# Background Information:

# **Federal Stored Communications Act**

The federal Stored Communications Act (SCA)[[1]](#footnote-1) was enacted in 1986 to provide Fourth Amendment-like privacy protections for certain electronic communication and computing services. In essence, it “creates a zone of privacy to protect internet subscribers from having their personal information wrongfully used and publicly disclosed . . . .” *In re* Subpoena Duces Tecum to AOL LLC, 550 F. Supp. 2d 606 (E.D. Va. 2008). The law balances this interest, however, with the needs of government agencies to access this information for legitimate law enforcement purposes. The Act generally prohibits governments agencies from compelling disclosure of certain electronic information from third-party service providers, without obtaining a warrant or, in some instances, a court order or administrative subpoena. It also limits the circumstances under which the third-party service providers may disclose the information voluntarily to a government or private entity.

The following analysis focuses on the application of the SCA when a government entity contracts with an external service provider to furnish remote communication, software, processing, platform, or storage services for a government’s electronic information. Although the SCA does not directly regulate the relationship between a government entity (as customer) and a service provider, several of its provisions may (perhaps inadvertently) limit a government-customer’s ability to retrieve its electronic information from the service provider. This is because the SCA, in relevant part, generally prohibits certain service providers from voluntarily divulging content and, under certain circumstances, non-content information related to an electronic communication, unless certain exceptions apply. In effect, these provisions could prohibit a government entity from retrieving its own electronic information from the service provider. This is problematic for a number of reasons, not the least of which is that some of the electronic information likely is subject to public access requirements under the State’s public records laws.

The Act’s prohibitions apply to two types of services—electronic communication services and remote computing services. The relevant provisions of each are summarized below.

Electronic Communication Services

Any person or entity that provides *electronic communication services* to the *public* may not “divulge . . . the *contents* of a communication while in *electronic storage* by that service.” 18 U.S.C. 2702(a)(1) (emphasis added).

* An *electronic communication service* (ECS) is defined as “any service which provides to users thereof the ability to send or receive wire or electronic communications.” 18 U.S.C. 2510(15). E-mail, text messaging and electronic bulletin boards likely constitute ECSs.
* The SCA privacy protections apply only when a provider furnishes ECSs *to the public.* The statute does not define the term “public” but it likely requires that services be available to any member of the general population who complies with the provider’s requisite procedures and pays any requisite fees. An ECS provider does not furnish services to the public, however, if its services are only available to those with a special relationship with the provider, such as when an employer provides e-mail accounts to its employees. *See* Andersen Consulting LLP v. UOP, 991 F.Supp. 1041 (N.D. Ill. 1998). Thus, if a local government establishes and maintains its own internal e-mail system, the SCA does not apply. On the other hand, if a local government contracts with an external provider to furnish e-mail or text messaging services to its employees and officials, the SCA may apply (if other applicable requirements are satisfied).
* The SCA privacy protections apply to the *contents* of a communication. The statute defines “content” as information “concerning the substance, purport, or meaning” of a communication. 18 U.S.C. §2510(8). To illustrate, with respect to an e-mail, the content likely comprises the actual text of the message, as well as the subject line. (There are separate provisions that prohibit the disclosure of non-content information to a government entity, such as logs of account usage, basic subscriber information, and e-mail addresses of intended recipients, but there is an exception when the government is the subscriber to the external provider’s services.)
* Finally, the SCA privacy protections apply only while the contents of an electronic communication are held in *electronic storage* by the service provider. Electronic storage is defined by statute and (at least potentially) has a very limited scope. It applies to:

1. “temporary, intermediate storage . . . incidental to the electronic transmission” of the communication; and
2. copies made by the service provider for “backup protection.”

* There is a split in authority as to how broadly to interpret this statutory language. The traditional understanding was that “electronic storage” referred to temporary storage made in the course of transmission by a service provider—for example, storing an e-mail that was received by a recipient’s service provider but not yet opened by the recipient. It also referred to administrative backup copies of electronic transmissions made by a provider to ensure system integrity. It was not understood to encompass post-transmission storage of communications for the recipient, such as long-term storage of opened e-mails. *See, e.g.,* United States v. Weaver, 636 F. Supp. 2d 769 (C.D. Ill. 2009) (holding that opened e-mails on web-based e-mail systems or not in electronic storage for purposes of the SCA). A few courts have rejected this traditional understanding, though, and applied a much broader interpretation of the statutory provisions. *See, e.g.,* Theofel v. Farey-Jones, 341 F.3d 978 (9th Cir. 2003) (holding that e-mail stored on a provider’s server indefinitely is stored as a form of backup protection for purpose of satisfying the SCAs electronic storage provisions until “the underlying message has expired in the normal course,” regardless of whether the e-mail has been accessed).

There are certain statutory exceptions to the general prohibition against disclosing the contents of an electronic communication outlined above. An ECS service provider may voluntarily disclose the contents of an electronic communication held in electronic storage if one of eight statutory exceptions applies. *See* 18 U.S.C. § 2702(b). In relevant part, a service provider may voluntarily reveal the contents:

1. To an addressee or intended recipient of such communication or an agent of such address or intended recipient;
2. With the lawful consent of the originator or an addressee or intended recipient of such communication; and
3. As may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service.

*Note that an ECS service provider may not divulge the contents of an electronic communication held by the ECS provider in electronic storage at the request, or with the consent, of the subscriber (or customer) to the service.*

*Remote Computing Service*

Any person or entity that provides *remote computing services* to the public may not “divulge . . .the *contents* of any communication which is *carried or maintained on that service* on behalf of, and *received by means of electronic transmission* *from* (or created by means of computer processing of communications received by means of electronic transmission from), *a subscriber or customer* of such service *solely for the purpose of providing storage or computer processing services* to such subscriber or customer, *if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing* . . . .” 18 U.S.C. §2702(a)(2) (emphasis added).

* A *remote computing service* (RCS) is defined as “the provision to the public of computer storage or processing services by means of an electronic communication system . . . .” *See* 18 U.S.C. §2711(2).
* The SCA privacy protections apply only when an RCS provider furnishes services *to the public*. The term “public” likely has the same meaning as outlined above for ECS providers.
* The SCA privacy protections apply to the *contents* of a communication. The statute defines “content” as information “concerning the substance, purport, or meaning” of a communication. 18 U.S.C. §2510(8).
* The SCA privacy protections apply only when an RCS provider meets the following additional criteria:
  + The *data* *must be received electronically* from the customer or subscriber;
  + The *content must be carried or maintained* by the service provider *solely for the purpose of providing storage or computer processing services to the customer*; and
  + The *provider may not be authorized to access the customer’s content for any purposes other than providing storage or computer processing*.

There are certain statutory exceptions to the general prohibition outlined above. A RCS service provider may voluntarily disclose the contents of an electronic communication held in electronic storage if one of eight statutory exceptions applies. *See* 18 U.S.C. § 2702(b). In relevant part, a service provider may voluntarily reveal the contents:

1. To an addressee or intended recipient of such communication or an agent of such address or intended recipient;
2. With the lawful consent of the originator or an addressee or intended recipient of such communication;
3. With the lawful consent of the subscriber to the service; and
4. As may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service.

*Note that unlike an ECS service provider, an RCS service provider may divulge the contents of a communication to the subscriber (or customer) of the service.*

**Access to Electronic Information by Government-Subscriber**

Given these statutory provisions, when, and under what circumstances, does the SCA prevent (or hinder) a government from accessing or obtaining copies of its employee’s or official’s e-mails or text messages that are hosted on a third-party system?

* If the third-party provider does not meet the criteria as an ECS or RCS provider, then the SCA does not apply and the government-subscriber may access the contents of e-mails or text messages, subject to any contractual limitations imposed by the provider and (at least potential) Fourth Amendment privacy protections.
* If the third-party provider is an ECS provider and holds the contents of the communication in electronic storage, then the government-subscriber likely only may access the contents of e-mails or text messages with the consent of the originator, or an addressee or intended recipient, of the communication at issue. This restriction is in addition to any contractual limitations imposed by the provider and any Fourth Amendment privacy protections.
* If the third-party provider is a RCS provider, then the government-subscriber may provide the requisite consent, authorizing the service provider to release the contents of the e-mails or text messages. The government is still subject to any contractual limitations imposed by the provider and any Fourth Amendment privacy protections.

The more difficult inquiry is determining whether a provider is an ECS provider that holds the contents of a communication in electronic storage or an RCS provider.

**Summary of Key Cases to Date**

The following are two cases in which a government entity procured the services of an external service provider to provide text messaging services and then had some difficulties in obtaining the contents of the text messages from the service providers due (at least ostensibly) to the SCA. The two courts reach almost diametrically opposed conclusions as to the applicability of the SCA, and the limitations it imposes, when a government entity contracts with an external service provider to furnish text messaging services. The cases illustrate the potential minefields that local governments may face when contracting with “cloud” service providers, particularly for e-mail or text messaging services.

***Quon v. Arch Wireless Operating Company, Inc*., 529 F.3d 892 (9th Cir. 2008)**

The City of Ontario, California, contracted with Arch Wireless to provide text-messaging services for certain city employees, who were issued Arch Wireless pagers. Any message sent or received by one of the pagers followed the following transmittal path: the message would leave the originating pager and be received by one of Arch Wireless’ receiving stations. The message then entered Arch Wireless’ computer network and was sent to a computer server. A copy of the message was archived and the message was stored on the server for a period of up to 72 hours, until the recipient pager was ready to receive delivery of the message. The City did not capture or store the content of the text messages in its own IT system. The only record of the texts existed in Arch Wireless’ system.

The City did not have an official policy governing the use of text-messaging devices by employees. It did have a general “Computer Usage, Internet and E-mail Policy” (Policy) that prohibited the use of city-owned computers and all associated equipment and software programs, including e-mail and the Internet, for personal reasons. The Policy also specified that the City reserved the right to record and monitor all network activity, including e-mail and Internet use, with or without notice, and that users should have no expectation of privacy or confidentiality when using these resources. All employees were required to sign an acknowledgement that they read and understood the Policy. After the City subscribed to the pager service, city employees were informed verbally that the pagers were covered by the Policy.

At least one manager (Lieutenant Duke) instituted an unofficial policy regarding the use of pagers by certain law enforcement personnel, though. The City’s contract with Arch Wireless allowed each pager 25,000 characters per billing period, after which the City was required to pay overage charges. Lieutenant Duke allowed employees to pay for any overage. There was an implicit agreement that if an employee paid for the overage, the Lieutenant would not inquire into whether the employee used the pagers for personal reasons, as well as for official City business. The Lieutenant collected overages from several employees for a period of time, after which he became tired of serving as a bill collector. He subsequently performed an audit of the contents of the employees’ text messages to determine if the messages were work related. In order to perform the audit, the Lieutenant requested transcripts from certain pagers. One of the officers whose transcripts were requested was Jeff Quon.

The audit revealed that Quon made extensive use of his pager to send and receive personal messages, many of which were sexually explicit. The police chief eventually referred the matter to internal affairs to determine if Quon wasted City time due to his excessive personal messaging.

Quon subsequently instituted suit against the City alleging violations of the SCA and the Fourth Amendment. With respect to his SCA claim, Quon asserted that Arch Wireless violated the Act by disclosing the contents of the pager messages to the City without Quon’s consent. The district court rejected Quon’s SCA claim, concluding that Arch Wireless provided a RCS service in storing the pager messages. The City, as subscriber to the service, was statutorily authorized to consent to the release of the content of the messages.

The Ninth Circuit disagreed. Noting that Arch Wireless maintained an archived copy of the text messages, the court held that it was not providing a RCS, but rather an ECS. The SCA defines an ECS as “any service which provides to users thereof the ability to send or receive wire or electronic communications.” The court found that the text-messaging services provided to the City by Arch Wireless fit this definition. But, recall that the SCA only prohibits the disclosure of the contents of a communication by an ECS provider while that communication is in “electronic storage” and unless a statutory exception applies. Electronic storage is defined by the SCA to include “any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof” and “any storage of such communication by an electronic communication service for purposes of backup protection of such communication.” The court determined that the text messages at issue were not in temporary, intermediate storage. It held, however, that by archiving the text messages in its server, Arch Wireless was storing the messages for the purposes of backup protection. The court noted that it was unclear whether Arch Wireless created the archive copies of the messages for its own purposes or for the City, but it found the distinction meaningless for purposes of its analysis.

Because Arch Wireless was an ECS provider and the text-messages were communications held in electronic storage, Arch Wireless was prohibited from disclosing the contents of the text messages to anyone, unless one of the statutory exceptions in 18 U.S.C. §2702(b) applied. The court determined that none of the exceptions were satisfied. Notably, the City, as subscriber to the messaging service, was not statutorily authorized to consent to the disclosure of the contents of the text messages. This is true even though at least some of the text messages related to City business and likely constituted public records subject to public access under the state’s public records law.

***Flagg v. City of Detroit*, 252 F.R.D. 346 (E.D. Mich. 2008)**

The City of Detroit, Michigan, contracted for text messaging services with SkyTel, Inc. SkyTel provided the text messaging services and devices to various City officials and employees for a period of time. At some point the City discontinued its contract with SkyTel, but the company continued to maintain copies of at least some of the text messages sent and received by City officials and employees during the contract period.

In a civil suit alleging improper conduct by certain city employees and officials, the plaintiff served subpoenas to SkyTel seeking disclosure of certain text messages. The City filed a motion objecting to the third-party subpoena. Specifically, the City claimed, among other things, that the SCA prohibited SkyTel, as an RCS provider, from disclosing the contents of the text messages to the plaintiff absent specific consent from the City, which it refused to grant.

Although the specific issue before the court was whether the Plaintiff could compel disclosure of the text messages directly from SkyTel, the court analyzed the issue as if the request for the text messages had been made to the City directly, pursuant to the civil discovery rules. Under the Federal Rules of Civil Procedure, a party is required to disclose information that is relevant to the civil suit and that is within the party’s possession, custody or control. Although the record did not include information about the actual contract terms between the City and SkyTel, the court concluded that the City must have had “control” over the text messages at issue. The court’s analysis was colored, in part, by the fact that at least some of the records at issue constituted public records subject to public access. The court found it impossible to believe that the City would engage in a contract whereby it would relinquish control over its public records because this likely would violate state law.

The court then analyzed whether the SCA prohibited SkyTel from disclosing the contents of the text messages to the City. Under a number of alternative theories, the court held that it did not.

First, the court indicated that if SkyTel was producing the text messages to the City pursuant to its contractual agreement, it might not be “divulging” the contents of the communications for purposes of the SCA. Under this theory, it did not matter if SkyTel was an ECS or a RCS provider. In either case, SkyTel would not violate the SCA by providing the contents of the messages to the City.

Second, the court held that SkyTel was neither a RCS or an ECS provider with respect to the text messages at issue. To constitute a RCS, among other things, the provider must not be “authorized to access the contents of any such communications for purposes of providing any services other than storage or computer process.” In a strict interpretation of this requirement, the court held that SkyTel was authorized to access the City’s messages to provide the additional “service of retrieval” for the stored text messages. And, to constitute an ECS, the provider had to hold the communications in electronic storage, as defined by the SCA. The court held that the text messages were not held in temporary, intermediate storage or in backup storage. SkyTel had ceased providing text messaging service to the City and could not be holding the messages for temporary, intermediate storage. Furthermore, the text messages archived by SkyTel were the only available records of these communications and, because of this, they did not constitute “backup” copies. (The court engaged in an extensive discussion of the *Quon* case, but ultimately rejected the Ninth Circuit’s broad interpretation of what constitutes a backup copy for purposes of the SCA.)

Third, even if SkyTel was a RCS or an ECS provider, the court concluded that at least one of the statutory exceptions applied. If it was a RCS provider, the City, as subscriber, could consent to the disclosure. And the court found that the City actually had an obligation to consent under the civil discovery rules. And, if the City was an ECS provider, the City could compel its employees to consent to the disclosure. (The court cited to several cases in which courts had held that employers may compel their employees to turn over records related to the scope of their employment.)

The court ultimately directed the Plaintiff to seek the requested text messages from the City directly. It further held, based on the analysis set forth above, that SkyTel could disclose the content of these communications to the City without running afoul of the SCA.

1. The Stored Communications Act is part of the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 201 (codified as amended at 18 U.S.C. §§ 2701-2711). [↑](#footnote-ref-1)