

Stored Communications Act

From Wikipedia, the free encyclopedia

The **Stored Communications Act (SCA)**, [codified at 18 U.S.C. Chapter 121](#) §§ 2701–2712) is a law that addresses voluntary and compelled disclosure of "stored wire and electronic communications and transactional records" held by third-party [internet service providers](#) (ISPs). It was enacted as Title II of the [Electronic Communications Privacy Act](#) (ECPA, [Pub.L. 99–508](#), 100 [Stat.](#) 1848, enacted October 21, 1986).

The [Fourth Amendment to the U.S. Constitution](#) protects the people's right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures...." However, when applied to information stored online, the Fourth Amendment's protections are potentially far weaker. In part, this is because the Fourth Amendment defines the "right to be secure" in spatial terms that do not directly apply to the "reasonable expectation of privacy" in an online context. In addition, society has not reached clear consensus over expectations of privacy in terms of more modern (and developing, future) forms of recorded and/or transmitted information.

Furthermore, users generally entrust the security of online information to a third party, an ISP. In many cases, Fourth Amendment doctrine has held that, in so doing, users relinquish any expectation of privacy. The "third party doctrine" holds "...that knowingly revealing information to a third party relinquishes Fourth Amendment protection in that information."^[1] While a [search warrant](#) and [probable cause](#) are required to search one's home, under the third party doctrine only a subpoena and prior notice (a much lower hurdle than probable cause) are needed to compel an ISP to disclose the contents of an email or of files stored on a server.^[2] The SCA creates Fourth Amendment-like privacy protection for email and other digital communications stored on the internet. It limits the ability of the government to compel an ISP to turn over content information and noncontent information (such as logs and "envelope" information from email). In addition, it limits the ability of commercial ISPs to reveal content information to nongovernment entities.

Contents [\[hide\]](#)

- [1 Overview](#)
- [2 Constitutionality of Compelled Government Disclosure](#)
- [3 Robbins v. Lower Merion School District](#)
- [4 References](#)

Overview

[\[edit\]](#)

Section 2701 of the SCA provides criminal penalties for anyone who "intentionally accesses without authorization a facility through which an electronic communication service is provided or...

intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorize access to a wire or electronic communication while it is in electronic storage in such system."

The SCA targets two types of online service, "electronic communication services" and "remote computing services." The statute defines an electronic communication service as "...any service which provides to users thereof the ability to send or receive wire or electronic communications." A remote computing service is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system." Section 2703 of the SCA describes the conditions under which the government is able to compel an ISP to disclose "customer or subscriber" content and non-content information for each of these types of service:

- **Electronic communication service.** If an unopened email has been in storage for 180 days or less, the government must obtain a search warrant. There has been debate over the status of opened emails in storage for 180 days or less, which may fall in this category or the "remote computing service" category.^[2]

- **Remote computing service.** If a communication has been in storage for more than 180 days or is held "solely for the purpose of providing storage or computer processing services" the government can use a search warrant, or, alternatively, a subpoena or a "specific and articulable facts" court order (called a 2703(d) order) combined with prior notice to compel disclosure. Prior notice can be delayed for up to 90 days if it would jeopardize an investigation. Historically, opened or downloaded email held for 180 days or less has fallen in this category, on the grounds that it is held "solely for the purpose of storage."^[2]

§ 2702 of the SCA describes conditions under which a public ISP can voluntarily disclose customer communications or records. In general, ISPs are forbidden to "divulge to any person or entity the contents of any communication which is carried or maintained on that service." However, ISPs are allowed to share "non-content" information, such as log data and the name and email address of the recipient, with anyone other than a governmental entity. In addition, ISPs that do not offer services to the public, such as businesses and universities, can freely disclose content and non-content information.^[2] An ISP can disclose the contents of a subscriber's communications authorized by that subscriber.^[3]

Constitutionality of Compelled Government Disclosure

[\[edit\]](#)

With respect to the government's ability to compel disclosure, the most significant distinction made by the SCA is between communications held in electronic communications services, which require a search warrant and probable cause, and those in remote computing services, which require only a subpoena or court order, with prior notice. This lower level of protection is essentially the same as would be provided by the Fourth Amendment—or potentially less, since notice can be delayed indefinitely in 90-day increments. Orin Kerr argues that, "the SCA was passed to bolster the weak Fourth Amendment privacy protections that applied to the Internet. Incorporating those weak

Fourth Amendment principles into statutory law makes little sense."^[2] In *Warshak v U.S.* (2007)^[4] this point of view found fleeting support from a panel of the Sixth Circuit, which ruled that a reasonable expectation of privacy extends to emails that would otherwise fall under the SCA's lower level of protection: "Where the third party is not expected to access the e-mails in the normal course of business, however, the party maintains a reasonable expectation of privacy, and subpoenaing the entity with mere custody over the documents is insufficient to trump the Fourth Amendment warrant requirement." Subsequently, the Sixth Circuit *en banc* vacated the panel's ruling and remanded for dismissal of the constitutional claim, reasoning that, because the Court had "no idea whether the government will conduct an *ex parte* search of Warshak's e-mail account in the future and plenty of reason to doubt that it will," the matter was not ripe for adjudication.^[5] [Zerwillinger](#) and Sommer^[6] observed that this decision erected a barrier to "prospective" challenges by individuals with reason to believe they will be targets of surveillance. While Warshak's civil case ended without a resolution to this issue, his criminal case provided another opportunity. In *United States v. Warshak* (2010)^[7] the Sixth Circuit found that email users have a Fourth Amendment-protected reasonable expectation of privacy in the contents of their email accounts and that "to the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional."^{[7][8]}

Robbins v. Lower Merion School District

[\[edit\]](#)

The Act was invoked in the 2010 *Robbins v. Lower Merion School District* case, where plaintiffs charged two suburban Philadelphia high schools secretly spied on students by surreptitiously and remotely activating webcams embedded in school-issued laptops the students were using at home, violating their right to privacy. The schools admitted to secretly snapping over 66,000 webshots and screenshots, including webcam shots of students in their bedrooms.^{[9][10]}

References

[\[edit\]](#)

- ¹ [^] Kerr, Orin S., *The Case for the Third-Party Doctrine*, Michigan L. Rev., Vol. 107, 2009; GWU Legal Studies Research Paper No. 421.
- ² [^] ^a ^b ^c ^d ^e Kerr, Orin S., *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, George Washington L. Rev. (2004). Available at [doi:10.2139/ssrn.421860](#).
- ³ [^] 18 U.S.C. § 2701(c)(2) ^[1]
- ⁴ [^] Warshak v United States (2007)
- ⁵ [^] *Warshak v. United States*, 532 F.3d 521 (6th Cir. 2008) (*en banc*)
- ⁶ [^] Marc Zwillinger, Jacob Sommer. "Warshak Decision: Sixth Circuit's En Banc Reversal in Warshak Sidesteps Constitutionality of Stored Communication Act's Delayed Notification Provision," ^[2] , BNA Privacy & Security Law Report, Vol. 7, No. 31, (Aug. 4, 2008).
- ⁷ [^] ^a ^b *United States v. Warshak*, No. 08-3997 (6th Cir. Dec. 14, 2010).
- ⁸ [^] Kevin Bankston, *Breaking News on EFF Victory: Appeals Court Holds that Email Privacy Protected by Fourth Amendment*, EFF DeepLinks (Dec. 14, 2010).
- ⁹ [^] Doug Stanglin (February 18, 2010). "School district accused of spying on kids via laptop webcams". *USA*

Today. Retrieved February 19, 2010.

10. [^] ["Initial LANrev System Findings"](#) , LMSD Redacted Forensic Analysis, L-3 Services – prepared for [Ballard Spahr](#) (LMSD's counsel), May 2010. Retrieved August 15, 2010.

Categories (+⁺):

United States federal computer law legislation (–) (±)

| United States federal defense and national security legislation (–) (±) | 1986 in law (–) (±)

| Privacy of telecommunications (–) (±) | Privacy law in the United States (–) (±) | (+)