Congressional Research Service
Informing the legislative debate since 1914

Legal Sidebar

Overview of Governmental Action Under the Stored Communications Act (SCA)

August 3, 2022

The Stored Communications Act (SCA), 18 U.S.C. §§ 2701 et seq., governs access to stored wire and electronic communications such as emails and other online messages held by service providers. Congress passed the SCA as Title II of the Electronic Communications Privacy Act of 1986 (ECPA), which was enacted to address government wiretaps and other communications tracing issues. The SCA prohibits providers from sharing electronic communications with any person or entity but also contains exceptions, such as when the government compels the information. The SCA governs electronic communications and records "at rest" or in electronic storage held by providers. Other provisions of ECPA, such as the Wiretap Act, address communications "in transmission." Other federal laws, including the Communications Act of 1934, as amended, may prohibit communications-sharing conduct not covered by the SCA.

While the SCA was passed in 1986 to update communications privacy in light of rapidly changing technology of the time, modern electronic communications devices, applications, and online platforms have since outpaced the law. Government requests for the disclosure of communications may be of particular interest to Congress given (1) the general shift to online communications since the SCA was enacted and (2) the few updates to the law in the intervening decades.

This Legal Sidebar examines selected SCA provisions that govern government requests for electronic information from third parties. It also analyzes the Supreme Court's interpretation of a SCA government order for communications data in *Carpenter v. United States* and discusses possible considerations for Congress.

The SCA's Legal Framework

The Fourth Amendment of the U.S. Constitution protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" by the government. Accordingly, a government seizure of personal communications generally requires the issuance of a warrant based on probable cause due to an individual's "constitutionally protected reasonable expectation of privacy." This protection extends to communications and records kept in the physical home.

Sending an email or another kind of message online requires the user to give information to a company that transfers, processes, and holds the user's information. The principle known as the third-party doctrine

Congressional Research Service
https://crsreports.congress.gov
LSB10801

holds that the Fourth Amendment generally does not protect private information shared with third parties. Congress passed the SCA to address growing privacy concerns regarding technology and government searches and to provide statutory privacy protections for stored electronic communications where such communications may not be protected by the Fourth Amendment.

Provisions of the SCA most relevant to the government's access to communications and records include:

- § 2701, which is the SCA's general prohibition against obtaining, altering, or preventing access to electronic communications in storage by intentionally accessing communications without authorization. The prohibition has several exceptions, including circumstances when the conduct to access the communication is authorized by the government.
- § 2702, which prohibits providers of electronic communication services (or "ECS," including cell phone providers, email providers, or social media platforms) and remote computing services (or "RCS," such as cloud computing providers) to the public from knowingly divulging communications held in electronic storage to any person or entity. Similar to § 2701, there are statutory exceptions to § 2702. The Department of Justice has taken the position that § 2702's prohibition on voluntary disclosures does not apply to sharing aggregate, de-identified non-content data with the government so long as it does not identify or otherwise provide information about any particular subscriber or customer.
- § 2703, which identifies how government entities can compel providers to disclose electronic communication information through a court-issued warrant, a court order, or an administrative subpoena. While § 2703 provides different degrees of process for law enforcement to obtain different types of communications, it generally requires a warrant for new ECS communications content (held for 180 days or less) and less robust protection for older content and non-content information.
- § 2705, which sets out the process by which the government may obtain a non-disclosure order to delay notification to an individual or entity under investigation that the government has requested the disclosure of a communication or record pursuant to § 2703.

Against this statutory scheme, there are a number of ways that law enforcement can obtain information—such as text messages, emails, and private messages over social media—from a third-party provider. To obtain information held by entities covered by § 2703 of the SCA (i.e., ECS and RCS), law enforcement must obtain a search warrant, a court order, or a subpoena. For example, absent customer consent or another discrete exception, an RCS must generally disclose the contents of an electronic communication to law enforcement only if law enforcement obtains a court-issued warrant upon a showing of probable cause (§ 2703(b)(1)(A)). If notice to the customer is provided, law enforcement can obtain such information with a court order or an administrative subpoena upon a showing of relevancy to the investigation. For electronic communications held by an ECS for 180 days or less, only a court-issued warrant issued upon a showing of probable cause is sufficient to obtain such information (§ 2703(a)). Other kinds of non-content customer records, such as metadata, held by an ECS or RCS may be obtained by a search warrant, a court order, or a subpoena depending on the circumstances.

Carpenter v. United States

The Supreme Court considered the sufficiency of the SCA's privacy protections from the government under the Fourth Amendment in the 2018 case *Carpenter v. United States*. *Carpenter* held that the government's acquisition of an individual's historical cell-site location information (CSLI) via an SCA court order was a violation of the Fourth Amendment.

In the *Carpenter* case, the government obtained an individual's cellphone location records with a court order, as permitted by § 2703(d), that was supported by "specific and articulable facts showing that there are reasonable grounds to believe" that the records sought were "relevant and material to an ongoing criminal investigation." The Court determined that, since the individual had a reasonable expectation of privacy in the detailed record of his physical movements, the government was required under the Fourth Amendment to obtain a warrant supported by probable cause and that the court order was therefore insufficient.

The Court rejected the government's arguments that the Court should apply the third-party doctrine, which establishes that voluntarily providing data to a third party can extinguish a reasonable expectation that the data will be kept private. The Court distinguished historical CSLI from bank and home telephone records that the Court had held to be covered by the third-party doctrine in earlier cases, *United States v. Miller* and *Smith v. Maryland*. Instead, the Court in *Carpenter* compared the facts of the case to *United States v. Jones*, where the Court held that the police installing a GPS device on a suspect's vehicle was a Fourth Amendment search requiring a warrant. The Court also stated that cell phone location data is not "shared" in an affirmative sense because "a cell phone logs a cell-site record by dint of its operation," and carrying a cellphone on one's person is "indispensable to participation in modern society." The Court explained that, "[a]part from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data." The Court held that "in no meaningful sense does the user voluntarily 'assume the risk' of turning over a comprehensive dossier of his physical movements."

While the Supreme Court has not extended the protections of the data at issue in *Carpenter* to other types of communications held by service providers, some lower courts have extended the Fourth Amendment's protections over electronic communications further than the SCA. For example, the U.S. Court of Appeals for the Sixth Circuit recognized an exception to the third-party doctrine when it held that there is a reasonable expectation of privacy in the content of emails, requiring the government to obtain a warrant before obtaining a user's emails from a service provider.

Considerations for Congress

Past congressional proposals to amend the SCA have focused on removing the differences in protection between older and newer communications and clarifying whether the statute applies to congressional requests for communications. Proposals to amend the SCA that have been introduced in the 117th Congress include the NDO Fairness Act and the Government Surveillance Transparency Act of 2022, which would increase requirements for the government to obtain non-disclosure orders and set new requirements to notify individuals of the monitoring of their communications. The Fourth Amendment Is Not For Sale Act would prohibit the government from purchasing communications data from data brokers.

As the 117th Congress considers whether to amend the SCA, it may consider updating the law to better address modern internet services and data storage. Courts have, at times, struggled to apply the SCA in an evolving technological landscape. The SCA is a product of how the internet was used in 1986 and the limited range of internet services that existed at that time. Scholars observe that "[s]ervice providers now routinely store everything, and they can turn over everything to law enforcement," compared to the limited data stored by providers in the 1980s. A recent Ninth Circuit decision held that the government requiring a provider to preserve communications records and other evidence under § 2703(f) pending the issuance of a court order or other process "did not amount to an unreasonable seizure in violation of the Fourth Amendment," raising questions about what limitations might exist on government requests to providers to preserve the universes of data they store on their users.

While courts have found social media companies operating messaging services to be covered providers for purposes of the SCA, these cases involving social media websites and applications may suggest that

Congress has an interest in more clearly defining when and how these services fall under SCA coverage. Congress may also have an interest in reexamining the SCA in light of the practice of purchasing communications data through third-party "data brokers," such as when the government buys access to location data that originated with a provider from a broker.

Author Information

Jimmy Balser
Legislative Attorney

Disclaimer