Coates' Canons Blog: Outsourcing Local Government Communications: Implications of the Federal Stored Communications Act

By Kara Millonzi

Article: https://canons.sog.unc.edu/outsourcing-local-government-communications-implications-of-the-federal-stored-communications-act/

This entry was posted on April 26, 2012 and is filed under Open Government, Public Records (Electronic)

In August 2011, the City of HighTech contracted with an external SaaS (software as a service) provider to host its e-mail system. The basic parameters of the contract require the SaaS provider to furnish e-mail service to all city employees and officials. City employees and officials access the e-mail system through a web-based portal from any computer or device with an internet connection. Each user may manage her e-mails by keeping them in her inbox or moving them to one or more file folders set up in the e-mail system. There is no option to download the e-mails to a user's computing device or to the city's IT system. However, a user may copy and paste the substance of the e-mails into word processing files and save them to her hard-drive or the city's IT system.

According to the provisions of the contract, the SaaS provider will store any unopened e-mails and opened e-mails that are not deleted by the user indefinitely on its active system. If a user deletes an e-mail, it is retrievable for a period of 30 days, after which it is permanently deleted from the SaaS provider's system. The SaaS provider does not maintain a back-up or "archive" copy of any of the e-mails.

The city manager has instructed all employees and officials to "store" any e-mails that contain substantive information that must be retained according to the state's public records law in appropriate file folders (labeled according to subject matter) in the e-mail system. None of these records are available on the city's IT system.

The city manager recently received a public records request for copies of all e-mails sent or received by Emme Bezzler, a former city clerk, during the six month period from September 1, 2011 through March 1, 2011. Emme was fired by the city for cause on March 1, 2011. She since has fled the state in fear of criminal prosecution.

Before her termination, the city failed to verify whether or not Emme retained any records in her e-mail folders that might be subject to public access and/or subject to retention requirements under the State's public records law. (Emme did not save the content of any of the e-mails as word processing files on the city's IT system.) The only way to determine if records exist that are responsive to the public records request is to access Emme's e-mail account. Unfortunately, the city failed to obtain Emme's password for her city e-mail account before she skipped town. Instead, the city requests that the SaaS provider give the city access to Emme's stored e-mails or provide the city with a copy of the e-mails. The SaaS provider refuses, claiming that federal law prohibits it from disclosing the contents of the e-mails in Emme's account to the city, even though the city is the subscriber to the e-mail service.

The SaaS provider may be correct. The federal law at issue is the **Stored Communications Act (SCA)** and it restricts access to certain electronically stored information by third-party providers, even in the circumstances described above.

Stored Communications Act

The SCA was enacted in 1986 to provide Fourth Amendment-like privacy protections for certain electronic communications 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 Act generally prohibits government 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. (My colleague, Jeff Welty, has **written** about the implications of the Act in the law enforcement context.) The Act also limits the circumstances under which the third-party service providers may disclose the

information voluntarily to a government or private entity, which is the subject of this post.

The SCA does not directly regulate the relationship between a government entity and a service provider, but several of its provisions nonetheless may limit a government-customer's ability to retrieve its electronic information from the service provider. Significantly, among the electronic information that may be restricted are e-mails and text messages that are sent or received by government employees and officials when the government agency contracts with a third-party provider for these services.

Specifically, the Act specifies that 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). Each of these terms is discussed below. (Note that electronic communications services are not the only type of electronic information regulated by the Act. Other provisions will be discussed in future posts.)

Electronic Communications Service

The Act defines *electronic communications service* (ECS) 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 board services likely constitute ECSs. *See, e.g.,* Glazer v. Fireman's Fund Insurance Co., 2012 WL 1197167 (S.D.N.Y. Apr. 5, 2012) (noting that several courts have held that email providers and social networking websites are ECS providers); Jennings v. Jennings, 389 S.C. 190, 697 S.E.2d 671 (2010) (holding that Yahoo is a provider of electronic communication services).

Provided to the Public

The Act limits its coverage to ECSs that are provided 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. An ECS provider does not furnish services to the public, however, if its services only are 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. If, however, a local government contracts with a third-party provider to furnish e-mail or text messaging services to its employees and officials, the SCA may apply.

In North Carolina, some local governments contract with the State to provide e-mail services. Under these circumstances, is the State providing electronic communications services to the public such that it may be subject to the SCA? The answer is unclear. On the one hand, the State arguably has a special relationship with local governments (particularly counties, which are considered "arms of the State" for many purposes). The relationship is not exactly akin to that of an employer/employee, though. And the local governments pay the State for the e-mail services in the same manner as they would a private provider. The safest approach may be to assume that the e-mail service provided by the State is covered by the SCA and follow the guidance set forth below to ensure that the unit has full access to all e-mails (or at least those e-mails that constitute public records).

Divulging Contents of Electronic Communications

The provision at issue is further limited to protecting the contents of an electronic communication. The statute defines "content" as information "concerning the substance, purport, or meaning" of a communication. 18 U.S.C. §2510(8). With respect to an e-mail, the content likely comprises the actual text of the message and the subject line, but not the other header information. (There are separate provisions of the Act 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 or phone numbers of intended recipients, but there is an exception when the government is the subscriber to the external provider's services. 18 U.S.C. 2703(c).)

Held in Electronic Storage

Finally, the provision only applies while the contents of an electronic communication are held in electronic storage by the service provider. 18 U.S.C. §2510(17) defines "electronic storage" as

(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.

Subsection (A) is limited to electronic communications, such as e-mails and text messages, which have not yet been accessed by their intended recipients. *See, e.g.,* United States v. Weaver, 636 F.Supp.2d 769 (C.D. Ill. 2009); *In re* DoubleClick, Inc. Privacy Litig., 154 F.Supp.2d 497 (S.D.N.Y. 2001).

There is a split of authority as to how broadly to interpret Subsection (B). Some courts have held that electronic communications held in post-transmission storage (whereby the e-mails or text messages are retained on the provider's system after they have been accessed by the intended recipients) are not stored for purposes of backup protection and, therefore, not covered by the SCA. *See, e.g.,* United States v. Weaver, 636 F.Supp. 2d 769 (C.D. Ill, 2009); Flagg v. City of Detroit, 252 F.R.D. 346 (E.D. Mich. 2008); Fraser v. Nationwide Mut. Ins. Co., 135 F.Supp.2d 623 (E.D.Pa. 2001), *aff'd on other grounds*, 352 F.3d 107 (3rd Cir. 2003).

Other courts have adopted a much broader interpretation of what constitutes backup protection. The leading case is *Theofel v. Farey-Jones*, 341 F.3d 978 (9th Cir. 2003). In *Theofel* the Ninth Circuit held that e-mail stored on a provider's server indefinitely is stored as a form of backup protection for purpose of satisfying the SCA's electronic storage provision until "the underlying message has expired in the normal course," regardless of whether the e-mail has been accessed. *See also* Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F.Supp.2d 548 (S.D.N.Y. 2008) ("[E]-mail stored on an electronic communication service provider's systems after it has been delivered, as opposed to e-mail stored on a personal computer, is a stored communication subject to the SCA."). Thus, if an entity provides e-mail or text messaging services to the public it likely may not divulge the contents of the electronic communications while those communications remain on the entity's system regardless of whether or not the communications have been accessed by the intended recipients.

Exceptions to SCA Prohibitions

But the very purpose of an electronic communications service is to transmit communications from one person or entity to another. Surely there must be exceptions to the general prohibition against divulging the contents of an electronic communication. In fact, there are eight statutory exceptions to the general prohibition, but they are fairly limited in scope. *See* 18 U.S.C. §2702(b). In relevant part, a service provider may voluntarily reveal the contents of a communication to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient. A service provider also may reveal the contents with the lawful consent of the originator or an addressee or intended recipient of such communication. And a service provider may disclose the contents "as may be necessarily incident to the rendition of the service. . . ." Significantly, however, a service provider may not divulge the contents of an electronic communication held in electronic storage to the subscriber to the service. That means that if an entity contracts with a service provider for e-mail or text messaging services, the entity itself (or the entity's management or leadership) does not have automatic access to the contents of the electronic communications sent or received by the entity's employees and officials.

This could prove particularly problematic for a government agency that must comply with public records requirements and provide public access to certain electronic communications. In *Quon v. Arch Wireless Operating Company, Inc.*, 529 F.3d 892 (9th Cir. 2008), the Ninth Circuit held that a third-party text messaging provider violated the SCA when it released transcripts of text messages sent and received by city employees to the city pursuant to a city audit. The court determined that the third-party was providing an ECS to the public and that the text messages at issue were retained in electronic storage as defined under the Act. Thus, the third-party provider needed the consent of the addressee or intended recipients of the text messages to disclose the content of those messages to the city.

Intersection of SCA and North Carolina Public Records Requirements

In North Carolina, a public record is defined broadly to include "all documents, papers, letters, maps, books, photographs, films, sound recordings, magnetic or other tapes, electronic data?processing records, artifacts, or other documentary material, regardless of physical form or characteristics, made or received pursuant to law or ordinance in connection with

the transaction of public business . . . ." **G.S. 132-1**. And there is a broad right of public access to these records, subject only to specific statutory exceptions. **G.S. 132-6**. Furthermore, certain public records (those with more than fleeting value) are subject to **retention requirements**, as promulgated by the Government Records Branch of the State's Division of Historical Resources.

Most of the information in a text message sent or received by public officials and employees in the performance of their job duties is of no lasting value and may be deleted as soon as the message has served its useful purpose. That also is true of many e-mail messages. But some text and e-mail messages are public records that must be retained for some period of time. (Recall that retention of a public record is based on subject matter, not on the form or format of the record.) A unit must make sure it has ready access to the public records that must be retained to ensure compliance with the retention schedules and to respond to any public record requests. Furthermore, even if a custodian of a text message or e-mail could have deleted it according to the retention schedules, if the message was not deleted it still is subject to public access unless one of the statutory exceptions applies.

G.S. 132-6.1 specifies that "no public agency shall purchase, lease, create, or otherwise acquire any electronic data?processing system for the storage, manipulation, or retrieval of public records unless it first determines that the system will not impair or impede the agency's ability to permit the public inspection and examination, and to provide electronic copies of such records." Although this provision does not directly address the issue of outsourcing electronic communication systems, certainly the spirit of the provision suggests that a local government should not contract with an external provider if doing so impairs the public's access to public records.

Ensuring Access to Public Records Retained on External Systems

What should a government agency that outsources its e-mail or text messaging services do to protect its access to its public records?

First, the government should work closely with the external provider to ensure that the contract provisions recognize the unique nature of government operations and the state law requirements related to public records. (My colleague, Shannon Tufts, has compiled a list of contracting considerations for government entities that outsource information technology services, including e-mail and text messaging.)

Second, the unit should obtain signed consent agreements from all of its employees and officials who use the e-mail or messaging systems authorizing the third-party provider to disclose to the unit all electronic communications sent or received through the external system. A unit may wish to verify with the external provider that it would accept the particular consent agreement. (The government also should ensure that whatever policies and practices it adopts with respect to accessing personal (non-public record) e-mail and text messages sent or received through the third-party's system do not violate the employees' or officials' Fourth Amendment rights. *See* City of Ontario v. Quon, 560 U.S. ___ , 130 S. Ct. 2619 (2010).)

Finally, to ensure proper preservation of public records that are subject to retention a government unit may wish to establish a process whereby individual record custodians save the public records to the government's IT system instead of relying on storage through the external provider's system.

Links

- www.law.cornell.edu/uscode/text/18/part-I/chapter-121
- sogpubs.unc.edu/electronicversions/pdfs/aojb0905.pdf
- www.ncleg.net/EnactedLegislation/Statutes/HTML/BySection/Chapter_132/GS_132-1.html
- www.ncleg.net/EnactedLegislation/Statutes/HTML/BySection/Chapter_132/GS_132-6.html
- www.records.ncdcr.gov/
- www.ncleg.net/EnactedLegislation/Statutes/HTML/BySection/Chapter_132/GS_132-6.1.html
- www.cpt.unc.edu/documents/Cloud_contractV3_000.pdf