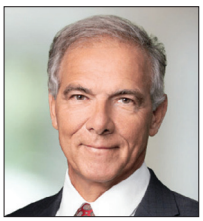
ALM | LAW.COM

New York Law Journal

WHITE-COLLAR CRIME

Can an ISP's Terms of Service Defeat Fourth Amendment Protections?

By Robert J. Anello and Richard F. Albert
June 9, 2026



By **Robert J. Anello**

And **Richard F. Albert**

Virtually every major digital platform—Google, Microsoft, Apple, Meta—includes in its terms of service a privacy policy by which the platform reserves the right to scan or review user content. Does such a policy, which most users never read, defeat the user's reasonable expectation of privacy, thereby permitting a warrantless government search? In its recent decision in *United States v. Lowers,* 170 F.4th 134 (4th Cir. 2026), the Fourth Circuit, rejecting the government's arguments based on an Eleventh Circuit decision outside the digital context, joined the Second and Sixth circuits in holding that the answer is no.

For clients facing white collar criminal investigations, the stakes of this issue that has divided the circuits are profound. Virtually all of us use digital platforms to transmit sensitive business and financial information. Advances in technology—think artificial intelligence—increase the chances that digital service providers may use algorithms or other techniques to scan for evidence of potential illegal activity, such as transactions with sanctioned countries or money laundering.

If the government's position in *Lowers* had prevailed, fine print that virtually all users overlook would be enough to give the government unfettered access to user content, without demonstrating probable cause or obtaining a search warrant.

The Rule in the Second and Sixth Circuits: "May" Does Not Invite the Government In

Under what has come to be known as the *Katz* test, a defendant seeking to invoke Fourth Amendment protections against a warrantless government search must prove that he or she had a subjective expectation of privacy and that the expectation was objectively reasonable. *Katz v. United States,* 389 U.S. 347 (1967). In cases involving warrantless searches of digital content, the government has argued that an

expectation of privacy is unreasonable for users who agree to permit providers to review content.

The rule adopted by the Second and Sixth Circuits rejects the government's argument by drawing a critical distinction between a private company's reserved right to inspect its users' content and the government's right to conduct warrantless searches.

These courts focus on the fact that the providers' policies used permissive language like "may" rather than mandatory terms like "will audit, inspect, and monitor." The central premise is that a company "alerting" its users that it might look at their content is fundamentally different from the government claiming the right to do the same without obtaining a warrant. The rule is illustrated by the example of a hotel guest whose reasonable expectation that the police will not barge in without a warrant is not defeated by the guest's knowledge that housekeeping has a key and may enter the room.

The first circuit to adopt this principle was the Sixth Circuit in *United States v. Warshak,* 631 F.3d 266 (6th Cir. 2010), which the other circuits have treated as the seminal case on the issue. In *Warshak*, in connection with a fraud investigation, the government obtained approximately 27,000 private emails without a warrant from the defendant's Internet Service Provider (ISP). The ISP's subscriber agreement warned users that it "may access and use individual Subscriber information in the operation of the Service and as necessary to protect the service."

The Sixth Circuit was unpersuaded that "the mere ability of a third-party intermediary to access the contents of a communication" extinguishes a reasonable expectation of privacy in digital content. Analogizing to privacy expectations found in sealed letters despite handling by multiple intermediaries, telephone calls despite the ability of operators to listen, and in rented spaces such as hotel rooms despite the ability of housekeeping to enter, the court held that a permissive reservation by a third party does not open the door to government access.

The court, however, drew an important distinction: it was "unwilling to hold" that a contractual reservation of the right to access user content would "never be broad enough to snuff out a reasonable expectation of privacy" and acknowledged that a policy that expressly states that a provider will "audit, inspect, and monitor" user content might yield a different result. See *Warshak v. United States*, 490 F.3d 455 (6th Cir. 2007) (*Warshak* I).

The Second Circuit adopted *Warshak's* reasoning in *United States v. Maher,* 120 F.4th 297 (2d Cir. 2024). Maher involved child pornography files that Google flagged through an algorithmic scan but did not visually examine before reporting the files to the National Center for Missing and Exploited Children, which sent the report and files to the New York State Police who conducted a warrantless visual review.

Google's Terms of Service advised users that it "may review content to determine whether it is illegal or violates our policies," and "may" report "illegal content" to "appropriate authorities." Relying on *Warshak*, the Second Circuit concluded that this language did not extinguish the defendant's reasonable expectation of privacy.

The court emphasized the significance of the word "may." Google's Terms of Services advise users that it "may" but "does not necessarily... review content," and instruct users not to "assume that we do." "Such qualified language," the court concluded, "is hardly a per se signal to Google users that they can have no expectation of privacy in their emails, even as against the government."

Notably, although the Second Circuit in *Maher* and the Sixth Circuit in *Warshak* both found that the government had violated the Fourth Amendment, in both cases the courts declined to exclude the contested evidence on grounds that the government acted in good faith when it accessed the defendants' files.

The Contrary Rule: the Eleventh Circuit's Approach

The Eleventh Circuit's holding in *United States v. Young,* 350 F.3d 1302 (11th Cir. 2003), although outside the digital context, reflects a fundamentally different view of how terms of service may have an impact on a user's reasonable expectation of privacy. The Eleventh Circuit has treated an explicit warning about potential inspection as extinguishing the defendant's reasonable expectation of privacy against a warrantless government search.

In *Young*, the defendants shipped 14 packages containing large quantities of currency via Federal Express. The airbill and envelopes utilized by the defendants warned "DO NOT SEND CASH" and stated that FedEx "may, at our option, open and inspect your packages prior to or after you give them to us to deliver."

When IRS agents asked FedEx to turn over the packages for inspection in connection with a suspected tax scheme, the Eleventh Circuit found that "[n]o reasonable person would expect to retain his or her privacy interest" in a package bearing such a warning. The court went further, holding, as an alternative ground, that the notice authorized FedEx, as the packages' bailee, to consent to the government's search on the defendants' behalf.

The Fourth Circuit Joins the Majority

The Fourth Circuit's decision in *United States v. Lowers,* 170 F.4th 134 (4th Cir. 2026), decided on March 10, 2026, squarely confronted whether clicking "I agree" to a provider's terms of service forfeits Fourth Amendment protections in content stored by that provider.

Accepting the government's argument to apply the Eleventh Circuit's holding in Young in the digital context, the district court had ruled that Google's privacy policy stripped the defendant of any right to challenge warrantless intrusions into his Google Drive. The holding, if affirmed, would have meant that every Google user effectively had waived Fourth Amendment protections in digital content on Google's platforms. The Fourth Circuit reversed, joining the Second and Sixth Circuits.

Like *Maher*, *Lowers* arose from a Google algorithmic match that flagged child sexual abuse material in the defendant's private Google Drive. The district court denied the defendant's suppression motion, and on appeal the Fourth Circuit drew an instructive analogy to *Katz*, which held that even though telephone companies retained the right to monitor calls for illegal conduct and the defendant knew that an operator could eavesdrop, the defendant had a reasonable expectation that government agents would not eavesdrop.

The Fourth Circuit reasoned that similarly, even though a Google Drive user may know that Google might occasionally sift through his files, and the warning reduces his expectation of privacy to "some degree," this "does not mean that he expects the government to have equally unfettered access to those same files." Finding the Eleventh Circuit's analysis in Young "unpersuasive," the Fourth Circuit expressly rejected its application to the digital context and joined the rule adopted by the Second and Sixth Circuits.

The Fourth Circuit also distinguished its prior decision in *United States v. Simons*, 206 F.3d 392 (4th Cir. 2000), which held that an internet usage policy defeated an employee's

expectation of privacy in internet activity. The critical difference, the court explained, was that the employer issuing the warning in *Simons* was not a private service provider, but the government itself—a subdivision of the CIA that warned it would "periodically audit, inspect, and/or monitor" user activity.

When the government is both the provider and the searcher, users face a far steeper burden. But when a private company uses permissive language, the calculus is entirely different. The critical threads running through *Lowers*, *Warshak*, and *Maher* are the difference between a provider's authority and the government's authority and the power of "may" in the language of privacy policies.

Notably, once again, the appellate court's ruling in *Lowers* did not help the defendant. Although finding a Fourth Amendment violation, the court held that the attenuation doctrine, which permits admission of derivative evidence obtained downstream from an illegal search, ultimately precluded suppression of the contested evidence.

Implications for White Collar Defense

Third-party service providers' privacy policies carry significant Fourth Amendment implications for practitioners and their clients. Courts care about the language in a service agreement. A policy that states the provider "will audit, inspect, and monitor" all user content might be enough to extinguish a reasonable expectation of privacy, even under the majority's approach. Highlighting permissive language should give clients a leg up when arguing for suppression of communications or other content obtained by the government without a warrant, at least in the Second, Fourth, and Sixth Circuits.

Apart from expectations of privacy, third party service providers' agreements pose additional Fourth Amendment concerns for white collar defendants. If a private party conducts a search and turns evidence over to the government, the government need not "avert their eyes" from what the private party put in plain view under the "private search doctrine" exception to the Fourth Amendment's warrant requirement.

The presence of a policy authorizing a private party to review content and turn it over to the government may increase the chance that the government can conduct a warrantless search of users' files, so long as the search does not "exceed the scope of the private search."

As advances in AI increase the chances that digital platforms use algorithmic or similar systems to detect potential evidence of illegal user activity relevant to white-collar crime, the private search doctrine is likely to become of increased relevance to practitioners. An open question is how broadly courts will define the "scope" of an algorithmic or similar search that identifies that a file matches known illegal content but does not reveal the file's full contents.

Further, even under the majority rule, a service provider's ability to search and flag content increases the ease with which the government can obtain a warrant. In an era when virtually every business transaction passes through third-party digital platforms, the fine print of these platforms' terms of service can have far-reaching consequences for white-collar defendants.

Robert J. Anello *and* **Richard F. Albert** *are members of Morvillo Abramowitz Grand Iason & Anello, P.C.* **Emily Smit**, *an associate at the firm, assisted in the preparation of this article.*