

No. 20-1737

IN THE SUPREME COURT OF THE UNITED STATES

Luke Noel Wilson,

Petitioner,

-v-

State Of California,

Respondent.

REPLY IN SUPPORT OF PETITION FOR WRIT OF CERTIORARI
TO THE CALIFORNIA COURT OF APPEAL,
FOURTH APPELLATE DISTRICT, DIVISION ONE

Devin Burstein
* Counsel of Record for Petitioner
Warren & Burstein
501 W. Broadway, Suite 240
San Diego, CA 92101
(619) 234-4433
db@wabulaw.com

Charles M. Sevilla
402 W. Broadway, #720
San Diego, CA 92101
(619) 232-2222
chuck@charlessevilla.com

TABLE OF CONTENTS

TABLE OF AUTHORITIES.....	ii
PETITIONER'S REPLY TO THE BRIEF IN OPPOSITION	1
CONCLUSION	15

TABLE OF AUTHORITIES

Federal Cases

<i>Carpenter v. United States,</i> 138 S. Ct. 2206 (2018).....	2
<i>Ex Parte Jackson,</i> 96 U.S. 727 (1877).....	15
<i>Riley v. California,</i> 573 U.S. 373 (2014).....	1, 13
<i>Sessions v. Dimaya,</i> 138 S. Ct. 1204 (2018).....	3
<i>United States v. Ackerman,</i> 831 F.3d 1292 (10th Cir. 2016)	8, 15
<i>United States v. Jacobsen,</i> 466 U.S. 109 (1984).....	4
<i>United States v. Jones,</i> 565 U.S. 400 (2012).....	15
<i>United States v. Miller,</i> 982 F.3d 412 (6th Cir. 2020)	1, 10
<i>United States v. Reddick,</i> 900 F.3d 636 (5th Cir. 2018)	1
<i>United States v. Ringland,</i> 966 F.3d 731 (8th Cir. 2020)	10
<i>United States v. Wilson,</i> 13 F.4th 961 (9th Cir. 2021)	<i>passim</i>
<i>Walter v. United States,</i> 447 U.S. 649 (1980).....	4

California Cases

<i>People v. Williams,</i> 20 Cal. 4th 119 (1999)	15
------------------------------------------------------------	----

People v. Wilson,
56 Cal. App. 5th 128 (2020) *passim*

A single warrantless search of Mr. Wilson’s email files resulted in two conflicting published opinions and created a split in the circuits on a critical Fourth Amendment question: whether the private search doctrine allows the government to search individuals’ email files without a warrant. As a result of the opposing opinions, the Fourth Amendment applies differently throughout the country, and law enforcement officers must operate under divergent constitutional constraints. The problem is particularly acute in California where the state and federal courts have reached opposite results on identical facts.

The current state of the law is as follows: Officers investigating federal cases within the Ninth Circuit must secure a warrant before searching a hash-matched file attached to an email. *See United States v. Wilson*, 13 F.4th 961 (9th Cir. 2021). But they need not do so in Fifth and Sixth Circuits. *See United States v. Reddick*, 900 F.3d 636 (5th Cir. 2018), *United States v. Miller*, 982 F.3d 412 (6th Cir. 2020). And in California, under the Ninth Circuit’s *Wilson* decision, an officer investigating a case for *federal* prosecution must secure a warrant before searching an email file. Yet based on the conflicting California Court of Appeal’s *Wilson* decision, the same officer investigating a case for *state* prosecution does not. *See People v. Wilson*, 56 Cal. App. 5th 128 (2020).

This divergence is untenable. *See Riley v. California*, 573 U.S. 373, 398 (2014) (“[I]f police are to have workable rules, the balancing of the competing interests . . . ‘must in large part be done on a categorical basis[.]’”).¹ Indeed, beyond law enforcement considerations, the Fourth Amendment stands as a singular bulwark against government overreach. Its purpose is to protect the People. And as of now, the People of the United States, depending on their circuit, have

¹ Unless noted, all internal citations are omitted, and all emphasis is added.

different levels of Fourth Amendment protections for their electronic communications.

The ubiquity of such communications – email, texting, direct-messaging – is beyond dispute, as is the ability of companies like Google and Facebook to scan their users’ content. Indeed, “[t]he Gmail scanner [alone] processes an incredible 300 billion Gmail attachments every single week[.]”² If the government can piggyback on those scans to avoid the warrant requirement, the Fourth Amendment implications are staggering. “As technology has enhanced the Government’s capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to ‘assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.’” *Carpenter v. United States*, 138 S. Ct. 2206, 2214 (2018). Here, given the split of authority on this important constitutional issue, the Court should grant review and bring uniformity to the law.

I

Mr. Wilson begins by briefly reviewing the relevant circumstances of the subject search. He will then discuss the state-federal split on that search, the split within the circuits, and the overall importance of the issue presented.

A

The events giving rise to this case were triggered when Google, as required by federal law, reported to the National Center for Missing and Exploited Children (NCMEC) that Mr. Wilson had uploaded four images of apparent child pornography to his email account as attachments (this report is known as a “CyberTip”). *See Wilson*, 13 F.4th at 963-65. No one at Google, however, opened or viewed Mr. Wilson’s email attachments. Rather, its report was based on a purely automated, algorithmic assessment that Mr. Wilson’s files were the same as those belonging to

² Google Confirms New AI Tool Scans 300 Billion Gmail Attachments Every Week, *Forbes*, <https://bit.ly/3DdCBSg>.

some other unknown person that an unknown Google employee/contractor had earlier viewed and classified as child pornography. *See id.*

NCMEC then, also without opening Mr. Wilson's files, forwarded them to the San Diego Internet Crimes Against Children Task Force, where an agent viewed them *without a warrant*. *See id.* at 965-66. The agent was the *first* person to examine the contents of the uploaded files in Mr. Wilson's email. Based on what the agent saw, he applied for warrants to search both Mr. Wilson's email account and home. In the warrant applications, the agent included detailed descriptions of the subject files based on what he learned by viewing the files (these descriptions were not included in the automated Google or NCMEC reports). *See id.* The subsequent searches revealed additional contraband.

Thereafter, the federal government and State of California independently charged Mr. Wilson with criminal offenses. *See id*; *Wilson*, 56 Cal. App. 5th at 134.³ He filed similar motions to suppress in each case, arguing that the agent's warrantless search of his email files violated his reasonable expectation of privacy and constituted an unlawful trespass on his electronic property. *See Wilson*, 13 F.4th at 966; *Wilson*, 56 Cal. App. 5th at 139-140. The respective trial courts held hearings, with nearly identical evidence. *See id.* Although the State now claims there were material differences between the proceedings, as discussed below, this is “slicing the baloney mighty thin.” *Sessions v. Dimaya*, 138 S. Ct. 1204, 1215 (2018).

The trial courts denied the suppression motions, and Mr. Wilson was convicted in both proceedings. *See Wilson*, 13 F.4th at 966; *Wilson*, 56 Cal. App. 5th at 139-40. He appealed to

³ The Court already has access to the state-court record under Rule 12.7. The briefs in the federal appeal are available at ECF Nos. 8, 29, 39 in *United States v. Wilson*, Case No. 18-50440 (9th Cir.). The district court record is at 15-cr-2838-GPC (S.D. Cal.).

the California Court of Appeal and the Ninth Circuit, respectively. *See id.* In both appeals, Mr. Wilson again raised identical arguments about the warrantless search of his email files – that it violated his privacy and property rights under the Fourth Amendment. *See id.*

B

The state court issued its opinion first. As already discussed in both the petition for certiorari and the state’s opposition (and thus addressed only briefly now), the California Court of Appeal held the search did not violate Mr. Wilson’s Fourth Amendment rights. Relying heavily on *United States v. Jacobsen*, 466 U.S. 109 (1984), and distinguishing *Walter v. United States*, 447 U.S. 649 (1980), the court concluded:

[T]he government’s warrantless search of Wilson’s four images was permissible under the private search doctrine. Google’s private search frustrated Wilson’s expectation of privacy in the files before they were viewed by the government. Google had already identified Wilson’s files as having matching hash values to images that had previously been viewed and identified by a Google employee as apparent child pornography. The government’s subsequent opening and viewing of the four photographs did not significantly expand on the search that had previously been conducted by Google. The agent’s actions in opening the files and viewing the images merely confirmed that the flagged files were child pornography, as reflected in Google’s Cybertip report.

Wilson, 56 Cal. App. 5th at 147.

The court next considered Mr. Wilson’s property-based argument: “Wilson contends he can establish a violation of his Fourth Amendment rights based on a trespass theory, irrespective of whether his privacy interests were invaded.” *Id.* at 152. The court concluded there was “no sound basis for finding a Fourth Amendment violation under these circumstances, even if Google’s search can be characterized as an unlawful trespass, a physical intrusion on defendant’s property interests, or any other type of wrongful conduct.” *Id.*

C

The Ninth Circuit reached the opposite result. Although the court acknowledged the

state-court’s opinion, it rejected the reasoning. *See Wilson*, 13 F.4th at 966 n.5.

The Ninth Circuit framed the issue as follows: “We once again consider the application of the Fourth Amendment’s warrant requirement to new forms of communication technology. ‘When confronting [such] concerns wrought by digital technology, the Supreme Court has been careful not to uncritically extend existing precedents.’ Our question this time concerns the private search exception to the Fourth Amendment—specifically, the intersection between electronic communications providers’ control over material on their own servers and the Fourth Amendment’s restriction of warrantless searches and seizures[.]’” *Id.* at 963-64 (cleaned up).

The Ninth Circuit, contrary to the California Court of Appeal, determined that “the government’s actions here exceed the limits of the private search exception as delineated in *Walter* and *Jacobsen* and their progeny.” *Id.* at 971-72. “First, the government search exceeded the scope of the antecedent private search because it allowed the government to learn new, critical information that it used first to obtain a warrant and then to prosecute Wilson. Second, the government search also expanded the scope of the antecedent private search because the government agent viewed Wilson’s email attachments even though no Google employee—or other person—had done so, thereby exceeding any earlier privacy intrusion.” *Id.*

In support, the court noted, “Google does not keep a repository of child pornography images, so no Google employee could have shown the government the images it believed to match Wilson’s.” *Id.* at 972. Rather, “Google keeps a repository of unique hash values corresponding to illicit images, and tags each image with one of four generic labels. 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 Based only on the barebones CyberTip, Agent Thompson testified, he opened

and reviewed each of Wilson’s images to determine ‘whether or not it is a case that . . . can be investigated’ for violations of federal law.” *Id.* Thereafter, based on that review, Agent Thompson, included “[a] detailed description of the images . . . in the applications for search warrants. The gulf between what Agent Thompson knew about Wilson’s images from the CyberTip and what he subsequently learned is apparent from those descriptions.” *Id.*

Under these facts – which were identical to the state-court record, because it was the same search – the Ninth Circuit concluded that “the large gap between the information in the CyberTip and the information the government obtained and used to support the warrant application and to prosecute Wilson, [demonstrates that] the government search in *Walter* offers a much more apt comparison to the circumstances here than does the government search in *Jacobsen*.” *Id.* at 973.

To this end, the court explained: “Viewing Wilson’s email attachments—like viewing the movie in *Walter*—substantively expanded the information available to law enforcement far beyond what the label alone conveyed The government learned at least two things above and beyond the information conveyed by the CyberTip by viewing Wilson’s images: First, Agent Thompson learned exactly what the image showed. Second, [he] learned the image was in fact child pornography. Until he viewed the images, they were at most ‘suspected’ child pornography.” *Id.* And “[j]ust as it ‘was clearly necessary for the FBI to screen the films [in *Walter*], which the private party had not done, in order to obtain the evidence needed to accomplish its law enforcement objectives,’ so here, to prosecute Wilson it was necessary for Agent Thompson to view the images no Google employee had opened.” *Id.* Thus, “[b]ecause the government saw more from its search than the private party had seen, it exceeded the scope of the private search.” *Id.* at 974.

The Ninth Circuit further rejected the California Court of Appeal’s premise that “Wilson’s

expectation of privacy in his images was fully frustrated when Google’s computer technology scanned them[.]” *Id.* at 974. “Although Google’s proprietary technology labelled Wilson’s email attachments as [child pornography,] ‘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.” *Id.*

This was equally true for Agent Thompson. “Until he viewed the images, he had no image at hand at all; the entire composition was hidden. Only the image itself could reveal, for example, the number of minors depicted, their identity, the number of adults depicted alongside the minors, the setting, and the actual sexual acts depicted. Reading a label affixed to an image is a different experience entirely from looking at the image itself.” *Id.*

Nor did it matter that an unknown person at Google had previously viewed some “other individuals’ files” and “classified [them] as child pornography in Google’s database of hash values.” *Id.* at 975. “Even if Wilson’s email attachments were precise duplicates of different files a Google employee had earlier reviewed and categorized as child pornography, both *Walter* and *Jacobsen*—and general Fourth Amendment principles— instruct that we must specifically focus on the extent of Google’s private search of Wilson’s effects, not of other individuals’ belongings, to assess whether ‘the additional invasions of [Wilson’s] privacy by the government agent . . . exceeded the scope of the private search.’” *Id.*

This is because “Fourth Amendment rights are personal rights.” *Id.* “A violation of a third party’s privacy has no bearing on *my* reasonable expectation of privacy in my own documents.” *Id.* “[W]hether Google had previously reviewed, at some earlier time, other individuals’ files is not pertinent to whether a private search eroded Wilson’s expectation of

privacy. Under the private search doctrine, the Fourth Amendment remains implicated ‘if the authorities use information with respect to which the expectation of privacy has not already been frustrated.’” *Id.*

After addressing Mr. Wilson’s privacy interest and the agent’s expansion of the private search,⁴ the Ninth Circuit turned to the relevant caselaw from other circuits.

Beginning with Justice (then-Judge) Gorsuch’s opinion in *United States v. Ackerman*, 831 F.3d 1292, 1294 (10th Cir. 2016), the Ninth Circuit noted that, “[a]lthough *Ackerman* did not decide the precise issue before us [regarding the warrantless search of email attachments] . . . its underlying analysis is entirely consistent with ours, and its suggestions about why there could be a search in our circumstances echo some of the reasons we have given for so concluding.” *Id.* at 976-77. Namely, “the government’s action may still be a new search, as the government, ‘might . . . have risked exposing new and protected information, maybe because the hash value match could have proven mistaken . . . or because the [] employee who identified the original image as child pornography was mistaken in his assessment.’” *Id.*⁵

On the other hand, the court recognized the Circuit split it created: “the Fifth and Sixth Circuits recently decided the issue before us and came to a conclusion contrary to the one we reach, although the reasoning of the two opinions diverged.” *Id.* at 978. First, in *Reddick*, “[t]he Fifth Circuit held the private search exception justified the government’s warrantless search because the

⁴ Because the court ruled on this basis, it did “not consider Wilson’s alternative argument that the government’s search violated his property-based Fourth Amendment rights.” *Id.* at 967 n.7.

⁵ This observation accords with the record here. Google’s declaration noted a hash match was indicative of “apparent child pornography.” 1 CT 196, 197. The CyberTip also characterized it as such. 1 CT 203. This phrasing accounts for plausible human or hash-match error, which shows that a hash alone cannot provide certainty that the subject file is contraband.

government agent’s ‘visual review of the suspect images . . . was akin to the government agents’ decision to conduct chemical tests on the white powder in *Jacobsen*,’ insofar as ‘opening the file merely confirmed that the flagged file was indeed child pornography, as suspected.’” *Id.* at 978.

The Ninth Circuit rejected “this analysis,” concluding that *Reddick* misread *Jacobsen*: “*Reddick* conflates *Jacobsen*’s first holding regarding the private search exception to the Fourth Amendment with its second holding regarding whether the field test constituted a search under the Fourth Amendment.” *Id.* “Moreover, in *Jacobsen*, the white powder was fully visible to the government officers when they repeated the steps taken by the FedEx employees to inspect the package. Not so here, as no human had viewed Wilson’s images before.” *Id.* And contrary to *Reddick*’s reasoning, the court determined that “the government’s ‘visual review of the suspect images’ was not analogous to ‘the government agents’ decision to conduct chemical tests on the white powder in *Jacobsen*.’” *Id.* at 979.

The Ninth Circuit further pointed out that, in *Miller*, “[t]he Sixth Circuit [also] recognized the error in *Reddick* concerning the reach of the private search holding in *Jacobsen* and ‘opt[ed] not to rely’ on it.” *Id.* Instead, *Miller*, “resolved the Fourth Amendment question it faced by focusing exclusively on the assumed reliability of Google’s proprietary technology.” *Id.* The Ninth Circuit, however, disagreed with that analysis too. “In our view, the critical factors in the private search analysis, both unacknowledged in *Miller*, include the personal nature of Fourth Amendment rights and the breadth of essential information Agent Thompson obtained by opening the attachment, information—and a privacy invasion—well beyond what Google communicated to NCMEC.” *Id.*

The court ended with a cautionary note. “[T]here were 18.4 million CyberTips in 2018, making it all the more important that we take care that the automated scanning of email, and the

automated reporting of suspected illegal content, not undermine individuals' Fourth Amendment protections." *Id.* at 979-80.

II

There is now a clear split of authority on the application of the private search doctrine to digital files. The split exists as to the specific search in this case between the Ninth Circuit and California Court of Appeal. It also exists between the Ninth, Fifth, and Sixth Circuits. And as noted, even the Fifth and Sixth Circuits do not agree in their reasoning. *See Wilson*, 13 F.4th at 978-79, *Miller*, 982 F.3d at 429.⁶

A

Despite this broad precedential schism, the State claims there is no "need for further review" and seeks to minimize the extent of the split. Brief in Opposition (Opp.) at 10. It begins by arguing the state and federal *Wilson* opinions do not conflict because "[t]he Ninth Circuit's analysis was based on a record that differed in significant respects from the record that led the lower courts in this case to uphold the search." Opp. at 10.

This is wrong on multiple levels. First, the record in the two cases was not materially different. The exact same search was before both courts. The *only* difference was as to a single, non-percipient witness at the suppression hearing. Opp. at 20. During the state hearing, but not the federal, a government computer forensic agent testified about the unlikelihood of different files having the same hash value. In other words, there was marginally more evidence on hash reliability in the state proceedings. Otherwise, the evidence was equivalent.

The slight distinction, moreover, was of no moment, as the Ninth Circuit made clear: "The

⁶ The Eighth Circuit has entered the fray under materially different facts. In *United States v. Ringland*, 966 F.3d 731, 737 (8th Cir. 2020), unlike here, Google examined the actual files in the defendant's account *before* sending them to NCMEC. On that basis, the court held, "the government did not expand the search beyond Google's private party search." *Id.*

reliability of Google’s proprietary technology, in our estimation, is pertinent to whether probable cause could be shown to obtain a warrant, *not* to whether the private search doctrine precludes the need for the warrant.” *Wilson*, 13 F.4th at 979. The court continued, “even if the[] [files] were duplicates, such viewing of others’ digital communications would not have violated Wilson’s expectation of privacy in his images, as Fourth Amendment rights are personal.” *Id.* at 972. This refutes the State’s reliance on the supposed difference in the records below; neither opinion turned on the reliability of hashing technology.

The State, moreover, ignores the fact that Google’s hashing process remains an unknown. There was (and is) no evidence about the hashing method Google used or how Google assigned the subject hash values. Was it done by a Google employee or a computer? If a human, how was the person trained? When did it happen? How did those other files come to Google’s attention? The record provides none of that information. Plainly, it is unreasonable to allow warrantless searches based on untested, unreviewed “proprietary” (AKA secret) technology. This is a far cry from an employee opening a physical package in front of the police.

B

The State is also mistaken in attempting to diminish the significance of the Circuit split. It says, “the Ninth Circuit’s opinion . . . is unlikely to lead to the risk of entrenched disagreement among lower courts that would merit this Court’s immediate resolution.” Opp. at 10. This is incorrect on its face. By virtue of the Ninth Circuit’s decision, there is already entrenched disagreement in the lower appellate courts governing huge swaths of the country. Three circuits have published opinions that differ in analysis and outcome. Within these jurisdictions – geographically and by population, covering most of America – the courts, the citizenry, and law enforcement are operating under different Fourth Amendment requirements.

The State overlooks this fact, arguing instead that the California court reached the right result under the private search doctrine and thus “the Ninth Circuit’s decision [was] incorrect.” Opp. at 21. For present purposes, however, this argument helps Mr. Wilson. If the state court is right, this proves the need for further review to correct an error in the largest federal circuit. And if the Ninth Circuit is right, individuals living under the jurisdiction of the Fifth and Sixth Circuits (as well as the California Court of Appeal) have less Fourth Amendment protection than they should. Either way, this Court’s intervention is needed.

C

The State, therefore, attempts to trivialize the importance of the issue presented. It claims this case “addresses only the warrantless viewing of an image file with a hash value identical to one that has already been viewed by trained personnel at an electronic service provider and identified as child pornography.” Opp. at 28.

Not so. *Every* electronic file has a hash value.⁷ And companies like Google and Facebook scan and check the hash of *every* file sent or uploaded through their servers.⁸ Hashing technology is of general application, in no way limited to contraband or even a particular file type.⁹ Once a file’s hash value is known – *e.g.*, by reviewing a copy of the file – companies can use hashing to identify the same file automatically, so long as it appears *anywhere* on their servers. By this process, the companies could easily flag and forward to the government files containing

⁷ What is Hashing?, SentinelOne, <https://www.sentinelone.com/cybersecurity-101/hashing/>.

⁸ See, *e.g.*, Facebook scans the photos and links you send on Messenger and it reads flagged chats, Los Angeles Times, <https://www.latimes.com/business/la-fi-tn-facebook-messenger-privacy-20180404-story.html>.

⁹ Amicus Brief, *United States v. Wilson*, ECF No. 16 at 14-17, Case No. 18-50440 (9th Cir.).

political papers or medical records, just as effortlessly as contraband images.

The Fourth Amendment import is thus clear. If these private hash matches constitute automated “private searches” of the files – as the California Court of Appeal, Fifth, and Sixth Circuits have held – then the government does not need a warrant to open any of them. Any file identified by a hash match would have been privately searched and could be warrantlessly read by the government.

The State cannot avoid the far-reaching implication of such a rule. “Service providers offer many gigabytes of storage for free, so people have little incentive to delete email.”¹⁰ In particular, “Google offers its email users 15 gigabytes of storage—the equivalent of about 150 yards of books on a shelf.” *Id.* at n.2. “One study found that, on average, people have around 8,000 emails stored with their service provider, and about 20 percent of users have more than 21,000 emails stored in their inbox.” *Id.* at 6-7. In short, given the ubiquity of electronic communications, everything this Court said in *Riley* about cell phones is equally true here.

Email and the like are a “pervasive and insistent part of daily life[.]” *Riley*, 573 U.S. at 385. The public stores “many sensitive [documents]” and “a digital record of nearly every aspect of their lives” on the servers of private companies, who can – and do – scan them at will. *Id.* at 395-96. Email and related accounts, therefore, “differ in both a quantitative and a qualitative sense from other objects[.]” *Id.* at 375. And given the billions of electronic files sent by Americans, the application of the private search doctrine to those communications is at least as important as the application of the search incident to arrest exception to cell phones (*Riley*) and

¹⁰ Amicus Brief, *United States v. Ackerman II*, Case No. 17-3238, at 6 (10th Cir.), www.eff.org/files/2018/04/13/eff_et_al_10th_cir_amicus_brief_in_us_v_ackerman_4.13.18.pdf

the application of the third-party doctrine to cell-site location information (*Carpenter*).¹¹

Accordingly, there is no merit to the State’s suggestion that the issue here is not worthy of review.

The State’s remaining points are easily dispelled. First, it says, the record “establishes [] the task force that investigated petitioner [] changed its practices by the time petitioner’s motion to suppress was heard[.]” Opp. at 28-29. This claim rests on the testimony of a single agent in 2017. It says nothing about what is currently happening with that “task force,” let alone any other law enforcement agency, and it does not preclude re-adoption of the practice.

Second, the State says, “this Court’s resolution of the questions presented might not even have a substantial effect with respect to petitioner himself” because the good faith exception might apply. Opp. at 29. Not only is this wrong – the good faith exception does not apply – it is irrelevant. Because the Court of Appeal did not opine on the application of the good faith exception, it has no bearing on this petition. And regardless of whether the evidence against Mr. Wilson is ultimately suppressed, the Court should settle the larger legal issue.¹²

Finally, the State claims, Mr. Wilson’s “trespass theory is unsupportable on the merits.” Opp. at 24.¹³ The State is mistaken. Indeed, the trespass theory arguably provides the most

¹¹ The importance of the issue is further demonstrated by the amicus briefs of Google, Facebook, the ACLU, the Electronic Frontier Foundation, and the Electronic Privacy Information Center. *See United States v. Wilson*, ECF Nos. 14, 16, 34, Case No. 18-50440 (9th Cir.).

¹² The State’s reliance on Google’s terms of service also fails. The California court “resolve[d] th[e] case without addressing the terms of service.” *Wilson*, 56 Cal. App. 5th at 136 n.3. And Google’s amicus brief states its terms of service do not impact “users’ reasonable expectations of privacy[.]” ECF No. 34 at 18, *United States v. Wilson*, Case No. 18-50440 (9th Cir.).

¹³ The issue was briefed below and directly ruled on by the Court of Appeal. There is no basis for the State’s assertion that Mr. Wilson had to raise the argument in his opening suppression motion to the state *trial* court, rather than in the reply. In California, there is no such requirement. *See People v. Williams*, 20 Cal. 4th 119, 127 (1999). Thus, as the Court of Appeal decision on the merits demonstrates, the claim was preserved.

direct path to resolving the issue presented. *See United States v. Jones*, 565 U.S. 400, 404 (2012).

In *Ex Parte Jackson*, 96 U.S. 727, 733 (1877), the Court held, “[l]etters and sealed packages . . . in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles . . . Whilst in the mail, they can only be opened and examined under [a] warrant.”

Because email is the electronic equivalent of physical mail, *Ex Parte Jackson* should apply equivalently. *See Ackerman*, 831 F.3d at 1304 (“an email is a ‘paper’ or ‘effect’ for Fourth Amendment purposes, a form of communication capable of storing all sorts of private and personal details, from correspondence to images, video or audio files, and so much more.”). When a government agent examines the contents of an email without a warrant, “that seems pretty clearly to qualify as exactly the type of trespass . . . that the framers sought to prevent when they adopted the Fourth Amendment.” *Id.* at 1307. And while “the framers were concerned with the protection of physical rather than virtual correspondence[,] a more obvious analogy from principle to new technology is hard to imagine[.]” *Id.* at 1308.

Under this analysis, moreover, the private search doctrine is beside the point. *See id.* at 1307-08. If a private person trespasses on your property, that does not give the government the right to commit the same trespass. Otherwise said, the fact that a nosy neighbor wanders through your house does not mean a government agent could do so without a warrant. The Fourth Amendment prohibits such trespass. So too here.

The Court should grant Mr. Wilson’s petition.

Respectfully submitted,



Devin Burstein

* Counsel of Record for Petitioner

Dated: December 4, 2021

Warren & Burstein
501 W. Broadway, Suite 240
San Diego, CA 92101
(619) 234-4433
db@wabulaw.com

Charles M. Sevilla
402 W. Broadway, #720
San Diego, CA 92101
(619) 232-2222
chuck@charlessevilla.com