Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

Selected Federal Legislation on Search and Seizure Authority

September 17, 2026

The Fourth Amendment protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures[.]" As interpreted by the Supreme Court, the Amendment imposes certain limits on searches and seizures by the government. Within these limits, Congress has the option to further restrict or explicitly authorize a variety of law enforcement activities by legislation. This In Focus identifies a selection of such laws Congress has previously enacted and provides considerations for Congress related to potential legislation in the realm of search and seizure authority.

Fourth Amendment Backdrop

Courts have determined that a Fourth Amendment search occurs if "the Government obtains information by physically intruding on a constitutionally protected area" or "when the government violates a subjective expectation of privacy that society recognizes as reasonable." The Supreme Court has said that "'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property." If a law enforcement activity qualifies as a search or seizure, then the Fourth Amendment requires it to be reasonable, which ordinarily means that the search or seizure must be conducted pursuant to a warrant supported by probable cause and issued by a neutral magistrate (with some exceptions). To satisfy the probable cause standard to obtain a search warrant, law enforcement must generally show a likelihood that (1) the materials sought are "seizable by virtue of being connected with criminal activity," and (2) the materials "will be found in the place to be searched." The Fourth Amendment dictates that the resulting warrant must "particularly describ[e] the place to be searched, and the persons or things to be seized." The purpose of this requirement is to prohibit "general searches" and not permit seizure of "one thing under a warrant describing another."

Federal Law Governing Search and Seizure Authority

Federal Rule of Criminal Procedure 41 governs processes for federal search warrants. It addresses venue; persons or property subject to seizure; the process for obtaining, issuing, and executing warrants; and motions to return property and suppress evidence. Substantively, Congress has enacted legislation to specifically authorize or further restrict law enforcement search and seizure activities in particular circumstances. The following are selected examples of such legislation, presented chronologically.

The Wiretap Act

Following two 1967 landmark Supreme Court cases addressing the application of the Fourth Amendment to law enforcement surveillance of communications, Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968, also referred to as the Wiretap Act, with the purpose of both protecting the privacy of communications and allowing their interception and use as appropriate to combat organized crime. Title III, as amended, prohibits the real-time interception of wire, oral, and electronic communications, except as authorized in the statute, and sets forth detailed procedures for their access by law enforcement in criminal investigations.

Under these procedures, a court must find probable cause that "particular communications" about an enumerated offense will be obtained through interception. The statute also contains prerequisites for approval and demonstrations related to particularity and necessity, and further requires that law enforcement minimize the interception of communications not covered by the authorization. Courts have assessed compliance with this provision by analyzing whether minimization techniques were reasonable based on the facts and circumstances of each case. The statute also provides protections for intercepted communications, criminal penalties and evidentiary exclusion provisions for violations, and notice requirements.

The Foreign Intelligence and Surveillance Act (FISA)

Following revelations regarding widespread privacy violations by the federal government during the Watergate era, Congress enacted the Foreign Intelligence Surveillance Act (FISA) in 1978 to govern domestic foreign intelligence surveillance. FISA provides a statutory framework for government agencies to obtain authorization from specialized courts to gather foreign intelligence by means of electronic surveillance, physical searches, pen registers and trap and trace devices, or the production of certain business records. To obtain a court order under FISA, the executive branch must generally show, among other things, probable cause that a target is a foreign power or an agent of a foreign power.

Section 702 of FISA authorized programmatic surveillance of foreign intelligence traveling through domestic communications infrastructure, subject to oversight by the Foreign Intelligence Surveillance Court (FISC). (FISA Section 702 was automatically repealed pursuant to statute in April 2026, though certain associated surveillance authorities will remain in effect through early 2027.) The FISC was, in addition to other responsibilities, required to ensure that federal agencies' searching of data gathered pursuant to Section 702 was consistent with the Fourth Amendment. There were numerous statutory querying restrictions specific to the FBI, including that FBI personnel could not conduct queries using U.S.-person terms or identifiers solely addressing criminal activity (except in limited circumstances) and were required to seek senior officials' approval for any query involving a U.S.-person term. At least one federal district court has held that querying Section

702 data with U.S.-person terms presumptively requires a warrant.

The Privacy Protection Act

In 1978, the Supreme Court held in *Zurcher v. Stanford Daily* that the First Amendment's guarantee of press freedom did not preclude law enforcement's search of a student newspaper office. Congress responded to *Zurcher* in 1980 by enacting the Privacy Protection Act (PPA), which limits the ability of federal, state, and local officials to conduct certain searches and seizures implicating First Amendment activities. A Senate Judiciary Committee Report accompanying the PPA expressed concern that "the search warrant procedure in itself does not sufficiently protect the press and other innocent third parties," requiring additional protections beyond Fourth Amendment warrant requirements for those engaged in "public communication." The PPA therefore generally prohibits, with exceptions, law enforcement search or seizure of news media work product materials. The PPA also prohibits searches and seizures of documentary materials (defined as "materials upon which information is recorded"), but with additional exceptions authorizing searches when grand jury subpoenas have been or would be ineffective. The PPA creates a civil cause of action for damages against governmental entities or individual government actors who conduct searches or seizures in violation of the statute, but does not permit the exclusion of evidence from a criminal trial of a third party based on a PPA violation.

The Electronic Communications Privacy Act

Congress also enacted the Electronic Communications Privacy Act of 1986 (ECPA), which, among other things, amended the Wiretap Act to cover electronic communications, and both generally prohibited access and provided procedures for law enforcement to access certain other communications records in prescribed circumstances. Such procedures included use of devices that obtain phone records in real time, referred to as pen registers and trap and trace devices, which record dialing and routing information to identify the source and destination of a wire or electronic communication. Pursuant to the statute, law enforcement access must be configured to avoid the collection of content information and can be authorized for up to sixty days with extensions. Law enforcement must demonstrate "relevan[ce] to an ongoing criminal investigation" to obtain a court order, which identifies the device, the suspect, and the offense, and may include direction for assistance from a provider. Such orders are sealed and disclosure of their existence is prohibited.

The Stored Communications Act

Title II of ECPA is the Stored Communications Act (SCA), which created additional statutory protections for particular categories of electronic communications and related metadata that are stored with third party service providers. The Senate Judiciary report accompanying ECPA described the proliferation of electronic data storage and the risk that such data "may be subject to no constitutional privacy protection" because it "is subject to control by a third party computer operator." In general terms, the SCA restricts when certain information may be disclosed by Electronic Communication Services or Remote Computing Services, which typically include entities such as "cell phone providers, email providers, or social media platforms" and cloud computing providers. Pursuant to a provision of the SCA codified at 18 U.S.C. § 2703, the government may compel such providers to share communications' content and metadata if the government obtains the requisite level of legal process. Generally, contents of recent communications require a search warrant, while older and non-content information can be obtained with a subpoena or court order. In 2018, the Supreme Court applied the Fourth Amendment to certain location data and held that, while the SCA broadly authorized disclosure of non-content information to law enforcement pursuant to court order, law enforcement could not constitutionally compel the location data at issue in that case without a search warrant because people have a reasonable expectation of privacy in the whole of their physical movements.

Considerations for Congress

Laws relating to search and seizure generally reflect congressional balancing of law enforcement interests and privacy interests. For example, by limiting law enforcement searches of the news media with the PPA, Congress prevented law enforcement from obtaining confidential source information in some circumstances; the resulting potential impairment of leak investigations, however, is balanced against promotion of press freedoms. With the Wiretap Act and FISA, Congress likewise struck a balance, authorizing powerful investigative techniques but imposing substantial restrictions on their use. In the SCA, Congress opted to tie the requisite legal process to the sensitivity of the data, authorizing law enforcement access to some materials with subpoenas or court orders while requiring search warrants for others. With the caveat that "no Act of Congress can authorize a violation of the Constitution," Congress has the power to regulate executive branch exercise of search and seizure authority to effectuate its policy priorities.

Congress has not always opted to act via major legislation. For example, Congress created discrete criminal prohibitions related to law enforcement exercise of search and seizure authority in Title 18, such as willfully exceeding authority in executing a search warrant or exercising such authority "with unnecessary severity." Congress has also acted in situations where courts have found that the Fourth Amendment does not protect certain information. For example, after the Supreme Court held in 1976 that bank customers do not have a right to privacy in their bank records, Congress passed the Right to Financial Privacy Act to restrict warrantless law enforcement access to bank records.

In the 119th Congress, proposed legislation in the search and seizure realm has addressed, in alphabetical order: automated license plate readers, drones, and other surveillance technology; border searches; data brokers; financial records; FISA reform, including electronic surveillance authority and a proposed full FISA repeal; heightened warrant requirements; immigration enforcement; procedures and other requirements under the SCA; and warrant execution procedures, among others.

Cassandra J. Barnum, Legislative Attorney
Tamsin G. Harrington, Supervisory Attorney
Andreas Kuersten, Legislative Attorney

IF13315

Disclaimer