NO. 18-50440

IN THE UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

LUKE WILSON,

Defendant-Appellant.

Appeal from the United States District Court
for the Southern District of California
Honorable Gonzalo P. Curiel, District Judge Presiding

APPELLANT'S REPLY BRIEF

DEVIN BURSTEIN
Warren & Burstein
501 West Broadway, Suite 240
San Diego, CA 92101
(619) 234-4433
Attorneys for Defendant-Appellant

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Federal Cases

UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, Plaintiff-Appellee, v. LUKE WILSON, Defendant-Appellant.	C.A. No. 18-50440 U.S.D.C. No. 15-cr-2838-GPC Southern District of California APPELLANT'S REPLY BRIEF

I.
SUPPRESSION

A. Introduction.

The government claims this case fits neatly within the private search doctrine. It doesn't. The doctrine is inapplicable. And even if it applied, Agent Thompson significantly expanded on Google's review.

Unlike *Jacobsen*, it was Agent Thompson, not Google, who opened the files Mr. Wilson sent via email. While Google intercepted the files and hashed them, it did not open them to reveal their content. The files were still closed when they reached the government. Thus, a warrant was required. And whatever may have happened with someone else's files at some other time is irrelevant.

A hypothetical proves the point: Mr. Jones finds and opens an envelope – envelope A. He truthfully tells the police that, in envelope A, he saw a picture of child pornography involving prepubescent minors and nothing else. However, Mr. Jones does *not* show the image to the police. Thus, they do not know what it depicts – e.g., how many people, what they're doing, etc.

Some unknown time later, the police lawfully obtain a different envelope – envelope B. The sender/owner of envelope B is different than that of envelope A, and no one physically examined the contents of envelope B before providing it to police. But as a result of private automated technology, the police learn envelope B contains the same image as envelope A, and nothing else. The technology, however, does not allow them to see the image. Can the police search envelope B without a warrant under the private search doctrine?

No. The prior private search of envelope A does not lessen owner B's Fourth Amendment rights. Because the police never saw envelope A's contents, they must expand on the automated technology by opening envelope B to learn the details of the image – thereby frustrating owner B's privacy. After all, knowing an envelope contains a contraband picture is far different than knowing what that picture looks like, or being able to convict the sender for its possession. Moreover, the contents of envelope B remain that sender's property, on which the government cannot

trespass without judicial authorization. Thus, while the police may have probable cause to search envelope B, a warrant is still required.

The same is true here. As Agent Thompson testified, before viewing the contents of Mr. Wilson's emailed files, he could not confirm the hash match, and he had no idea what the images specifically depicted – e.g., how many people, what they were doing, etc. ER:163. To obtain that evidence, he needed to open the files.

This is constitutionally significant. "[T]he act of double-clicking to open a previously unopened file is analogous to the act of physically opening a closed container." Roderick O'Dorisio, "*You've Got Mail!" Decoding the Bits and Bytes of Fourth Amendment Computer Searches After Ackerman*, 94 Denv. L. Rev. 651, 674 (2017) ("*You've Got Mail!*"). Thus, the warrantless search here violated the Fourth Amendment.

And the private search doctrine does not excuse the violation. This case is analogous to *Walter v. United States*, 447 U.S. 649 (1980). Like the film canisters there, at the time of Agent Thompson's search, Google had not already opened Mr. Wilson's files, and its hash match could not be used to sustain a conviction. Rather, "[f]urther investigation – that is to say, a search of the contents of the [images] – was necessary in order to obtain the evidence which was to be used at trial." *Id.* at 654. And that further investigation was a distinct search.

As noted, this is far different than the scenario in *United States v. Jacobsen*, 466 U.S. 107 (1984), where the private employees had already opened the package to reveal the brick of cocaine. Here, Agent Thompson conducted that initial invasive search.

Nor should the Court follow *United States v. Reddick*, 900 F.3d 636, 637 (5th Cir. 2018). It was poorly reasoned and wrongly decided, in part because the appellant did not even raise the issue of whether the search violated the Fourth Amendment. MJN:10.[1] He focused instead on whether the court "should have applied the independent source doctrine rather than the good faith exception to the Fourth Amendment violation[.]" MJN:10. Although he touched on the private search issue (barely) in his reply brief, he did not assert a property claim. MJN:122-25. Thus, the Fifth Circuit's decision was made without the benefit of briefing on the central constitutional issues. Moreover, *Reddick* did not involve an email account – a critical, constitutional distinction – and the automated technology was different. As such, it is not persuasive. *See Woods v. Carey*, 722 F.3d 1177, 1183 n.8 (9th Cir. 2013) ("When there is a 'compelling reason to do so' we do not hesitate to create a circuit split.").

[1] MJN is the appendix to Mr. Wilson's motion for judicial notice.

B. Relevant facts.

More on this later, but it is first important to correct a few key misstatements in the government's brief.

The government repeatedly suggests that a Google employee examined the image files Mr. Wilson sent via email. GB:3, 6. This did not happen, ever. Whatever images an unknown Google employee may have looked at, at some unknown time in the past, they belonged to someone else (also unknown) and had nothing to do with Mr. Wilson. It is undisputed that *no one* at either Google or NCMEC saw the contents of the particular files in his email before Agent Thompson.[2]

Specifically, Google reported to NCMEC that a Google employee had *not* reviewed the images. ER:80, 153. Similarly, NCMEC reported the files were "unconfirmed," and it had "not opened or viewed any uploaded files submitted with this report and ha[d] no information concerning the content of the uploaded files[.]" ER:101. Thus, while Google reported a hash match to NCMEC, which NCMEC

[2] The government also claims an employee "described (prepubescent minors in sex acts), and classified (A1) the contents of each file." GB:6. There was only a subjective classification, not a separate description. ER:98, 192.

then forwarded, neither had opened nor examined the image files in Mr. Wilson's email.[3]

Additionally, the government misstates the nature of hash matching. It says: "a matched hash identifies a file's precise contents. It equates to a full-color, high-definition view of the inside." GB:6-7. But "matching the hash value of a file to a stored hash value is not the virtual equivalent of viewing the contents of the file . . . . it does not itself convey any information about the contents of the file." *United States v. Keith*, 980 F. Supp.2d 33, 43 (D. Mass. 2013). A hash value is just a series of numbers that act as a label. It does not open the file or reveal the content of the matched image file. "That is surely why [the agent] opens the file to view it, because the actual viewing of the contents provides information additional to the information provided by the hash match." *Keith*, 98 F. Supp.2d at 43

The government's summary of the reporting process from Google to NCMEC, and NCMEC to Agent Thompson is also inaccurate. GB:4. The salient fact is all the reports from Google and NCMEC were generated automatically, with no human involvement. ER:79-80, 101, 147, 158-59, 192-93.

[3] The government says: "Google's no-look referral indicates it thought the process reliable." GB:13. But Google makes both "no-look" and "look" referrals. ER:79-80. If Google's hash system were failsafe, these routine secondary human reviews would be unnecessary.

C. The private search doctrine does not excuse the warrantless search.

Moving to the merits, the government puts all its eggs in the private search basket. The basket has holes.

First, the government has not met its burden to establish the contours of the private search on which it relies. It cannot demonstrate any connection between Google's alleged prior review of files belonging to someone else at some other time and those attached to Mr. Wilson's email. Second, as to the hash match, there is no evidence as to what technology Google used, whether it was generally reliable, or whether it was properly used in this case. Third, even assuming the technology's accuracy, Agent Thompson significantly expanded on Google's private conduct by downloading and opening Mr. Wilson's files – as such, this case is like *Walter* not *Jacobsen*, *Keith* proves the point, and *Reddick* is irrelevant as well as wrongly decided.

1. The government cannot establish a connection between any initial private search and Mr. Wilson.

The government claims: "Before the agent saw the contents of the four digital files, a Google employee had seen . . . the contents of each file. Google then assigned each a "digital fingerprint ('hash')" that enabled it to search for and 'match[]' 'duplicate images' on its systems." GB:13. In support, it cites the declaration of Cathy McGoff. GB:13; ER:79-80.

But the declaration does not say that a Google employee examined any image files identical to those later found in Mr. Wilson's email. While it talks in general terms about Google's process, it does not confirm that process was applied here and contains no specifics about the subject files. ER:79-80. At most, it says the report to NCMEC "included [] four photos that Google classified as 'A1' under an industry classification standard." ER:80.

What the declaration does not explain is *how* Google assigned that classification to those specific image files. Was it done by a Google employee, someone else, a computer? When did it happen – a month before Mr. Wilson sent his email, a year, five years? How did those other files come to Google's attention? The government provides none of that information, which is wholly absent from the record.[4] Nor is there evidence that the particular employee who assigned the A1 rating was qualified to do so. These points are important for at least two reasons.

First, it is one thing to rely on a private search about which there is detailed evidence – as in both *Walter* and *Jacobsen*. It is another thing to the tell the Court, essentially, "we are the government, take our word for it, there was an expansive private search by someone, we just don't know who, when, where, how, or why." Indeed, it is just this type of distorted approach that led the Court to observe, "the ten most terrifying words in the English language may be, 'I'm from the government

[4] Google's amicus brief withholds the same information.

and I'm here to help you.'" *Garcia-Aguilar v. United States Dist. Court*, 535 F.3d 1021, 1023 (9th Cir. 2008).

Second, "the legality of the governmental search must be tested by the scope of the antecedent private search." *Jacobsen*, 466 U.S. at 116. Here, this Court has no details of that purported antecedent private search. As just one example, the government cannot establish any temporal connection.

The relevant Fourth Amendment principle usually arises in the seizure context: "a seizure reasonable at its inception . . . may become unreasonable as a result of its duration or for other reasons." *United States v. Cha*, 597 F.3d 995, 999-1000 (9th Cir. 2010). The same should be true in the private search context.

Consider the scenario in which a child allows a parent to read his or her diary. Twenty years later, the government searches the diary of the now adult without a warrant, relying on the prior private search. Is that reliance reasonable? Is the search permissible?

Surely not – "[t]he reasonableness of an official invasion of the citizen's privacy must be appraised on the basis of the facts as they existed *at the time* that invasion occurred." *Jacobsen*, 466 U.S. at 115 (emphasis added). To this end, *Jacobsen* itself noted the private search justified the government's search only "temporarily." *Id*. at 121. The Supreme Court, therefore, was careful to explain: "we do not '[sanction] warrantless searches of closed or covered containers or

packages *whenever* probable cause exists as a result of a prior private search.'" *Id.* at 120 n.17 (emphasis added).

These principles directly undermine the government's attempt to deploy the private search doctrine against Mr. Wilson. Because it cannot demonstrate when, where, by whom or how the initial purported private search took place, the government cannot establish the subsequent search by Agent Thompson was reasonably related. And research reveals no case in which this Court has approved the exception when there is no evidence establishing a close connection between the private action and the official search.

2. The government has not demonstrated the hashing technology was reliable or reliably used.

Nor can the hash match fill the gap. Other than Google's self-interested assurances, the government provides no objective evidence as to the reliability of Google's hashing technology. Thus, there is a fundamental *Daubert*-type problem. *Cf. Estate of Barabin v. AstenJohnson, Inc.*, 740 F.3d 457, 464 (9th Cir. 2014) (en banc) (it is error to allow "expert testimony without first finding it to be relevant and reliable under *Daubert*.").

Even at this late stage, it is unclear what hashing method Google used. And it is unreasonable to allow warrantless searches based on untested "proprietary" (AKA secret) technology. "When neither the public nor the accused is allowed to

look at how the software operates, it undermines the legitimacy of the judicial system and can send innocent people to prison[.]" *Opening the Black Box: Defendants' Rights to Confront Forensic Software*, available at https://bit.ly/2vLz5Pj. Indeed, the technology's demonstrated reliability, or lack thereof, should be a relevant consideration for a judge considering whether to issue a warrant.

This is especially true because the government concedes the possibility of data entry error and improper training such that employees incorrectly label non-contraband images as child pornography. GB:16. Although Google claims hashing is performed by a "team of employees" "trained by counsel on the federal statutory definition of child pornography and how to recognize it," it provides no details. ER:79. Similar to the issue just discussed, there is no evidence as to the nature of the training (was it an hour, a day, a week?), the employees' error rate in identifying contraband, or whether their decisions are reviewed before the hash is included in the private database.

This raises serious Fourth Amendment concerns. The identification of child pornography is no easy task. It relies on a multi-factor subjective inquiry known as the *Dost* test, which is often the purview of expert witnesses. *Shoemaker v. Taylor*, 730 F.3d 778, 785 (9th Cir. 2013) ("To determine whether depictions of nude children are . . . child pornography, our court and other circuits have relied on the *Dost* factors[.]"). The test includes: "whether the visual depiction suggests sexual

coyness or a willingness to engage in sexual activity; and [] whether the visual depiction is intended or designed to elicit a sexual response in the viewer." *Id.* Plainly, given these subjective interpretations, human error in hash matching is inevitable.

As discussed in EPIC's brief, this inherent flaw undermines the government's "virtual certainty" argument. It maintains that warrantless searches based on hashing should be allowed because they are guaranteed to reveal only contraband. But no, they aren't. People make mistakes.[5]

This is another reason the decision to search (open personal files) should be made by a judge, who can weigh the possibility of false positives in deciding whether to issue a warrant. That level of review is needed to protect individuals from warrantless searches based on mistaken hash entries.

Accordingly, given the government's failure to provide any details about what Google did in this case, it cannot meet its threshold burden to establish the contours of the predicate private search, or its reliability. Thus, its reliance on the doctrine fails from inception.

[5] Even Agent Thompson could not confirm whether *every* hash match referral was accurate. ER:157.

3. Agent Thompson expanded on the hash match report.

Moreover, even accepting the government's speculative portrayal of Google's private conduct, Agent Thompson's search was a significant expansion.

At its core, the private search test is straightforward. The question is whether, "at the time" of the official search, the private party had already revealed all the material information the agent later gleaned from the official search. *Jacobsen,* 466 U.S. at 115. Or, did the private acts expose only part of the information the agent would come to learn, such that additional steps were needed to find (view) the contraband?

For instance, by the time the *Jacobsen* agents arrived, the employees had found a bag of white powder inside the package. The agents needed only to confirm the chemical composition of the powder they were already staring at. On the other hand, in *Walter*, the employees found film canisters marked as pornography, but had not viewed the film. The agents, therefore, needed to take an extra step – to go beyond what the employees' exposed – to watch the films. That's the distinction.

Applying this rule, Agent Thompson's testimony is dispositive. He "wouldn't be able to compare [Google's hash value] against law enforcement's hash value databases[.]" ER:163. Rather, he needed to download and open the files to determine what the image portrayed. ER:163. He needed more information than the private search provided. And in obtaining that information, he exceeded the

scope of Google's automated hash review, and violated the Fourth Amendment. *See Arizona v. Hicks*, 480 U.S. 321, 325 (1987) (merely moving a record player a few inches to reveal the serial number "produce[s] a new invasion of [] privacy" because it "expose[s] to view concealed portions of . . . its contents.").

a. *Walter* controls.

Indeed, what happened here is not materially different than *Walter*. Just like the labels in *Walter*, the information provided by Google's hash review told Agent Thompson what the files likely were, but did not reveal the images. 447 U.S. at 657. And, as in *Walter*, Agent Thompson had no evidence that the person who hash-marked the files as child pornography was any more qualified to do so than whoever marked the film canisters with labels indicating they were pornography.

The government tries to distinguish *Walter*, claiming, "Google saw and described what the images depicted." GB:14. Not so. No Google employee opened the image files attached to Mr. Wilson's email. And that is what matters.

Walter proves this point. Surely someone, at some time, viewed a copy of the obscene films before they were placed in the mail. Yet the government could not rely on that unrelated private act. The Supreme Court was concerned only with whether a private employee had viewed the films in *that package*. *Walter,* 447 U.S. at 656-57. Here, for the same reason, whatever some unknown Google employee may have done at some other time with some other person's account is irrelevant.

b. *Jacobsen* is inapposite.

Nor is this case like *Jacobsen*. The private employees there conducted the full-blown search of the package by removing the contents and finding (viewing) the cocaine. Immediately after, the officers repeated the identical search, adding only the non-intrusive field test. That is why there was no Fourth Amendment violation. *Jacobsen*, 446 U.S. at 126 ("the federal agents did not infringe any constitutionally protected privacy interest that had not already been frustrated as the result of private conduct.").

Here, in contrast, because Agent Thompson was the first person to view the closed files Mr. Wilson's emailed, this case is the inverse of *Jacobsen*. Google performed the limited, non-invasive scan, which the government then expanded by opening the files.[6]

A comparable scenario would be if FedEx used automated technology to identify cocaine inside a package without opening it. Using that technology, FedEx detected such a package, which it turned over to the FBI. Without a warrant, the FBI opened the package, confirming it contained cocaine. Plainly, that search would be unconstitutional. *See id.* at 120 n.17 ("we do not '[sanction] warrantless searches

[6] The fact that the government opened a copy of the file, rather than the original file attached to Mr. Wilson's email is of no consequence, any more than it would have mattered if the government had cloned the smart-phone in *Riley* and then examined the contents of the copy.

of closed or covered containers or packages whenever probable cause exists as a result of a prior private search.'").

To this end, as noted, the "virtual certainty" in *Jacobsen* stemmed from the fact that the private party and the officers were staring at a chunk of cocaine, which the private party had already revealed by opening the package. *Id*. at 111. Thus, while "no Fourth Amendment interest is implicated [when] the police have done no more than fail to avert their eyes," here, Agent Thompson's conduct went much further. *Id.* at 130 (White, J., concurring).

c. *Keith*'s analysis is compelling.

Keith provides an excellent analysis of this issue. The court explained: "[a]n argument that *Jacobsen* is factually similar to this case is untenable in light of the [fact] . . . that [Google] forwarded the suspect file only because its hash value matched a stored hash value, not because some [Google] employee had opened the file and viewed the contents. The [government] expanded the review by opening the file and viewing (and evaluating) its contents. *Walter*, and not *Jacobsen*, is the better analog." *Keith*, 980 F. Supp.2d at 42-43.

While the government tries to distinguish *Keith*, its arguments are unavailing. It claims: (1) "[t]he service provider in that case did not classify or describe the contents of the file in its report to NCMEC, and did not know 'how the file came to be originally hashed and added to [its] database,'" and (2) "*Keith* suggests the

outcome would have been different with the hash match if, like here, the record established an AOL employee or other private actor saw the original file's contents and identified child pornography." GB:15 (citation omitted).

But all CyberTipline reports to NCMEC typically contain industry classifications. ER:98. There is nothing to suggest the report in *Keith* was different. In any event, that classification is irrelevant. The reports in both this case and *Keith* stated the files matched suspected child pornography, without disclosing how, when, or by who that determination was made.

Moreover, *Keith* does not suggest the outcome would have been different if AOL employees saw an identical image belonging to someone else at some other time in an account unrelated to Mr. Keith. In fact, it says the opposite: "a [hash] match alone indicts a file as contraband but cannot alone convict it. That is surely why a[n] [agent] opens the file to view it, because the actual viewing of the contents provides information additional to the information provided by the hash match. This is unlike what the Court found the case to be in *Jacobsen*, where the subsequent DEA search provided no more information than had already been exposed by the initial FedEx search. *Jacobsen* is inapposite." 980 F. Supp.2d at 43.

d. *Reddick* is distinguishable and should not be followed.

Finally, as with *Jacobsen*, the government's reliance on *Reddick* is misplaced.

First, *Reddick* was wrongly decided. Its cursory analysis ignores the fact that when a government agent downloads, opens, and views an image file for the first time, he or she significantly expands on the automated hash review.

Second, the issues presented in *Reddick* were different. MJN:10. Absent from that opening brief was any argument about whether the search violated the Fourth Amendment in the first instance. As such, the Fifth Circuit decided the case on an issue that was not fully litigated.

Third, even when that appellant touched on the threshold search issue in his reply brief, he never raised, and the court never ruled on, any property-based argument. Thus, *Reddick* has nothing to say about that aspect of Mr. Wilson's claim. *See Webster v. Fall*, 266 U.S. 507, 511 (1925) ("Questions which merely lurk in the record, neither brought to the attention of the court nor ruled upon, are not to be considered as having been so decided as to constitute precedents.").

Fourth, *Reddick* did not involve files sent via email. It involved a "cloud hosting service." 900 F.3d at 637. This takes *Reddick* outside of the mail framework on which *Ex parte Jackson* and *Walter* relied, and on which Mr. Wilson's argument partially rests.

Fifth, the database in *Reddick* was different: "When [the] Detective [] first received Reddick's files, he already knew that their hash values matched the hash values of child pornography images *known to NCMEC*." *Id.* at 639 (emphasis

added). Given that NCMEC acts as an arm of the government and that PhotoDNA was developed for NCMEC, it was as if the government had already internally confirmed the image was contraband. *See United States v. Ackerman*, 831 F.3d 1292 1297, (10th Cir. 2016); EPIC at 16. But Google does not use PhotoDNA, and has its own private database apart from NCMEC's. GB:16.

For all these reasons, this Court should not follow *Reddick*. The Fourth Amendment implications at issue are too important to follow the Fifth Circuit's mislaid path. *See Woods*, 722 F.3d at 1183 n.8. Instead, consistent with *Walter*, and in light of the paucity of evidence as to Google actions in this case, the Court should hold that the private search doctrine does not excuse Agent Thompson's warrantless search of Mr. Wilson's emailed files.

D. The private search doctrine does not apply.

There is also a simpler route to this result. The Court can and should hold that, as a matter of law, the private search doctrine does not apply to Fourth Amendment property claims and/or email hashing.

1. The doctrine has no impact on Mr. Wilson's property-rights claim.

As explained in the opening brief, email is property for Fourth Amendment purposes. *See Ex parte Jackson*, 96 U.S. 727, 733 (1877) ("[l]etters and sealed packages" fall within "[t]he constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures."); *United States*

v. Cotterman, 709 F.3d 952, 964 (9th Cir. 2013) (en banc) ("[email] implicates the Fourth Amendment's specific guarantee of the people's right to be secure in their 'papers.'"). But the private search doctrine is an exception to the warrant requirement only under the *Katz*-privacy rubric. *See You've Got Mail!* at 665 ("the applicability of the private search doctrine [is limited] to *Katz*-based reasonable-expectation-of-privacy searches."). Its justification is that the private party frustrates the sender's reasonable expectation of privacy by exposing the object of the search and "[o]nce 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.

a. The private search rationale does not extend to property-based arguments.

This reasoning does not hold in the property-rights context. *See Ackerman*, 831 F.3d at 1307-08. An individual's property interest remains unaffected by the frustration of his or her privacy interest. *You've Got Mail!* at 665 ("a person's property rights are not eroded when a private party searches (i.e., trespasses) the property.").

This is so even when the owner cedes possession of his or her property to the third party. At most, that creates a bailment. *United States v. Alcaraz-Garcia*, 79 F.3d 769, 774 n.11 (9th Cir. 1996) ("A bailment is the deposit of personal property

with another"). And "a bailment does not alter the bailor's title interest in the bailed property; moreover, a bailor may assert title against any third person to whom the property has been transferred." *Id*. at 775 (citation omitted). Thus, there is no room for a private search exception in the *Jones*-type property analysis. *See You've Got Mail!* at 654 (a "prior private party search becomes irrelevant under a *Jones* trespass-to-chattels analysis").

The government disputes this point, arguing "the [private search] exception started with *Burdeau*, when the Fourth Amendment focus was trespass on property." GB:25 (citation omitted). But that was a *seizure*, not a *search*, decision. *Burdeau v. McDowell,* 256 U.S. 465, 470 (1921). It arose from a petition for return of stolen documents. The Supreme Court's sole point was that, because the government did not participate in the theft, it did not have to return the papers. *See id*. at 476. There was no separate discussion of how to treat a subsequent search by government agents.

That came only later in *Walter* and *Jacobsen*. As the government concedes, and this Court has noted, both of those decisions relied solely on a frustration of privacy rationale. GB:25; *United States v. Tosti*, 733 F.3d 816, 821-23 (9th Cir. 2013). Their language controls. And no precedent decided after *Jones* reintroduced the property rubric holds that a private search can defeat the defendant's Fourth Amendment *property* interest vis-à-vis the government.

The government, therefore, tries a different approach. It claims the premise of "the private search exception is assumption of risk . . . . when a property owner gives another complete or partial control over his papers, effects, or home[,] [t]he owner assumes the risk the third party might frustrate the owner's ordinary ability to physically exclude others from his property—the right protected by the property rights side of the Fourth Amendment." GB:26.

This is wrong. As noted, the doctrine is based on privacy frustration, not assumption of risk. Moreover, the government's theory fails under its own weight.

Millions of people trust their data to private companies. By the government's logic, they have *no* Fourth Amendment protection for that data because, by giving the companies "complete or partial control" of their data, they assumed the risk the company will provide it to the government. This is not a hyperbolic example. It is one the government endorses. GB:26 (Mr. Wilson "did not just assume the risk Google might 'communicate' or 'distribute' his uploaded files to the authorities[,] [he] authorized Google to do it.").

But no decision has ever approved such an expansive view of the government's ability to piggyback on private action. *See*, *e.g.*, *Carpenter v. United States,* 138 S. Ct. 2206, 2217 (2018) ("the fact that [] information is held by a third party does not by itself overcome the user's claim to Fourth Amendment

protection."). Were it otherwise, the private search and third party exceptions would swallow the Fourth Amendment.

They do not. Even when private conduct exposes personal information, property rights remain intact and prevent the warrantless trespass. Thus, the private search rationale does not apply to, and cannot overcome, Mr. Wilson's property rights.

b. Mr. Wilson's emailed files were his property.

The government, therefore, seeks to skirt Mr. Wilson's property claim by persisting with a fanciful distinction between email and email-attachments. GB:8 ("The agent looked at . . . files Wilson uploaded as attachments to his account. He did not look at emails before obtaining a warrant."). It concedes the former are property under the Fourth Amendment, but not the latter. This is incorrect.

An email is like an envelope: it can contain a message (a letter) as well as other enclosures (pictures, health records, etc.). *See Ackerman*, 831 F.3d at 1304 ("an email is a 'paper' or 'effect' . . . capable of storing all sorts of private and personal details, from correspondence to images, video or audio files, and so much more."). For Fourth Amendment purposes there is no difference between the letter and its enclosures. *See Ex parte Jackson*, 96 U.S. at 733.

The government's back up argument is also mistaken. It says: "the agent looked at *copies* of Wilson's files which might not be Wilson's papers or effects."

GB:8. The theory is that the "copies" of files are not property because "the 'original' bits or ones and zeroes making up the files stayed in Wilson's email account." GB:24. This is an irrelevant distinction.

There is no rule that the Constitution only protects originals. *See You've Got Mail!* at 672 ("An individual's copied data on a government-owned hard disk drive is still property of the individual under the data-rights theory."). Indeed, sent "images, video or audio files, and [other attachments]" are part of the "email," thus constitutionally protected as part of the sender's papers and effects. *Ackerman*, 831 F.3d at 1304; *see Joffe v. Google, Inc.*, 746 F.3d 920, 931 (9th Cir. 2013) ("sent" "email attachment[s]" are protected).

Google itself makes the same point: "'Google does not claim any ownership in any of the content . . . that [users] upload, transmit or store in [their] Gmail account.'" *In re Google Inc.*, 2014 U.S. Dist. LEXIS 36957, *16 n.4 (N.D. Cal. 2014).

Thus, no one had a superior interest in Mr. Wilson's emailed files. They remained his property under the Fourth Amendment.[7] When Agent Thompson opened them, this was a trespass no different than opening Mr. Wilson's private mail and looking at the pictures inside. *See You've Got Mail!* at 677 ("Regardless of

[7] The government's copyright reference is similarly misplaced. GB:24. If a person is gifted a print of a painting, she has no copyright, but the print is hers.

where the data was accessed, a trespass occurred the moment [the government] opened [email] files without a warrant. The 'chattel' that is trespassed is the data, not the electronic device where the data is stored."). It was "exactly the type of trespass to chattels that the framers sought to prevent when they adopted the Fourth Amendment." *Ackerman*, 831 F.3d at 1307; *You've Got Mail!* at 679 ("opening a previously-closed file triggers a unique Fourth Amendment search in the absence of a warrant."). Accordingly, private search or not, the search was unconstitutional.

2. The private search doctrine is not triggered by Google's hash screening.

a. Google's hashing is not constitutionally different than a dog-sniff.

The private search doctrine is also inapplicable for another reason. Hash matching does not frustrate a reasonable expectation of privacy. Rather, it serves as a technological dog-sniff, identifying the presence of suspected contraband without opening the package (email). *See United States v. Place*, 462 U.S. 696, 707 (1983) ("'a canine sniff'. . . . does not expose noncontraband items that otherwise would remain hidden from public view.").

The government offers several responses. First, it disputes the proposition that the exception requires the private actor to have "acted in a way that infringed a reasonable expectation of privacy," and claims such a rule "produces strange results." GB:20. Second, it argues a hash match is not like a technological dog-sniff

because "[a] hash match identifies the exact content and in that way is a high-definition, full-color view of the inside." GB:21-22. Both arguments are mistaken.

As *Jacobsen* makes clear, the private party's conduct *must* in fact "frustrate[] the original expectation of privacy." 466 U.S. at 117, 126. Nor does this rule produce strange results. Even in the government's computer repairman scenario, regardless of consent, the act of "stumbling" upon the hidden image files frustrated the owner's expectation of privacy. GB:20-21. That is precisely what the Court held in *Tosti*, 733 F.3d at 821. The repairman's "prior viewing of the images had extinguished Tosti's reasonable expectation of privacy in them." *Id*.

The government is also misguided in suggesting a hash match is unlike a dog-sniff because it reveals a high definition view of the file's content. It does nothing of the sort. *See Keith*, 980 F. Supp.2d at 43. The hashed files remain closed and unseen. Accordingly, because a hash match cannot frustrate an individual's expectation of privacy in closed image files, it cannot serve as a basis to apply the private search exception.

b. The doctrine does not apply to automated hashing.

This is equally true due to the absence of human participation in the hash matching and reporting process. Only a human can violate another human's privacy – dogs don't read diaries. Thus, if no human knows what the computer found, there is no privacy frustration.

The government's only retort is that "Wilson does not offer authority for this view which is not universal." GB:22. But it is not Mr. Wilson's burden. And the government offers no case where this Court or the Supreme Court has ever applied the doctrine to a purely machine search.

3. The Court should not extend the doctrine to email.

To the extent any doubt remains as to the doctrine's inapplicability, *Riley v. California*, 134 S. Ct. 2473 (2014), and *Carpenter* provide further support. In both, the Supreme Court declined to extend established Fourth Amendment exceptions to technological innovations: "When confronting new concerns wrought by digital technology, this Court has been careful not to uncritically extend existing precedents." *Carpenter*, 138 S. Ct. at 2222.

The government responds: (1) there is an insufficient policy justification to exclude "NCMEC referrals" from the private search exception and (2) "[t]he usual requirement of a warrant is a problem in this scenario because of the breadth of the issue." GB:30.

As to the first contention, it relies on a false premise – that the line is drawn at NCMEC referrals. Nothing about the government's private search argument is so limited: "The type of reviewed material does not change [the analysis]." GB:28. According to the government, all data "uploaded [] to the servers of a corporation

[Google] that famously scans and mines all its users' content," is fair game under the private search doctrine. GB:28.

Under this rationale, the billions of emails and documents passing through the servers of Google, Facebook, etc., are open to inspection by law enforcement simply because the company happens to scan them for legitimate business reasons. Thus, while paying lip service to NCMEC referrals, its actual argument sweeps far beyond.

On the other side of the equation, an exception to the warrant requirement is not "needed for the promotion of legitimate governmental interests." *Riley*, 134 S. Ct. at 2484. There was nothing preventing Agent Thompson (or any other agent) from seeking a warrant before opening the image files. The government, therefore, invents an impediment.

It says there were "18.4 million [NCMEC referrals] in 2018." GB:30. But this is misleading. Those referrals "include reports of child pornography images, online enticement, child sex trafficking, and child molestation." GB:30. There is no evidence as to what percent come from emails, which have established Fourth Amendment protection. Moreover, given that there are nowhere near 18 million prosecutions per year, the statistic suggests that most NCMEC referrals do not pan out, which further undermines the government's reliability claim.

Finally, the government claims there is no point enforcing a warrant requirement when it comes to NCMEC referrals because "[a] court would be in no

position to challenge the description of the image (it cannot look at it) or the provider's belief in hashing's reliability." GB:32. Not so. This Court has held judges *should* examine the seized images of child pornography before authorizing a search warrant. *See United States v. Perkins*, 850 F.3d 1109, 1118 (9th Cir. 2017) ("Agent [] was required to provide copies of the images for the magistrate's independent review."). In cases with NCMEC referrals, there is nothing preventing an agent from submitting a warrant application with unopened image files for *in camera* review.

Anyway, the Supreme Court has already answered the government's policy argument: "We cannot deny that our decision today will have an impact on the ability of law enforcement to combat crime . . . . Privacy comes at a cost . . . . Our cases have historically recognized that the warrant requirement is 'an important working part of our machinery of government,' not merely 'an inconvenience to be somehow weighed against the claims of police efficiency.'" *Riley*, 134 S. Ct. at 2494. Thus, as a matter of first impression, the Court should not extend the private search doctrine to emailed files.

In the final analysis, the district court's reflection rings true: "I have little doubt that at some point in the future, given artificial intelligence and the capabilities of artificial intelligence, the ruling that [I] issued will not be one that is recognized

as being correct." ER:356. This Court should reverse the denial of Mr. Wilson's suppression motion, and vacate his convictions.[8]

II.
JURY WAIVER

The district court structurally erred in failing to obtain a written jury waiver. Binding precedent forecloses the government's argument that plain error review applies. *See United States v. Shorty*, 741 F.3d 961, 965 (9th Cir. 2013) ("We review the adequacy of a jury-trial waiver de novo.").

The government is also wrong on the merits. "[D]istrict courts [must] ensure that a jury trial waiver is knowing and intelligent by engaging in a substantial colloquy with defendants as well as informing them of four crucial facts: (1) twelve members of the community compose a jury; (2) the defendant may take part in jury selection; (3) jury verdicts must be unanimous; and (4) the court alone decides guilt or innocence if the defendant waives a jury trial." *Id.* at 966.

Here, that did not happen. The court told Mr. Wilson, "it would be required that all 12 jurors find you guilty." ER:219. This partially covered fact 1 and fact 3 (the number of jurors and unanimity). However, the court did not explain that jurors come from his "community" (fact 1); that he could help choose the jury (fact 2); or

[8] By failing to argue the good faith exception or that the terms of service impact the analysis, the government has waived these claims. *See United States v. Gamboa-Cardenas*, 508 F.3d 491, 502 (9th Cir. 2007).

the court alone decides guilt or innocence if he waived a jury trial (fact 4). Adding confusion, the court addressed the jury-waiver colloquy in the same breath as evidentiary stipulations. ER:219.

The government claims these shortfalls are irrelevant because "the bar is lower for an 'intellectually sophisticated and highly educated,' defendant like Wilson." GB:37 (citation omitted). This is a stretch.

Mr. Wilson was a young man working as a mid-level manager for an energy drink company. PSR:21. He was not at the sophistication level of a "practicing attorney," "securities broker," or "professor with a doctorate," as in the government's citations. GB:37-38. He did not have a graduate degree. He had no experience with the criminal justice system, and no basis to know the extent of his jury rights. PSR:17. Further, he is a Canadian citizen, raised in Canada, unfamiliar with American criminal procedure. PSR:3, 19.

Thus, the government's argument collapses with its sophistication premise. This Court should remand for a new trial.

Respectfully submitted,

s/ Devin Burstein

Dated: August 12, 2019

Devin Burstein
Warren & Burstein

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

Form 8. Certificate of Compliance for Briefs

Instructions for this form: http://www.ca9.uscourts.gov/forms/form08instructions.pdf

9th Cir. Case Number(s) 18-50440

I am the attorney or self-represented party.

This brief contains 6,991 words, excluding the items exempted by Fed. R. App. P. 32(f). The brief's type size and typeface comply with Fed. R. App. P. 32(a)(5) and (6).

I certify that this brief *(select only one)*:

[X] complies with the word limit of Cir. R. 32-1.

[ ] is a **cross-appeal** brief and complies with the word limit of Cir. R. 28.1-1.

[ ] is an **amicus** brief and complies with the word limit of Fed. R. App. P. 29(a)(5), Cir. R. 29-2(c)(2), or Cir. R. 29-2(c)(3).

[ ] is for a **death penalty** case and complies with the word limit of Cir. R. 32-4.

[ ] complies with the longer length limit permitted by Cir. R. 32-2(b) because *(select only one)*:
- [ ] it is a joint brief submitted by separately represented parties;
- [ ] a party or parties are filing a single brief in response to multiple briefs; or
- [ ] a party or parties are filing a single brief in response to a longer joint brief.

[ ] complies with the length limit designated by court order dated _____.

[ ] is accompanied by a motion to file a longer brief pursuant to Cir. R. 32-2(a).

Signature *s/ Devin Burstein* **Date** 08/12/2019
(use "s/[typed name]" to sign electronically-filed documents)