Congressional Research Service
Informing the legislative debate since 1914

Legal Sidebar

The Fourth Amendment and the Internet: Legal Limits on Digital Searches for Child Sexual Abuse Material (CSAM)

March 24, 2022

Various federal statutes criminalize the production, distribution, solicitation, and possession of "child pornography," defined in part as "any visual depiction" of sexually explicit conduct involving a minor. Over time, Congress has sought to augment the enforcement of these provisions and limit the dissemination of such material online in several ways. Among other things, federal law requires covered interactive computer service (ICS) providers, such as companies like Google and Meta, to report "apparent violation[s]" of the statutes that involve child pornography to the CyberTipline operated by the National Center for Missing and Exploited Children (NCMEC), a private, nonprofit organization that receives government funding. NCMEC refers to the material subject to reporting under the statute as Child Sexual Abuse Material (CSAM), a term it views as "most accurately reflect[ing] what is depicted—the sexual abuse and exploitation of children." NCMEC is required by federal law to make these provider reports available to law enforcement agencies, and NCMEC receives legal protection from any claims arising from the performance of its CyberTipline responsibilities and other actions, with certain exceptions.

Currently, nothing in federal law requires providers to monitor their services or content for CSAM in the first instance. Under the law, although providers must report CSAM to NCMEC, which must then make the reports available to law enforcement, providers are not obligated to "affirmatively search, screen, or scan for" these violations. Nevertheless, many providers opt to voluntarily detect, remove, and report CSAM on their platforms. Against the backdrop of an increase in reports to NCMEC of suspected online child sexual exploitation during the COVID-19 pandemic, legislation in the 117th Congress would seek to bolster the CSAM reporting regime by establishing a commission to promulgate voluntary best practices for providers, among other things, as well as to apply similar reporting frameworks to a broader set of criminal acts.

Although CSAM is both illegal by statute and unprotected under the First Amendment's Free Speech Clause, identifying and reporting CSAM nonetheless poses policy and legal hurdles. At least one major player in the effort to remove online CSAM, Apple, has faced backlash from privacy advocates over a reportedly delayed plan to scan iCloud-stored photos on a user's device for CSAM. Additionally, federal

Congressional Research Service
https://crsreports.congress.gov
LSB10713

courts are still grappling with the scope of important constitutional limits to the existing reporting regime. For instance, in a recent decision creating a circuit split, the Ninth Circuit held that law enforcement violated the Fourth Amendment to the U.S. Constitution, which protects against "unreasonable [government] searches and seizures," by viewing email attachments containing apparent CSAM flagged by Google and reported through NCMEC without a warrant. This Sidebar provides an overview of the Fourth Amendment's application to the existing CSAM reporting regime, including points of divergence in recent federal caselaw that could impact congressional efforts to further encourage private ICS providers to search for and report CSAM or other evidence of criminality.

Overview of Fourth Amendment State Action and Private Search Doctrines

The Fourth Amendment prohibits "unreasonable searches and seizures," which ordinarily means that law enforcement must obtain a judicially authorized warrant based on probable cause before conducting a search for evidence of criminal wrongdoing. In the absence of a warrant, the government typically must show that an exception to the warrant requirement, such as exigent circumstances, justified the search. The Supreme Court has interpreted the Fourth Amendment to require the exclusion from trial of evidence obtained in unreasonable searches unless an exception applies, generally preventing the government from using that evidence to prove that the defendant committed a crime.

As with other constitutional guarantees, the Fourth Amendment constrains only *governmental* action, meaning that it typically does not apply to a search, however unreasonable, that a private individual or entity voluntarily carries out. Under the state action doctrine, however, the Fourth Amendment does apply to private action "if the private party acted as an instrument or agent of the Government." Whether a private individual should be deemed such an instrument or agent for purposes of the Fourth Amendment "necessarily turns on the degree of the Government's participation in the private party's activities" in light of all the circumstances of the particular case. Where the government has directed a private party to conduct a search—for example, a police officer using a nurse to draw blood from a suspected drunk driver—the search likely involves state action.

A private search could also involve state action even in the absence of an express government mandate. In *Skinner v. Railway Labor Executives' Association*, the Supreme Court held that private railroads conducted searches subject to the Fourth Amendment when they tested employees for drug and alcohol use in light of federal regulations that authorized the tests. Although the regulations at issue did not mandate that the railroads order the challenged tests, they expressed a "strong preference for testing" and "removed all barriers" to doing so. Specifically, according to the Court, the regulations did this by authorizing and encouraging railroads to order the tests following certain procedures, preempting state law or private agreements on the subject, providing that railroads could not contract away the testing authority, entitling the regulating agency to receive certain testing results, and subjecting employees who refused the testing to certain employment consequences. In light of these "clear" signs of government "encouragement, endorsement, and participation," the Court concluded that the testing was not "primarily the result of private initiative" and thus was "suffic[ient] to implicate the Fourth Amendment."

Beyond the state action doctrine, a corollary concept sometimes referred to as the private search doctrine reflects that a private search without state action ordinarily will not implicate the protections of the Fourth Amendment even if the results of the search are thereafter transmitted to the government. Should government officials, such as law enforcement officers, subsequently conduct a search of the transmitted materials that "exceed[s] the scope of the private search," however, that secondary search may trigger the Fourth Amendment. Whether a government actor's follow-on search exceeds the scope of a private search hinges on the degree to which an individual's reasonable expectation of privacy has been frustrated. In *Walter v. United States*, the Court determined that FBI agents exceeded the scope of a private search of packages that revealed film boxes with pictures and descriptions on the outside suggesting they were obscene. On the basis of the pictures and descriptions, the private party that discovered the film boxes

contacted the FBI, which took and viewed the films to confirm they were obscene in violation of federal law. Although the Supreme Court did not settle on a single rationale, a majority of the Justices agreed that the FBI conducted an unlawful Fourth Amendment search. According to at least four Justices, the FBI exceeded the scope of the private search by opening the boxes and viewing the films, because although the private search may have frustrated the defendants' expectation of privacy in the contents of the *packages* in part, there remained an "unfrustrated portion of that expectation" of privacy as to the content of the *films*.

By contrast, in the later case *United States v. Jacobsen*, the Court held that DEA agents did not exceed the scope of a package search conducted by a private mail carrier, which revealed a suspicious white powder, by reopening the package, removing the powder, and conducting a field test identifying the powder as cocaine. In the Court's view, the DEA agent's re-removal of the powder from its package "hardly infringed respondents' privacy," as the private employees had already examined the package's contents of their own accord before contacting law enforcement. As to the field test, the Court indicated that the test did not compromise any "legitimate privacy interest" in the powder because it could only reveal whether the substance was cocaine—contraband that no one had a right to privately possess—and "no other arguably 'private' fact."

Status of ICS Providers and NCMEC Under Existing Law

Several federal courts of appeals have determined that ICS providers, despite their statutory obligation to report apparent violations of federal CSAM statutes to NCMEC (and ultimately law enforcement), are not considered government actors subject to the Fourth Amendment when they voluntarily undertake to search for such material on their platforms. For example, in *United States v. Stevenson*, the Eighth Circuit addressed AOL's practice of automatically scanning files on its network for CSAM. The defendant argued that AOL acted as a government agent when it scanned his email, because federal law required the company to report any violations it detected and immunized AOL for performing that duty. The Eighth Circuit disagreed, distinguishing the CSAM-specific obligations from the more comprehensive provisions in *Skinner* that preempted other laws and agreements and prescribed consequences for failure to submit to the favored private action. According to the appellate court, the statutory requirement to report CSAM, "standing alone, does not transform an Internet service provider into a government agent whenever it chooses to scan files sent on its network for [CSAM]."

In contrast, in an opinion authored by then-Judge Neil Gorsuch, the Tenth Circuit held in *United States v. Ackerman* that NCMEC itself *is* a government entity or agent in this context. Looking to the "comprehensive" statutory scheme governing NCMEC, the court recognized that Congress required NCMEC to report CSAM "at the government's expense and backed by threat of sanction" and with "special dispensation, too, to NCMEC to possess and review contraband knowingly and intentionally." In short, the court held that "Congress funded [NCMEC], required [providers] to cooperate with it, allowed it to review [the defendant's] email by excepting it from various federal criminal laws, and statutorily mandated or authorized every bit of its challenged conduct" in opening email attachments forwarded from AOL and alerting law enforcement. Although the court ultimately declined to exclude the evidence at issue in *Ackerman* from the defendant's trial based on an exception to the exclusionary rule, *Ackerman* suggests that NCMEC could be considered a state actor in facilitating the identification and reporting of CSAM.

Circuit Split Regarding Scope of Private Search for CSAM

With respect to the scope of private ICS provider searches for CSAM, and the question of whether NCMEC or law enforcement review of forwarded material exceeds that scope, recent appellate decisions have created a circuit split based on differing views of the technological mechanism providers use to screen for illicit material. Many providers rely on what is known as "hash-value" matching to identify

CSAM on their platforms. Essentially, the process involves assigning known CSAM a unique identifier, the hash value, so that files shared on a provider's platform can be efficiently and automatically screened against that universe for matches. In other words, a provider might use hash values to identify files that match the unique identifier of known CSAM automatically, suggesting with a high degree of accuracy that the files are themselves CSAM without a person having to inspect each individual file on a provider's platform visually. In recent cases, the Fifth, Sixth, Eighth, and Ninth Circuits have all addressed the practice of hash-value matching in similar contexts: where a provider identifies CSAM through the automated hash-value matching process, reports the offending files, and law enforcement ultimately opens and views the files that the provider flagged based on the matching hash values. The Fifth, Sixth, and Eighth Circuits held that in this situation, so long as only matching files are subsequently inspected by law enforcement, the follow-on government search does not exceed the scope of the provider's hash-value search, even though the nature of that underlying process does not involve visual inspection by provider employees of the files that are reported. These courts relied on the high degree of reliability of the process, analogies between the relevant search and the search and testing of the white powder in *Jacobsen*, and the fact that the nature of hash-value matching means that a person at some point viewed files identical to the flagged ones and identified them as CSAM.

In a 2021 opinion, *United States v. Wilson*, the Ninth Circuit split from the other circuits and held that law enforcement review of email attachments tagged by Google as CSAM through hash-value matching "exceed[ed] the limits of the private search exception as delineated in *Walter* and *Jacobsen* and their progeny." In the Ninth Circuit's view, a "large gap" existed between the information revealed by Google's process and by a law enforcement officer's subsequent visual inspection of the flagged email attachments, such that *Walter* "offer[ed] a much more apt comparison" than the search in *Jacobsen*. According to the court, as in *Walter*, viewing the email attachments "substantively expanded the information available to law enforcement far beyond what the label" from Google's matching process "alone conveyed, and was used to provide probable cause to search further and to prosecute." The court also emphasized that no one at Google had actually viewed the email attachments at issue but had only at some point viewed images that were then matched with the images in the attachments. The court expressly rejected the conclusions reached by the Fifth and Sixth Circuits described above.

Considerations for Congress

The Supreme Court has not addressed whether, in the context of CSAM reporting, (1) NCMEC is a government entity or agent, (2) ICS providers are private actors in light of statutory reporting requirements, or (3) law enforcement examination of a hash-value-matched file exceeds the scope of an initial search using that process. Based on appellate caselaw to date, it appears that the Fourth Amendment permits voluntary ICS provider searches for CSAM without a warrant but may not authorize NCMEC to exceed the scope of those searches absent judicial process or a recognized exception to the Fourth Amendment warrant requirement. (In this respect, it is always possible that particular searches could be permissible even assuming NCMEC or another entity is acting as a government agent and intrudes on a user's reasonable expectation of privacy without a warrant based on probable cause—for instance, if exigent circumstances exist.)

As the 117th Congress considers whether changes to the existing CSAM reporting regime should be made, it may wish to consider the extent to which additional statutory inducement for ICS providers to undertake CSAM searches could implicate the state action doctrine. Even in the absence of an express mandate to search, incentives or requisite procedures for CSAM searches might be viewed by a court as additional government "encouragement, endorsement, and participation" in ICS provider screening for CSAM under *Skinner*. Beyond the question of whether and when an entity is considered an agent of the government for Fourth Amendment purposes, courts' treatment of hash-value searching could also have implications for ICS providers' ability to stem the flow of CSAM voluntarily and for any contemplated

congressional support of such efforts. Under the Ninth Circuit's view in *Wilson*, hash-value matching by an ICS provider is not sufficient to permit subsequent warrantless review of the matched content by government actors. As such, under *Wilson*, to insulate its CSAM reporting and review from Fourth Amendment scrutiny, a provider employee would need to inspect visually the images flagged as CSAM through hash-value matching. In contrast, such inspection would not be required to invoke the private search doctrine under the caselaw from the Fifth, Sixth, and Eighth Circuits, which the Supreme Court declined to review. It remains to be seen whether and when the Court or additional circuits may address this nascent circuit split.

Author Information

Michael A. Foster
Legislative Attorney

Disclaimer