Id.* at 964.

[10] *Id.* at 972.

In June 2015, defendant Luke Wilson attached four images containing CSAM to an email on his Gmail account.[11] Google's proprietary screening system — which scans uploaded images and checks for identical matches in a database of confirmed CSAM[12] — immediately flagged Wilson's attachments as "apparent child pornography."[13] Without having an employee review the attachments first, Google's system then sent an automated report to the NCMEC's CyberTipline that included the attachments.[14] The report classified each image as "A1," a standard classification in the tech industry for "content [that] contains a depiction of a prepubescent minor engaged in a sex act."[15] NCMEC forwarded the report to local law enforcement.[16]

Agent Thompson, a member of San Diego's Internet Crimes Against Children Task Force, reviewed the report forwarded by the NCMEC.[17] Thompson inspected each of the images and confirmed that they were indeed CSAM.[18] Relying on Google's report and his personal observations, Thompson then applied for and obtained a search warrant for Wilson's email account.[19] When he searched Wilson's email account, "he discovered numerous email exchanges in which Wilson received and sent . . . child pornography and in which Wilson offered to pay for the creation of child pornography."[20] Law enforcement subsequently obtained a search warrant for Wilson's house, where they discovered electronic devices "containing thousands of images of child pornography," including the four email attachments.[21] A few months later, Wilson was arrested and charged with distributing and possessing CSAM.[22]

After his arrest, Wilson filed a motion to suppress the four attachments flagged by Google's screening technology and "all evidence subsequently seized from [his] email account and residence."[23] He argued

---

[11] *Id.* at 965.

[12] See *infra* notes 62–69 and accompanying text for a more detailed description of Google's screening process.

[13] *Wilson*, 13 F.4th at 965.

[14] *Id.* The report contained "information about the date and time [Wilson] uploaded the four child pornography images" along with Wilson's email address, login information, and the IP address of the device he used to upload the images. United States v. Wilson, No. 15-cr-02838, 2017 WL 2733879, at *3 (S.D. Cal. June 26, 2017).

[15] *Wilson*, 2017 WL 2733879, at *3.

[16] *Wilson*, 13 F.4th at 965.

[17] *Id.*

[18] *See id.*

[19] *See id.* at 965–66. Thompson's affidavit accompanying the request for a search warrant included descriptions of the four images but "did not contain any mention of hash values, any description of Google's screening process for child pornography, or the A1 classification Google assigned to the four images." *Wilson*, 2017 WL 2733879, at *11.

[20] *Wilson*, 13 F.4th at 966.

[21] *Id.*

[22] *Wilson*, 2017 WL 2733879, at *6.

[23] *Id.*

that Thompson's initial review of his attachments was a warrantless search in violation of the Fourth Amendment.[24] But the district court denied his motion.[25] Its reasoning was based on two Fourth Amendment doctrines: the private search doctrine and the virtual certainty doctrine.[26] The private search doctrine is the principle that "[t]he [government]'s viewing of what a private party ha[s] freely made available for [it]s inspection d[oes] not violate the Fourth Amendment."[27] The virtual certainty doctrine holds that the government does not perform a search within the meaning of the Fourth Amendment when it inspects something that is "virtually certain" to "contain[] nothing but contraband."[28]

These doctrines were both applied by the Supreme Court in *United States v. Jacobsen*,[29] which the district court in *Wilson* cited heavily.[30] In *Jacobsen*, the Supreme Court held that law enforcement agents did not conduct an unconstitutional search when they reopened a damaged package or when they conducted a drug field test on the suspicious white powder they found inside.[31] Federal Express (FedEx) employees had summoned the agents after opening the package and discovering the bag of powder.[32] The Court first reasoned that the agents did not violate the defendant's Fourth Amendment rights under the private search doctrine when they opened the box because their search merely repeated the FedEx employees' actions.[33] The Court then concluded that the field test was not a search "within the meaning of the Fourth Amendment"[34] because the agents had "virtual certainty"[35] that the test "could [have] reveal[ed] nothing about noncontraband items"[36] and therefore "d[id] not compromise any legitimate interest in privacy."[37]

Applying *Jacobsen*, the district court in *Wilson* concluded that the government's search did not violate Wilson's Fourth Amendment

---

[24] *See id.* at *6–7.

[25] *Id.* at *7.

[26] *See id.* at *10–11.

[27] United States v. Jacobsen, 466 U.S. 109, 119–20 (1984) (citing Coolidge v. New Hampshire, 403 U.S. 443, 487–90 (1971); Burdeau v. McDowell, 256 U.S. 465, 475–76 (1921)).

[28] *Id.* at 120 n.17 ("[T]he container could no longer support any expectation of privacy, and . . . it was virtually certain that it contained nothing but contraband."); *see also* Texas v. Brown, 460 U.S. 730, 751 (1983) (Stevens, J., concurring in the judgment); Illinois v. Andreas, 463 U.S. 765, 771–72 (1983); *id.* at 782 (Stevens, J., dissenting).

[29] 466 U.S. 109 (1984).

[30] *See Wilson*, 2017 WL 2733879, at *8–11.

[31] *See Jacobsen*, 466 U.S. at 111–12, 118, 126.

[32] *Id.* at 111.

[33] *See id.* at 119–20.

[34] *Id.* at 122.

[35] *Id.* at 119.

[36] *Id.* at 124 n.24.

[37] *Id.* at 123.

rights.[38] First, the court concluded that Google's use of "sophisticated hashing tools" to flag Wilson's email attachments as CSAM constituted a private search, so the government's warrantless review of Google's report was constitutional.[39] Second, the court concluded that, even assuming that Thompson's viewing of the attachments expanded on Google's search, the expansion was not an unconstitutional search because it was virtually certain that the view "could [have] reveal[ed] nothing about noncontraband items."[40]

The Ninth Circuit reversed.[41] Writing for the panel, Judge Berzon[42] concluded that Thompson's viewing of the attachments violated Wilson's Fourth Amendment rights.[43] She rejected the district court's application of the virtual certainty doctrine when she noted that the government's explanation of the accuracy of Google's CSAM screening system was "vague[]" and filled with "gaps."[44] Therefore, she focused her opinion on the private search doctrine, offering three reasons in support of the conclusion that the government exceeded the scope of Google's private search.

First, Judge Berzon pointed out that viewing the images allowed Thompson to learn "new, critical information"[45] that the government then used to obtain warrants to search Wilson's home and email account.[46] She highlighted that Thompson was able to confirm that the images were CSAM and learn about the images' settings and the people and sexual acts depicted.[47] Google's report, on the other hand, "specified only the general age of the child and the general nature of the acts shown."[48] Without the information Thompson gained from viewing the attachments, his affidavit would not have supported a search warrant.[49]

---

[38] United States v. Wilson, No. 15-cr-02838, 2017 WL 2733879, at *7 (S.D. Cal. June 26, 2017).

[39] *Id.* at *10.

[40] *Id.* at *11 (alteration in original) (quoting United States v. Ackerman, 831 F.3d 1292, 1306 (10th Cir. 2016)).

[41] *Wilson*, 13 F.4th at 964.

[42] Judge Berzon was joined by Judges Watford and Whaley.

[43] *Wilson*, 13 F.4th at 964.

[44] *Id.* Oddly, Judge Berzon never mentioned the virtual certainty doctrine outright in her opinion. Her decision not to mention the doctrine may have been motivated by the fact that the government stated at oral argument that "it [was] not relying on the contraband nature of child pornography as a justification for the search." *Id.* at 974 n.12. Regardless, it is significant that the government failed to establish the reliability of Google's CSAM screening technology because, as Judge Berzon pointed out, Wilson explicitly "challenge[d] the 'accuracy and reliability' of Google's hashing technology." *Id.* at 979 (contrasting this case with *United States v. Miller*, 982 F.3d 412, 429–30 (6th Cir. 2020), where the Sixth Circuit found no Fourth Amendment violation because the defendant never challenged the reliability of a service provider's CSAM screening technology).

[45] *Id.* at 972.

[46] *See id.* at 972–74.

[47] *See id.* at 973–74.

[48] *Id.* at 973.

[49] *See id.*

Second, Judge Berzon held that Thompson's inspection invaded Wilson's privacy interests to a greater degree than Google's scan.[50] She explained that Wilson maintained a privacy interest in the details of his images that was not frustrated by Google's scan, which merely flagged the images as CSAM and generally described their contents.[51] By contrast, after viewing the images, Thompson could describe "the number of minors depicted, their identity, the number of adults depicted alongside the minors, the setting, and the actual sexual acts depicted."[52]

Third, Judge Berzon addressed the counterargument that, because the Google employees who originally created the apparent CSAM database had viewed images identical to Wilson's, Thompson did not actually see things that "no Google employee viewed . . . before [he] did."[53] Judge Berzon insisted that Fourth Amendment rights are personal: the fact that Google employees had seen files identical to Wilson's was irrelevant to this case because the issue was whether a private party had viewed Wilson's files.[54] She explained that Wilson had a privacy interest in his files that was not frustrated when Google employees previously classified identical images as apparent CSAM.[55] Rather, his interest was fully frustrated when Thompson inspected the attachments himself.[56]

Judge Berzon correctly applied current Fourth Amendment doctrine in *Wilson*, but only because the government provided scant evidence about the reliability and accuracy of Google's CSAM screening process.[57] If the government had provided detailed information showing the accuracy of Google's CSAM detection system, this case would likely have come out differently. The government could have shown that Thompson had virtual certainty that Wilson's images were illegal CSAM, so his inspection of the images could not have been a search within the meaning of the Fourth Amendment. Thus, in future cases, the government is free to rely on internet service providers' ability to scan billions of images without obtaining warrants to ferret out CSAM producers, possessors, and distributors. This reality suggests that current Fourth Amendment jurisprudence does not provide meaningful protection against many forms of digital surveillance. Absent a shift in

---

[50] *See id.* at 974.

[51] *See id.* Even though Google employees viewed images identical to Wilson's to create Google's database of suspected CSAM, Judge Berzon found it significant that "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." *Id.* (emphasis added).

[52] *Id.*

[53] *Id.*

[54] *See id.*

[55] *See id.* at 975.

[56] *See id.*

[57] Google submitted only a "two-page declaration" about its screening process, and Judge Berzon noted that the declaration was "vague[]" and contained "gaps." *Id.* at 964.

Fourth Amendment doctrine, Congress shoulders the burden of deciding which digital privacy rights merit protection.

First, by proving the accuracy of Google's screening process, the government could have shown that Thompson could have obtained a search warrant for Wilson's email account without relying on the details he learned by viewing the attachments.[58] This would have undermined Judge Berzon's initial conclusion that Thompson gained "critical information" that allowed him to advance his investigation.[59] The standard for obtaining a search warrant is "probable cause,"[60] and Google's screening process produces much more than a "fair probability" that flagged images are illegal CSAM.[61] To identify illegal CSAM on its platforms, Google first employs counsel to train a group of employees on the legal definition of child pornography.[62] Those employees confirm images of CSAM and categorize them.[63] Hash values of the images are subsequently added to Google's apparent CSAM database.[64] While it is conceivable that the employees might make a mistake, it is unlikely.[65] Then, Google uses a hashing algorithm to match images on its platforms with the hash values in its database.[66] Good hashing algorithms provide hash values that, "for all practical purposes, [are] uniquely associated with [an] input,"[67] such as an image. "[C]hanging so little as one bit" of an image changes the hash value it will generate.[68] Thus, when Google's

---

[58] Judge Berzon acknowledged this point in footnote 11 of her opinion. *See id.* at 973 n.11.

[59] *Id.* at 972.

[60] *Id.* at 973 n.11.

[61] Illinois v. Gates, 462 U.S. 213, 238 (1983) (holding that, in deciding whether to issue a search warrant, "[t]he task of the issuing magistrate is simply to make a practical, common-sense decision whether . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place").

[62] *See Wilson*, 13 F.4th at 964–65.

[63] *See id.* at 965.

[64] *See id.*

[65] *See* United States v. Ackerman, 831 F.3d 1292, 1306 (10th Cir. 2016) (noting that it is "unlikely" that employees might make a mistake in identifying CSAM). Even so, the government could have helped the court be more confident in the Google employees' ability to identify CSAM by, for example, providing detailed information about Google's training program and materials or testing the employees on a fresh sample of images. Further, in future cases, the government and Google could work together to eliminate the risk of human error by, for instance, adding special flags to images that belong to "known series of confirmed child pornography," especially ones that have already "been the subject of adjudication." Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 HARV. L. REV. F. 38, 46 (2006); *see also* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 546 (2005) ("The National Drug Intelligence Center has calculated and collected common hash values . . . for many images of child pornography in a database called the Hashkeeper."). It is quite likely that Google's database already includes images from some known series because the PROTECT Act authorizes the NCMEC to "provide elements relating to any apparent child pornography . . . to a[] . . . provider for the sole and exclusive purpose of permitting that . . . provider to stop the further transmission of images." 18 U.S.C. § 2258C(a)(1).

[66] *See* United States v. Wilson, No. 15-cr-02838, 2017 WL 2733879, at *2 (S.D. Cal. June 26, 2017).

[67] Salgado, *supra* note 65, at 39.

[68] *Id.*

algorithm flagged Wilson's attachments, it had established to near mathematical certainty that his images were "bit-for-bit" duplicates of images identified by its employees as depicting prepubescent children engaged in sex acts.[69]

Second, the government could have argued that Thompson's review of the attachments did not intrude on Wilson's privacy more than Google's scan even though Thompson was certain to uncover more details than were contained in Google's report. Case law supports the proposition that the government does not "intrude upon any *legitimate* privacy interest" in the special case that its "conduct could reveal nothing about *noncontraband* items."[70] For example, in *United States v. Tosti*,[71] the Ninth Circuit held that the police did not conduct a search within the meaning of the Fourth Amendment when they enlarged thumbnails of CSAM that a technician discovered on the defendant's computer.[72] The police undoubtedly learned "innumerable granular private details"[73] about the defendant's CSAM by enlarging the images — for example, about their settings, the identities of the participants, and the particular acts being depicted — but the court never discussed this fact. Instead, it emphasized that the thumbnails already revealed that the images "depicted many graphic sex scenes of children,"[74] so for the court's purposes, "the police learned nothing new through their actions."[75] Similarly, in *United States v. Miller*[76] — a case with substantially the same facts as *Wilson* — the Sixth Circuit was never troubled that the police inspection could have revealed additional details about confirmed CSAM.[77] On the other hand, it expressed concern that, if Google's screening process proved inaccurate, the police's inspection of Google's report might reveal "an embarrassing picture of the sender or an innocuous family photo."[78]

The courts' reasoning in *Tosti* and *Miller* also explains how *Wilson* is distinguishable from *Walter v. United States*[79] and *United States v.*

---

[69] *See id.* The well-known MD-5 and SHA-1 hashing algorithms can each generate more than 340 billion, billion, billion, billion unique hashes, so their odds of assigning identical hashes to different images are "infinitesimally small." *Id.* at 39 n.6.

[70] United States v. Jacobsen, 466 U.S. 109, 124 n.24 (1984) (emphasis added).

[71] 733 F.3d 816 (9th Cir. 2013).

[72] *Id.* at 821–22.

[73] *Wilson*, 13 F.4th at 979.

[74] *Tosti*, 733 F.3d at 819.

[75] *Id.* at 822.

[76] 982 F.3d 412 (6th Cir. 2020).

[77] *See id.* at 429–30 ("At bottom, then, this case turns on the question whether Google's hash-value matching is sufficiently reliable.").

[78] *Id.* at 429.

[79] 447 U.S. 649 (1980) (plurality opinion).

Mulder,[80] two cases that featured prominently in Judge Berzon's opinion.[81] In *Walter*, the Supreme Court held that government agents conducted a warrantless search in violation of the Fourth Amendment when they screened films that had been accidentally shipped to a private firm, even though "[l]abels on the individual film boxes indicated that they contained obscene pictures."[82] In *Mulder*, the Ninth Circuit held that the government violated the Fourth Amendment when it took pills recovered from a hotel room to a laboratory and, without a warrant, performed "a series of tests designed to reveal [their] molecular structure . . . and indicate precisely what [they were]."[83] In both cases, "[p]rior to the Government [inspection], one could only draw *inferences* about what was on the films"[84] or in the pills. In neither case did the agents have virtual certainty that they were inspecting only contraband. These cases stand in sharp contrast to *Wilson*. There, Thompson knew with near-perfect certainty that Wilson's attachments contained CSAM, so Thompson's review of the attachments did not intrude on any reasonable expectation of privacy.

Given the information she was provided, Judge Berzon was correct to grant Wilson's motion to suppress. But in doing so, she mapped out exactly how the government can continue to rely on technology companies' powerful tools to prosecute child exploitation cases without running afoul of the Fourth Amendment. In one sense, this is a victory for justice. After all, the guilt and humiliation that plague survivors of CSAM production are awful and long-lasting.[85] But at the same time, *Wilson* shows how courts are largely incapable of protecting citizens against invasive digital surveillance with their current set of doctrinal tools. And courts will only become less effective as hashing technology and other screening methods become more powerful and the risk of human error is gradually eliminated. With the PROTECT Act, Congress took a step toward fulfilling the role of defining citizens' privacy rights: it weighed the harms of CSAM production and distribution against citizens' privacy interests in their online communications and emphatically declared that society will not accept as reasonable any expectation of privacy in possessing CSAM. Absent a clear shift in Fourth Amendment doctrine from the courts, society must continue to turn to Congress to define what expectations of digital privacy are reasonable and thus protected from warrantless searches by law enforcement.

---

[80] 808 F.2d 1346 (9th Cir. 1987).
[81] *See, e.g.*, *Wilson*, 13 F.4th at 968–69, 973, 975, 978–79.
[82] *Walter*, 447 U.S. at 651–52, 654 (plurality opinion).
[83] *Mulder*, 808 F.2d at 1347–48.
[84] *Walter*, 447 U.S. at 657 (plurality opinion) (emphasis added).
[85] *See* Gewirtz-Meydan et al., *supra* note 1, at 241, 243.