



Federal Wiretaps and the Fourth Amendment

September 21, 2026

The [Fourth Amendment](#) prohibits unreasonable searches and seizures, generally requiring that law enforcement obtain a [warrant](#) from a neutral and detached magistrate upon a showing of probable cause. In 1928, the Supreme Court determined in *Olmstead v. United States* that projected voices [passing](#) over telephone wires beyond a person's home were not protected by the Fourth Amendment, so no warrant was required for a wiretap installed outside of the home. Since the *Olmstead* decision, the case law and [statutory](#) framework governing law enforcement surveillance of real-time communications has changed significantly. This In Focus provides a brief history of the Fourth Amendment's application to such surveillance, an overview of the federal Wiretap Act, selected caselaw interpreting the statute, and considerations for Congress.

Selected Legal History

In *Olmstead*, the Supreme Court determined the projection of voices outside the home by telephone to be outside the scope of the Fourth Amendment protections because the Court perceived the text of the Amendment to be focused on “[material](#) things—the person, the house, his papers or his effects.” By the 1967 case *Berger v. New York*, the Court's views had shifted. The Court held that a state statute—which permitted a related type of surveillance, eavesdropping, when authorized by a court order—was [unconstitutional](#) under the Fourth Amendment. Explaining its [concern](#) about the development of “sophisticated electronic devices,” which “pick up whispers in a room,” the Court identified several aspects of the statute that did not “carefully [circumscribe](#)” the circumstances under which courts could authorize electronic eavesdropping to prevent so-called “[general searches](#)” through electronic listening devices. The Court held that the statute lacked the [particularity](#) required by the Fourth Amendment in that it did not require the applicant to describe a particular offense, particularly describe the property to be seized (i.e., the [conversations](#) sought), provide [notice](#) to parties, or obtain supervision from the court over the execution of the warrant. The decision also condemned the statute's unrestricted, two-month [authorization](#) and lack of sufficient probable cause for extensions. Later in 1967, in *Katz v. United States*, the Court clarified that the Fourth Amendment applies to “[people](#), not places,” officially [overturning](#) *Olmstead*'s physicality requirement and setting a threshold “[reasonable](#) expectation of privacy” test for Fourth Amendment queries.

Legislation

Following *Olmstead*, in 1934, Congress enacted a federal [law](#) prohibiting the interception of communications over wires, including by [federal](#) law enforcement as evidence in criminal proceedings. In 1968, after the *Berger* and *Katz* decisions, Congress enacted Title III of the Omnibus Crime Control and Safe Streets [Act](#) of 1968 (Title III or the Wiretap Act) with the dual [purpose](#) of “properly protect[ing] the privacy of oral and

wire communications, while providing a uniform basis for authorizing their interception in appropriate cases.”

Coverage and Relevant Exclusions

Title III, as [amended](#), generally [prohibits](#) the interception of [wire, oral, and electronic communications](#) (including wiretapping and eavesdropping). The categories of information cover aural transfers of the human voice using wires, cables or like connections (such as telephones), communications between two people with an expectation of privacy, and transfers of signs, signals, writing and other data, such as emails and text messages. Courts have generally found the statute to apply to the real-time, [contemporaneous](#) interception of [communications](#), not to prior recordings. There are numerous exceptions to Title III's coverage, including for certain types of [electronic](#) communications, [intelligence](#) interceptions and [technical](#) assistance, and certain interceptions when one of the parties to the communication [consents](#).

In [18 U.S.C. § 2518](#), the statute sets forth detailed procedures for federal law enforcement to obtain court-ordered interceptions of communications and authorizes certain [state](#) interceptions in conformity with that section. The statute also permits [emergency](#) interception in specific situations, usually involving an imminent [threat](#) to life, while requiring a full application to a court within 48 hours of interception.

Authorization

Under [18 U.S.C. § 2516](#), only a specifically designated Deputy Assistant Attorney General or higher official at the Department of Justice (DOJ) may authorize an application for a federal wiretap of wire or oral communications. In contrast, any attorney for the government, as [defined](#) by the Federal Rules of Criminal Procedure, [may](#) authorize an [application](#) for electronic communications. Reviewing § 2516, in *United States v. Giordano*, the Supreme Court [stated](#) that “[t]he mature judgment of a particular, responsible Department of Justice official is interposed as a critical precondition to any judicial order” and suppressed evidence obtained through an application signed by the Attorney General's executive assistant.

Relying on *Giordano*, the Second Circuit [determined](#) that a similar [requirement](#) that the interception order be authorized only from a “court of competent jurisdiction” precludes a federal judge's delegation of authority to a magistrate judge.

Probable Cause

To issue an interception order under Title III, a judge must find probable cause that “[particular communications](#)” about an [enumerated](#) offense will be obtained through interception of the [facility](#) (usually a phone, device) or target location. The law enforcement officer's affidavit [must](#) generally establish probable cause to believe that the suspects are using the targeted facility to conduct the criminal activity. DOJ has historically

imposed strict [time](#) constraints on such probable cause [evidence](#) to avoid [staleness](#) challenges.

Statement of Facts

Federal application packages for Title III authorization [typically](#) comprise an application, affidavit, and draft order. Each application for an interception [requires](#) the identification of the applicant and a sworn “full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued.” This statement must identify the suspects, the target facilities or locations, and the criminal offenses under investigation. The application package must describe the facility to be intercepted with particularity; however, upon a showing that targets are evading law enforcement’s detection, the statute authorizes a [roving](#) wiretap tied to a person in lieu of a facility under certain [conditions](#). Reviewing courts have generally distinguished between roving wiretaps and wiretap authorizations for [cell phones](#) (including those encompassing [changing](#) cell phone numbers associated with a listed serial [number](#) or other identifier).

Necessity

The law enforcement application package must include a “full and complete” statement of [investigative](#) techniques that have been “tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous” to “[assure](#) that wiretapping is not resorted to in situations where traditional investigative techniques would suffice to expose the crime.” Such traditional [techniques](#) typically include surveillance, interviews, infiltration, search warrants, and review of call records. Although the application’s description of such techniques [must](#) avoid generalities and conclusory statements and “specifically relate to the individuals targeted by the wiretap,” courts have found that this requirement is not “[designed](#) to force the government to exhaust all other conceivable investigative procedures.”

Minimization

Interception must be conducted “in such a way as to [minimize](#) the interception of communications not otherwise subject to interception.” In *Scott v. United States*, the Supreme Court explained that this provision does “not forbid the interception of all nonrelevant conversations” but requires law enforcement’s minimization to be [reasonable](#) based on the facts and circumstances of each case. In determining the reasonableness of the minimization, lower courts have looked at the [factors](#) identified in *Scott*, such as the percentage of non-pertinent calls intercepted, the length of calls, the use of code language, the extent of the conspiracy, and the stage of the investigation.

The application package [typically](#) includes a minimization plan, which can rely on civilian monitors if [supervised](#) by an investigative or law enforcement officer and [noticed](#) to the court. Minimization is conducted in real time with the exception of communications in a [foreign language](#) or code, which must be minimized as soon as practicable.

Duration, Disclosures, and Other Protections

Addressing the [concerns](#) of the *Berger* Court as to the extent and length of eavesdropping and wiretapping orders, 18 U.S.C. § [2518\(5\)](#) limits the duration to not “longer than is

necessary to achieve the objective of the authorization, nor in any event longer than thirty days,” with strict requirements for extensions.

[Notice](#) to the intercepted parties after the fact is required, as are [protections](#) for intercepted communications and [applications](#). Individuals in violation of the provisions of Title III are [subject](#) to potential criminal and [civil](#) liability.

The statute [contains](#) annual [reporting](#) requirements for state and federal judges issuing wiretap orders. In 2025, judges reported a [total](#) of 1,735 state and federal wiretaps authorized. Drug offenses were the most [prevalent](#) type of offense identified, and the average [cost](#) was \$92,963 per wiretap.

Suppression

18 U.S.C. § 2518(10)(a) provides for suppression of wire and oral communications evidence if (i) the interception was unlawful, (ii) the order was insufficient on its face, or (iii) the interception was not made in conformity with the order of authorization or approval. In *Giordano*, the Supreme Court [found](#) that the statute required suppression for an unauthorized delegation because the authorization provision “[play\[s\]](#) a central role in the statutory scheme.” After *Giordano*, courts concluded that “not [every](#) failure to comply fully with . . . Title III necessitates suppression.” To determine whether suppression was mandatory, courts generally have focused on whether the transgressed statutory provision played a central or [substantive](#) role in the regulatory system established by Congress.

In 2018, the Supreme Court [clarified](#) that § 2518(10)(a)(i) applies when the “Government’s use of a wiretap is unconstitutional or violates a statutory provision that reflects Congress’ [core](#) concerns.” Subparagraph (ii) applies when the order lacks information required by the statute; and subparagraph (iii) applies when the “Government fails to comply with conditions set forth” in the authorization.

Both Title III and the *Giordano* decision predate the judicially created exception to the exclusionary rule, which can preserve evidence if the government acted in [good faith](#). Federal appeals courts have [disagreed](#) whether the doctrine [can](#) be [applied](#) to avoid suppression of wiretap evidence or whether the statute [requires](#) suppression, irrespective of a showing of good faith.

Considerations for Congress

The Supreme Court has interpreted the Fourth Amendment to establish discrete parameters around law enforcement’s interception of real-time communications. Through Title III, Congress codified the Court’s standards and provided uniform guidance to law enforcement and courts to enable criminal investigations and prosecutions. Congress has amended the statute through the [Antiterrorism and Effective Death Penalty Act](#), the [Communications Assistance for Law Enforcement Act](#), and the [Electronic Communications Privacy Act](#), among others, to encompass new technology and to facilitate law enforcement access to these investigative tools. Congress may continue to examine these provisions in the face of emerging technology and caselaw and legislate, if it chooses to, in line with the Court’s Fourth Amendment jurisprudence.

Tamsin G. Harrington, Supervisory Attorney

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.