Online Service Providers and the Fight Against Child Exploitation: The Fourth Amendment Agency Dilemma

*By Jeff Kosseff**

January 2021

The Fourth Amendment government agency problem requires platforms to walk a fine—and sometimes untenable—line in searching for private user content that contains child sex abuse material and other illegal material.

Public-facing platforms such as social media services can give law enforcement a direct view into illegal online activities, providing crucial evidence for criminal investigations and prosecutions. But not all online communications are open to the public. Before law enforcement can search the contents of emails, chat logs, and other private communications, the Fourth Amendment generally requires that they obtain a warrant supported by probable cause.[1]

What about the private companies that provide the services? Can't they automatically or manually search their users' private accounts for evidence of a crime and then share that information with the government? The answer to that question, from a Fourth Amendment perspective, is not always

* Assistant Professor, Cyber Science Department, U.S. Naval Academy. The views expressed are only those of the author and do not reflect the views of the Naval Academy, Department of Navy, or Department of Defense. The author was not compensated by outside parties for this paper.

[1] See *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010) ("Accordingly, we hold that a subscriber enjoys a reasonable expectation of privacy in the contents of emails that are stored with, or sent or received through, a commercial ISP." (internal quotation marks and citations omitted); *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 899 (9th Cir. 2008) (finding "a reasonable expectation of privacy in [users'] text messages as a matter of law").

easy, and it points to one of the most substantial barriers to public-private partnerships in investigating distributors of child sex abuse material and other illegal content.

The Fourth Amendment constrains the activities of government entities such as local, state, or federal law enforcement, and if those public entities violate the Fourth Amendment, the exclusionary rule may prevent evidence from being used against a criminal defendant at trial.[2] The Fourth Amendment, however, typically does not apply to the activities of a private company that is acting purely in its own interests and completely independent of the government. Moreover, under the *private search doctrine*, if a private party conducts a search and then provides that information to the government entity, the government entity's use of that information is not considered a Fourth Amendment search, provided that the government did not expand on the private party's search.[3]

But the inquiry does not end with a binary distinction between government entities and private parties. Private companies that scan or search for illegal user content do not always fit into one of these two categories. In between are private companies that might search for illegal content for a variety of reasons and might have some interactions with the government as they conduct their investigations. At a certain point, the law treats these companies as *government agents*, and the evidence they collect is subject to the same Fourth Amendment restrictions as if the evidence had been collected by government-run law enforcement agencies.

The point at which a private company becomes a government agent is often unclear. The government wants to be careful in how closely it works with online service providers, lest the companies be viewed as government agents. The consequences are severe: Any evidence obtained as a result of their searches could be suppressed, jeopardizing the future of a criminal prosecution for child sex abuse material or other serious crimes.

This paper examines the Fourth Amendment *government agent doctrine* in the context of child sex abuse material, a problem that many online service providers have invested great resources to combat even as they have faced criticism for not doing enough. The paper argues that the Fourth Amendment government agency problem requires platforms to walk a fine—and sometimes untenable—line in searching for private user content that contains child sex abuse material and other illegal material. Under the private search doctrine, platforms could reduce the chances of a subsequent government inspection of user content by reviewing it before sending it to law

[2] See *Mapp v. Ohio*, 367 U.S. 643, 651 (1961).
[3] See *United States v. Reddick*, 900 F.3d 636, 637 (5th Cir. 2018) ("Under the private search doctrine, the Fourth Amendment is not implicated where the government does not conduct the search itself, but only receives and utilizes information uncovered by a search conducted by a private party.").

enforcement. But if platforms work too closely with law enforcement, a court might view the platforms as government agents whose own searches are subject to the Fourth Amendment.

The opaque Fourth Amendment government agency standards pose a real problem for private-sector efforts to combat child sex abuse material. There is no easy solution, as the barriers come not from a statute that can be amended, but from decades of frequently gnomic court interpretations of the Fourth Amendment. This paper focuses in particular on the difficulty that platforms may have in avoiding the classification as a government agent while also gathering sufficient information for law enforcement.

FOURTH AMENDMENT GOVERNMENT AGENT DOCTRINE

Although the Supreme Court has addressed the issue of when private companies become agents of the government for Fourth Amendment purposes, it has not articulated a clear test. Perhaps the most important Supreme Court case on this point is *Skinner v. Railway Labor Executives' Association*.[4] This 1989 case involved labor groups' Fourth Amendment challenge to federal railroad regulations that "authorize[d] railroads to require covered employees to submit to breath or urine tests" after certain types of safety incidents, or if the railroad had "reasonable suspicion" of an employee being under the influence of alcohol.[5]

The initial question for the court in *Skinner* was whether the tests carried out under these regulations were subject to the Fourth Amendment. After all, the railroads were private companies, and the regulations allowed them to determine whether to carry out the searches. "Whether a private party should be deemed an agent or instrument of the Government for Fourth Amendment purposes necessarily turns on the degree of the Government's participation in the private party's activities," Justice Anthony Kennedy wrote for the majority.[6]

Kennedy wrote that a search is not outside of the Fourth Amendment merely because "the Government has not compelled a private party to perform a search."[7] Searches conducted under the railroad regulations at issue in *Skinner*, he wrote, were subject to the Fourth Amendment. The government "has removed all legal barriers to the testing," he wrote, and "indeed has made plain not only its strong preference for testing, but also its desire to share the fruits of such intrusions."[8] The government also "mandated the railroads not bargain away the authority to perform tests granted"

[4] *Skinner v. Railway Labor Executives' Association*, 489 U.S. 602 (1989).
[5] *Skinner*, at 611.
[6] *Skinner*, at 614.
[7] *Skinner*, at 615.
[8] *Skinner*, at 615.

by the regulations, he wrote. "These are clear indices of the Government's encouragement, endorsement, and participation, and suffice to implicate the Fourth Amendment."[9]

The *Skinner* opinion thus affirms that private parties can qualify as government agents for Fourth Amendment purposes, but the opinion provides little guidance for lower courts as to how to make this determination. The court did not explain what level of government encouragement, endorsement, and participation in a private search would bring the private entity's activity under the umbrella of the Fourth Amendment.

Although *Skinner* did not articulate a specific test for determining whether a private party is a government agent, lower courts have developed their own tests for government agency, based on cases that were decided years before *Skinner*. The tests often can be traced back to *United States v. Walther*,[10] a 1981 decision from the U.S. Court of Appeals for the Ninth Circuit.

Walther involved an airline employee who encountered a suspicious case that was taped closed. The employee opened the case to discover white powder, at which point he alerted Drug Enforcement Administration (DEA) agents.[11] The employee had previously served as a confidential DEA informant and received money for some of the information he had provided the government over the years. The DEA agents tested the substance, confirmed that it was cocaine, and arrested Karyn Walther, who claimed the luggage at the airport.[12] After being indicted on drug-related charges, Walther convinced the district court to suppress the evidence, with the court ruling that the airline employee was a government agent for Fourth Amendment purposes.[13]

The Ninth Circuit affirmed the district court's decision to suppress the evidence, agreeing that the airline employee was a government agent. The court stated that two "critical factors" for government agent analysis are "(1) the government's knowledge and acquiescence, and (2) the intent of the party performing the search,"[14] in other words, whether the private party intended to assist the government.

Applying these factors, the Ninth Circuit concluded that the airline employee was a government agent. Although the court acknowledged that the government had "no prior knowledge that this particular search would be conducted" and "had not directly encouraged" the airline employee to search that particular luggage, "it had certainly encouraged" the employee "to engage in this type of

---

[9] *Skinner*, at 615–16.
[10] *United States v. Walther*, 652 F.2d 788 (9th Cir. 1981).
[11] *Walther*, at 790.
[12] *Walther*, at 790.
[13] *Walther*, at 791.
[14] *Walther*, at 792.

search."[15] Therefore, the court concluded, the government "had knowledge of a particular pattern of search activity dealing with a specific category of cargo, and had acquiesced in such activity."[16] Likewise, the second factor weighed in favor of a government agent finding, the court wrote, because the employee searched the luggage due to "his suspicion that it contained illegal drugs" and not for "legitimate business considerations such as prevention of fraudulent loss claims."[17]

The Ninth Circuit stressed the "narrowness" of the holding, which it wrote was due to the "finding of extensive contact" between the airline employee and the DEA and the employee's "motivation for opening the case." Yet these two factors would form the basis of the test that many other courts applied for years to come.[18] Some courts have expanded on the *Walther* test and added other factors. For instance, the U.S. Court of Appeals for the First Circuit has written that it does not adhere to a "specific 'standard' or 'test'" but, instead, considers the following factors: "the extent of the government's role in instigating or participating in the search, its intent and the degree of control it exercises over the search and the private party, and the extent to which the private party aims primarily to help the government or to serve its own interests."[19]

As I have argued previously, the *Walther* test is particularly difficult for courts (and private parties) to apply because of the focus on the private party's subjective intent.[20] Determining why a large online service provider has conducted a search is difficult, if not impossible, particularly because corporate decisions are made by many employees who might have different motivations. Even if we were to ascertain a company's motivations, the company might have many different reasons, some related to law enforcement and others related to business reasons. I proposed replacing the *Walther* test with an approach by which a court "should conclude that the private party was an agent or instrument of the government only if it determines that the government exercised substantial

---

[15] *Walther*, at 793.

[16] *Walther*, at 793.

[17] *Walther*, at 792.

[18] See, e.g., *United States v. Steiger*, 318 F.3d 1039, 1045 (11th Cir. 2003) ("For a private person to be considered an agent of the government, we look to two critical factors: (1) whether the government knew of and acquiesced in the intrusive conduct, and (2) whether the private actor's purpose was to assist law enforcement efforts rather than to further his own ends."); *United States v. Paige*, 136 F.3d 1012, 1017-18 (5th Cir. 1998) ("There is no indication from the record (1) that the government knew of or acquiesced in the intrusive conduct of Willard and Windell, and (2) that Willard and Windell intended to assist law enforcement efforts in conducting their search.").

[19] *United States v. Pervaz*, 118 F.3d 1, 6 (1st Cir. 1997).

[20] Jeff Kosseff, "Private Computer Searches and the Fourth Amendment," 14 *I/S: A Journal of Law and Policy for the Information Society* (2018) ("In addition to the inconsistencies with Fourth Amendment precedent and theory, the prevailing circuit court tests for Fourth Amendment agency are difficult to apply. The focus on subjective intent often leads to inconsistent and unpredictable results.").

control over the search" and that this finding should be "based on an objective evaluation of the actions of the government."[21] In particular, such a revision to Fourth Amendment government agent framework would be particularly useful in child sex abuse material cases.

APPLYING THE GOVERNMENT AGENT FRAMEWORK TO EFFORTS TO DETECT CHILD SEX ABUSE MATERIAL

The courts' continued reliance on a partly subjective government agent framework has caused uncertainty for online service providers' efforts to combat child sex abuse material. Over the past decade, courts increasingly have scrutinized systems that have detected illegal material and led to the prosecution of people who distributed child sex abuse material.

To examine the Fourth Amendment pitfalls of private child sex abuse material investigations, it first is necessary to understand online service providers' reporting obligations. If an online service provider obtains "actual knowledge" of an "apparent violation" of federal child sex abuse material laws on its services, the provider "as soon as reasonably possible" must file a CyberTipline report with the National Center for Missing & Exploited Children (NCMEC), a nonprofit.[22] The report may include user information, information about the suspected illegal content, information about the user's location, the apparent child sex abuse material, and the communication at issue.[23] If a provider knowingly and willfully fails to report, it is subject to a fine of up to $150,000 for the first violation, and up to $300,000 for a subsequent violation.[24] The NCMEC forwards the CyberTipline report to federal, state, or local law enforcement.[25] Federal law limits the online service providers' liability for participation in the reporting program only to misconduct that is intentional or reckless.[26] The NCMEC also may provide elements from CyberTipline reports, such as hash values, to online service providers "for the sole and exclusive purpose of permitting that provider to stop the online sexual exploitation of children."[27]

The mandatory reporting statute states explicitly that online service providers are not required to monitor their users.[28] Yet for their own business reasons, many email and cloud storage providers

---

[21] Kosseff, "Private Computer Searches and the Fourth Amendment," 221.
[22] 18 U.S.C. § 2258A(a). The Stored Communications Act explicitly allows providers to disclose the contents of communications to the NCMEC in CyberTipline reports. See 18 U.S.C. § 2702(b)(6).
[23] 18 U.S.C. § 2258A(b).
[24] 18 U.S.C. § 2258A(e).
[25] 18 U.S.C. § 2258A(c).
[26] 18 U.S.C. § 2258B.
[27] 18 U.S.C. § 2258C.
[28] 18 U.S.C. § 2258(f).

use programs such as PhotoDNA, which "automatically scan the hash values of user-uploaded files and compare them against the hash values of known images of child pornography."[29] If PhotoDNA or a similar program detects a match, the online service provider then has actual knowledge of an apparent legal violation and is obligated to file a CyberTipline report with the NCMEC.[30]

The first high-profile and successful challenge to this system came in a 2013 case in Massachusetts federal district court. In *United States v. Keith*, the defendant was charged with child sex abuse material–related crimes that were supported partly by evidence collected based on AOL's automated scan of the defendant's email account. AOL did not review the flagged email attachments but, rather, transmitted them in a CyberTipline report to the NCMEC, which reviewed the files and provided a report to law enforcement.[31]

The defendant moved to suppress the evidence, arguing that both AOL and the NCMEC were government agents. Applying the First Circuit's government agency factors, the court first concluded that AOL was not a government agent for Fourth Amendment purposes. Central to the court's ruling was its conclusion that "AOL is motivated by its own wholly private interests in seeking to detect and deter the transmission of child pornography through its network facilities."[32] The court relied in part on an AOL representative's testimony that "providing a safer, more family-friendly environment for our users sustains our ability to keep our members."[33] The court also noted that "AOL is not required by law to monitor email traffic for possible child pornography, but only to report it when it is found."[34]

But the NCMEC, the court concluded, was a government agent. Unlike AOL's mere scanning, the NCMEC's review of the images "was a search conducted for the sole purpose of assisting the prosecution of child pornography crimes," the court wrote.[35] The NCMEC's CyberTipline, the court wrote, "is intended to, and does, serve the public interest in crime prevention and prosecution, rather than a private interest."[36] The court also focused on the government's control of the NCMEC's

---

[29] *Reddick*, 900 F.3d at 638. "Hash values are short, distinctive identifiers that enable computer users to quickly compare the contents of one file to another. They allow investigators to identify suspect material from enormous masses of online data, through the use of specialized software programs — and to do so rapidly and automatically, without the need for human searchers." *Id.* at 636-37.
[30] *Reddick*, at 638.
[31] *United States v. Keith*, 980 F. Supp. 2d 33, 37–38 (D. Mass. 2013).
[32] *Keith*, at 40.
[33] *Keith*, at 40.
[34] *Keith*, at 40 (internal quotations omitted).
[35] *Keith*, at 41.
[36] *Keith*, at 41.

operations, including through congressional funding and authorization. "A statutory provision requires NCMEC to report discovered child pornography to federal law enforcement, and another encourages similar reporting to state and foreign law enforcement agencies," the court wrote.[37]

The *Keith* case provided at least some guidelines for establishing programs that search private content for child sex abuse material. An online service provider seeking to help the government should strive to fall into AOL's nonagent category by distancing itself from any government instigation of or control over its search. And it should carefully justify its efforts with reasoning that is separate from assisting law enforcement. Likewise, the government should ensure that its anti–child sex abuse material efforts are sufficiently distanced from those of the providers and that the government does not exercise any control over the providers' efforts.

This dilemma points to a larger problem with the government agent doctrine in child sex abuse material cases: How can a court fairly determine the subjective intent of a large company like Google or AOL? Online service providers may have a number of motivations to use hash scanning to detect child sex abuse material, both to protect their business interests *and* to assist law enforcement. These decisions are not made by one individual who has one goal, but by a wide range of internal stakeholders who have many different motivations. A more equitable and predictable method of determining whether an online service provider is a government agent is to focus on whether law enforcement requested, assisted in, or supervised the hash scanning. Unfortunately, the courts continue to rely on variations of the two-pronged *Walther* framework, so subjective intent continues to be an important factor in determining whether an online service provider is a government agent.

THE PRIVATE SEARCH DOCTRINE AND ONLINE SERVICE PROVIDERS

Even if an online service provider manages to avoid the "government agent" designation, the evidence still might be suppressed if the review of the material by the NCMEC or law enforcement is separately considered to be a search. This brings into play another unpredictable Fourth Amendment rule: the private search doctrine.[38]

The doctrine was articulated most clearly in a 1984 Supreme Court opinion, *United States v. Jacobsen*,[39] which involved Federal Express employees' inspection of an apparently damaged

[37] *Keith*, at 41.
[38] See Taylor J. Pfingst, "Digitizing the Private Search Doctrine: Is a Computer a Container," *Hastings Constitutional Law Quarterly* 44 (2017): 371.
[39] *United States v. Jacobsen*, 466 U.S. 109 (1984).

package—a process required by the company's insurance policy. After opening the inner package, they discovered plastic bags containing white powder.[40] The employees alerted the DEA, which physically inspected the package, tested the powder, and determined that it was cocaine.[41] The Supreme Court held that the agent's viewing of the materials in the package did not violate the Fourth Amendment. The defendants "could have no privacy interest in the contents of the package, since it remained unsealed and since the Federal Express employees had just examined the package and had, of their own accord, invited the federal agent to their offices for the express purpose of viewing its contents."[42]

The court also concluded that the test of the powder was not a Fourth Amendment search, as it "merely discloses whether or not a particular substance is cocaine" and "does not compromise any legitimate interest in privacy."[43] This second holding, regarding the powder testing, was justified under what is sometimes known as the *binary search doctrine*, which the Supreme Court the previous year had used to uphold a canine sniff of luggage because "the sniff discloses only the presence or absence of narcotics, a contraband item."[44]

---

[40] *Jacobsen*, at 111.
[41] *Jacobsen*, at 111–12.
[42] *Jacobsen*, at 119.
[43] *Jacobsen*, at 123.
[44] *United States v. Place,* 462 U.S. 696, 707 (1983). It is tempting to justify hash scanning under the binary search doctrine. Even if an online service provider were considered to be a government agent, could it still withstand a Fourth Amendment challenge under the binary search doctrine? Such an argument is far from certain to prevail in court. The question of whether online service providers' hash scanning qualifies for the binary search doctrine was recently addressed in an excellent student note by Denae Kassotis. After reviewing the history of the binary search doctrine and cases involving hash scanning, Kassotis aptly distinguishes hash scanning from the earlier cases involving dog sniffs and cocaine powder tests. "Hash-value matching is qualitatively different from other types of binary authentication, such as canine sniffs and spot tests. Other types of binary authentication methods are conducted after the government has an articulable suspicion of criminal wrongdoing. Alternatively, every internet communication is hashed, without any suspicion. Second, hashing is conducted by a private entity, at no cost to the government." Denae Kassotis, "The Fourth Amendment and Technological Exceptionalism After Carpenter: A Case Study on Hash-Value Matching," *Fordham Intell. Prop. Media & Ent. L.J.* 29 (2019): 1243, 1313. Kassotis further notes that, under the analytical framework of *Carpenter v. United States*, 138 S.Ct. 2206 (2018), if technology such as hash scanning is exceptional, "courts should decline to analogize hashing to pre-digital technologies, and instead employ a holistic analysis of hashing's functional and non-functional attributes when assessing its fit within established doctrine." *Id.* at 1308. Kassotis's assessment of hash-scanning is compelling, and counsels against assuming that an online service that is deemed a government agent could rely on the binary search doctrine to avoid running afoul of the Fourth Amendment.

As applied to child sex abuse material detection programs, the private search doctrine suggests that online service providers might reduce the chance of evidence suppression by fully reviewing flagged files before passing them along to the NCMEC. In the *Keith* case described above, after concluding that the NCMEC was a government agent, the court rejected the applicability of *Jacobsen* because "matching the hash value of a file to a stored hash value is not the virtual equivalent of viewing the contents of the file."[45] Conversely, in *United States v. Drivdahl*, a 2015 case involving suspected child sex abuse material flagged by Google, one of the defendant's arguments was that even if Google had conducted a private search, the NCMEC or law enforcement expanded on that private search by reviewing the files. The federal district court rejected this argument because "[p]art of Google's standard procedure involves a member of the Legal Removals Team opening each reported image to confirm that it appeared to meet the statutory definition of child pornography … prior to submitting a CyberTip report."[46] The judge explicitly distinguished Google's review process from the automated scanning in *Keith*.[47]

The incentive for online service providers to examine the files during a private search became even clearer in 2016, in a U.S. Court of Appeals for the Tenth Circuit opinion written by then-Judge Neil Gorsuch. In *United States v. Ackerman*, AOL's hash-matching program detected a child sex abuse material match on an image that was attached to the defendant's email. AOL filed a CyberTipline report to the NCMEC, attaching the email and the four images. The NCMEC viewed not only the flagged image but also three other images attached to the email, determined that all of the images were apparent child sex abuse material, and contacted law enforcement.[48]

Gorsuch concluded that the NCMEC was *both* a governmental entity and, in the alternative, a government agent, bringing its actions within the scope of the Fourth Amendment. The NCMEC is a government entity, he wrote, due to the many statutory requirements for it to combat child sex abuse material, as well as its federal funding. "That an entity might be incorporated, as NCMEC is, doesn't prevent it from also qualifying as a governmental entity: the dispositive question isn't one of

---

[45] *Keith*, 980 F.Supp.2d at 43 ("What the match says is that the two files are identical; it does not itself convey any information about the contents of the file. It does say that the suspect file is identical to a file that someone, sometime, identified as containing child pornography, but the provenance of that designation is unknown. So a match alone indicts a file as contraband but cannot alone convict it.").
[46] *United States v. Drivdahl*, No. CR 13-18-H-DLC, (D. Mont. Mar. 6, 2014).
[47] *Drivdahl* ("Unlike in *United States v. Keith*, where AOL's internal process for discovering child pornography relied entirely on algorithmic 'hash value' information, the suspect material was opened by a Google employee prior to being turned over to the government. Thus, there was no expansion of the private search, which would have required a warrant.") (internal citation omitted).
[48] *United States v. Ackerman*, 831 F.3d 1292, 1294 (10th Cir. 2016).

form but function, turning on what the entity does, not how it is organized," Gorsuch wrote.[49] Alternatively, Gorsuch wrote, the NCMEC also is a government agent.[50]

The government attempted to prevent the evidence from being suppressed by relying on the private search doctrine. The government argued that the NCMEC merely reviewed emails that already were the subject of a private search by AOL. Gorsuch rejected this attempt, concluding that the NCMEC expanded on AOL's search. "Yes, AOL ran a search that suggested a hash value match between one attachment to Mr. Ackerman's email and an image AOL employees had previously identified as child pornography," Gorsuch wrote. "But AOL never opened the email itself. Only NCMEC did that, and in at least this way exceeded rather than repeated AOL's private search."[51]

Unlike the chemical test in *Jacobsen*, the NCMEC's review of the email disclosed a private fact that would not otherwise have been known, Gorsuch wrote. "Indeed, when NCMEC opened Mr. Ackerman's email it could have learned any number of private and protected facts, for (again) no one before us disputes that an email is a virtual container, capable of storing all sorts of private and personal details, from correspondence to other private (and perfectly legal) images, video or audio files, and beyond," he wrote.[52]

Gorsuch emphasized that he was not deciding whether the result would have been the same had the NCMEC accessed only the single image that had been flagged by AOL's automated program, and not the email message or the other three images. "Could the government have argued that, in *that* case, NCMEC's actions didn't risk exposing any private information beyond what AOL had already reported to it?" Gorsuch asked. "Or might even that have risked exposing new and protected information, maybe because the hash value match could have proven mistaken (unlikely if not impossible) or because the AOL employee who identified the original image as child pornography was mistaken in his assessment (unlikely if maybe more possible)?"[53]

The court, Gorsuch wrote, did not need to resolve that question "because the undisputed facts before us indicate that NCMEC opened Mr. Ackerman's email first and did so before and in order to view not just the attachment that was the target of AOL's private search but three others as well." "And as we've seen," Gorsuch concluded, "each of these steps—opening the email and viewing the

---

[49] *Ackerman,* at 1295.
[50] *Ackerman,* at 1300 ("Even if we are wrong and NCMEC isn't a governmental entity, that doesn't necessarily mean its searches escape the Fourth Amendment's ambit. After all, since time out of mind the law has prevented agents from exercising powers their principals do not possess and so cannot delegate.").
[51] *Ackerman,* at 1305–06.
[52] *Ackerman,* at 1306.
[53] *Ackerman,* at 1306.

three other attachments—was enough to risk exposing private, noncontraband information that AOL had not previously examined."[54]

It is unclear how far the *Ackerman* holding extends; two years later, in *United States v. Reddick*, the U.S. Court of Appeals for the Fifth Circuit held that law enforcement did not expand the private search that took place when Microsoft's PhotoDNA program automatically flagged images on a customer's cloud account.[55] The Fifth Circuit distinguished the situation from *Ackerman*, where only one of the four images at issue had been automatically flagged by AOL. In contrast, the Fifth Circuit noted, law enforcement in *Reddick* "reviewed only those files whose hash values corresponded to the hash values of known child pornography images, as ascertained by the PhotoDNA program."[56]

Still, *Ackerman*, *Drivdahl*, and *Keith* suggest that evidence is less likely to be suppressed if online service providers reviewed it before providing it to the NCMEC, as the private search doctrine is more likely to apply. Evidence might be at a greater risk of suppression if the platforms provide the NCMEC with images that were automatically flagged as potential child sex abuse material but not reviewed by the company. And the evidence might be at even greater risk of suppression if only some of the files provided to the NCMEC were automatically flagged.

Indeed, the U.S. government stated in 2018 court filings that, in recent years, the NCMEC only views images that online service providers have viewed or that were available to the public.[57] If providers only detected an automated match but did not review the nonpublic image, the government wrote, the NCMEC will forward the image to law enforcement, which will then obtain a warrant that grants law enforcement permission to review the image.[58]

A DELICATE BALANCE FOR ONLINE SERVICE PROVIDERS

For online service providers to play a meaningful role in the detection of child sex abuse material on their private services, they must satisfy the increasingly complex web of requirements under both the government agent doctrine and the private search doctrine. To avoid being designated as government agents, their programs must be sufficiently independent of the government, and they also must have a convincing private business interest for these efforts. But online service providers

[54] *Ackerman,* at 1306–07.
[55] *United States v. Reddick*, 900 F.3d 636, 638 (5th Cir. 2018).
[56] *Reddick,* at 640.
[57] Government's Brief in Opposition to Defendant's Motion to Suppress, *United States v. Ringland*, Case No. 8:17-cr-00289 (D. Neb. May 3, 2018) at 10.
[58] *Id.*

also increase the chances that the private search doctrine will eventually apply to the evidence if they review all flagged content, rather than merely forwarding it to the NCMEC or law enforcement.

This dilemma is illustrated in one of the most recent challenges to CyberTipline evidence, *United States v. Ringland*,[59] a U.S. Court of Appeals for the Eighth Circuit opinion. Google provided the NCMEC with apparent child sex abuse material that it had detected on an account. Law enforcement only viewed files that Google had viewed.[60]

The Eighth Circuit concluded that Google was not a government agent "because it scanned its users' emails volitionally and out of its own private business interests."[61] The defendant argued that Google was a government agent in part because it "continued to scan his email and uncover his identifying information after its initial report to NCMEC, thus showing the government was aware of and acquiesced to Google's searches and Google acted to assist" state law enforcement. The court rejected this argument, finding no evidence of government control over the search: "The unity of interest between Google and the government does not imply some acquiescence or agreement between them to conduct searches in an informal, clandestine manner. Simply put, Google's continued actions in its own interest and the government's continued receipt of the reports does not give rise to some form of agency."[62]

As in *Drivdahl*, the private search doctrine prevented the evidence from being suppressed in *Ringland*. The court noted that law enforcement "searched only the same files that Google searched," and therefore "the government did not expand the search beyond Google's private party search."[63] In other words, Google's review of the images—rather than mere forwarding—may very well have prevented the evidence from being suppressed.

Although Google's review of the images likely ensures that the private search doctrine applies, such review increases the risk of a court eventually finding that Google is a government agent. Recall the two-part *Walther* framework for determining whether a private party was a government agent: (1) government acquiescence and control of a search, and (2) private party intent. When Google goes beyond using automated tools such as PhotoDNA—and reviews the images before filing a

[59] *United States v. Ringland*, 966 F.3d 731 (8th Cir. 2020).
[60] *Ringland*, at 735.
[61] *Ringland*, at 736.
[62] *Ringland*, at 737.
[63] *Ringland*, at 737. The court concluded it was irrelevant whether the NCMEC was a government agent or had exceeded the scope of Google's private search because law enforcement's application for a search warrant relied only on the images that Google had viewed.

CyberTipline report—it becomes harder for Google to argue that its searches were motivated entirely by its own business interests and not to help law enforcement. A PhotoDNA hit should be sufficient for Google to protect its own business interests by informing a decision to suspend a user account or take other remedial actions; there are few convincing justifications for Google to take the additional step of requiring its employees to review the images, other than to help the law enforcement process.

In *Ringland*, the federal government managed to convince the court both that Google was not a government agent *and* that the private search doctrine applied because the government reviewed only the images that Google already had reviewed. Yet the case demonstrates the very fine line that Google, the NCMEC, and the government walked in a post-*Ackerman* world.

During oral argument in the district court, Ringland's defense attorney highlighted the difficult balancing act: "In every other context, Google, the National Center for Missing and Exploited Children and law enforcement openly celebrate their working together, until you've set foot in a courtroom once a defense attorney mentions the Fourth Amendment. And then they're like three guys who just got pulled over in a car and are separated and claim not to know each other."[64]

The argument is a compelling one, particularly so when a private company is implementing extensive reviews to examine potential child sex abuse material in a private user account. In *Ringland*, the Eighth Circuit conducted a rather perfunctory analysis of the extent to which Google conducted its search and relied on the assumption that such an exhaustive operation was solely to advance Google's commercial interests. But it is not difficult to imagine a different judge taking a closer look at the review efforts and reaching an opposite conclusion.

There is no easy solution to this problem. The courts have generally settled on a government agency test that at least partly—if not mostly—focuses on the subjective motivations of the private party. Courts should reconsider the government agency tests that are rooted in *Walther*. As discussed earlier, it is increasingly difficult to determine the subjective intent of a large platform that is implementing an anti–child sex abuse material program. Criminal defendants, online service providers, and law enforcement should have more clarity and certainty as to the types of activities that render a provider a government agent for Fourth Amendment purposes. A purely objective test, which examines the amount of control that the government has exerted over the hash scanning, likely would lead to more equitable and predictable results. An objective focus would provide law

[64] Transcript of Hearing on Motions to Suppress Evidence and Statements and Application for Franks Hearing, *United States v. Ringland*, Case No. 8:17-cr-00289 (D. Neb. July 19, 2018) at 61.

enforcement with a strong incentive to avoid getting involved in private companies' monitoring efforts, and it also would allow online service providers to better structure their programs.

Unfortunately, courts have not shown much interest in improving the government agency test, so online service providers and law enforcement generally must work within the general *Walther* framework. So far, online service providers have been able to structure their efforts to detect child sex abuse material without a court ruling that they are government agents. But such success in the future is far from certain, particularly in a post-*Ackerman* world.

To avoid a government agent finding, online service providers will need to operate their detection efforts at arms' length from the NCMEC and law enforcement. Law enforcement should avoid offering online service providers guidelines, information, or other assistance in detecting child sex abuse material. Moreover, providers might further reduce their chances of being designated as government agents by ceasing any review of apparent child sex abuse material. Post-*Ackerman*, this might mean that law enforcement should obtain a warrant to review material that has been flagged by an automated system. Although this would add a step to the investigative process, it could reduce the Fourth Amendment government agency complications if the defendant moved to suppress the evidence. Alternatively, law enforcement might increase the chances that the private search doctrine applies by limiting their warrantless examinations of images to those that were flagged by automated programs such as PhotoDNA, though there is at least some risk that a court still would view such a process as an expansion beyond the private automated search. In light of the complex Fourth Amendment equities in CyberTipline cases, such precautions may be well worth the hassle for online service providers, the NCMEC, and law enforcement.

Online service providers also might attempt to obtain consent for searches through their terms of service, though such consent mechanisms, for Fourth Amendment purposes, are far from certain to succeed and highly fact-specific.[65] Even if online service providers could rely on consent, they must consider how to clearly inform users of such searches and the impact of these notices on their business interests.

This balancing act tells a broader story about platforms that extends beyond the child sex abuse material problem.[66] Private companies are the gatekeepers for a vast amount of information, some of

[65] See *United States v. Heleniak*, No. 14CR42A (W.D.N.Y. Feb. 9, 2015) ("[T]here are issues of fact whether this defendant was familiar with AOL's policy to make his use of the service consent to search by a Government agent.").

[66] Outside the context of child sex abuse material, providers also may face statutory restrictions. For instance, evidence of other potential crimes may not be covered by a Stored Communications Act exception as the NCMEC reporting is. See 18 U.S.C. § 2702(b)(6).

which may be evidence of a crime. Even if these companies want to help law enforcement in detecting, prosecuting, and ultimately preventing online crimes, they must walk a very fine line, particularly when searching private user data. Under the existing Fourth Amendment government agent doctrine, there is a reasonable chance that online service providers and government agencies will be unable to continue to strike this balance and that child sex abuse material prevention methods will be unable to survive suppression motions.

The Digital Social Contract paper series is supported by funding from Facebook, which played no role in the selection of the specific topics or authors and which played no editorial role in the individual papers.