Stored Communications Act

Lisa Soronen
State and Local Legal Center
lsoronen@sso.org (202) 434-4845

Before you Search an Employee's Email…

- First don't forget the 4th Amendment
  - *O'Connor v. Ortega*, 480 U.S. 700 (1987)
  - *Ontario v. Quon*, 560 U.S. __ (2010)
- Then think about whether the Stored Communications Act applies

Stored Communications Act

- 18 U.S.C. §§ 2701-2712 (most relevant sections are 2701-2702)
- Notice the Act is from **1986**
- Generally: purpose of the act is to prevent network service providers from disclosing content of private communications to the government and other entities
- More specifically: "customers" and "subscriber" have rights to information held by "electronic communication service" and "remote computing service" providers

Forest v. Trees

- Do searching the following without consent violate the Stored Communications Act (SCA)?
  - Email on an employer owned and operated email network -- No
  - Email or texts where the employer is not the service provider -- Maybe
  - Personal email – Yes

Why Did Congress Pass the SCA?

- Why is the Fourth Amendment not enough?
  - Information held by internet service providers (third parties) might not be protected by the Fourth Amendment
  - Grand juries can easily compel disclosure of information protected by the Fourth Amendment
  - Internet service providers are usually private actors
- Source: Orin S. Kerr, A User's Guide to the SCA, GW Law Review (2004)

Section 2701

- (a) **Offense—** Except as provided in subsection (c) of this section whoever—**(1) intentionally accesses without authorization a facility through which an electronic communication service is provided**; or (2)intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.
- (c) **Exceptions.—** Subsection (a) of this section does not apply with respect to conduct authorized—(1) by the person or **entity providing a wire or electronic communications service**

In Plain English Please…

- No one can enter without permission a service that allows users to send and receive messages *unless* they are the provider of that service

Section 2702

- (a) **Prohibitions.—** Except as provided in subsection (b) or (c)—(1)a person or entity providing an **electronic communication service** to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and
- (2)a person or entity providing **remote computing service** to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service
- (b) **Exceptions for disclosure of communications.—** A provider described in subsection (a) may divulge the contents of a communication (3) with the lawful consent of the originator or an addressee or intended recipient of such communication, **or the subscriber in the case of remote computing service**

In Plain English Please…

- Providers of electronic communication services (ECS) to the public may not disclose information in electronic storage
- Providers of remote communication services (RCS) to the public may not disclose communication *except to subscribers*

Definitions

- ECS—”any service which provides to users thereof the ability to send or receive wire or electronic communications”
  - In plain English: ECS facilitates communication between sender and receiver—Verizon, Comcast, Facebook, etc.
- RCS—”the provision to the public of computer storage or processing services by means on an electronic communications system”
  - In plain English: off-site computer that stores or processes data

Keeping it Simple

- Critical question for employers regarding the Stored Communication Act:
  - Are you planning on searching an email on an employer owned and operated email network?
  - If yes, the Stored Communications Act is not violated

Employer Owned and Operated System

- Why is the SCA not violated?
  - Section 2701(c)(2) creates is an exception for an "entity providing a wire or electronic communications service" accessing electronic communication
  - In other words, you can disclose your information to yourself

Relevant Case Law

- *Fraser v. Nationwide Mutual Insurance Co.*, 352 F.3d 107 (2003) (SCA was not violated when Nationwide searched the emails of a disloyal employee stored on Nationwide's system which Nationwide administered)
- *Bohach v. City of Reno*, 932 F. Supp. 1232 (D. Nev. 1996) (Reno police department could retrieve text messages on the police department computer system where the department is the service provider)

Brain Teaser

- Facts: My work email is accessible by my personal iPhone; I own the phone and the SLLC pays part of my monthly bill
- Question: If I worked for your City, would it violate the SCA if you searched my work emails on my iPhone?
  - The email is your system but the phone is not
- Easy solution: don't search my iPhone…just search the inbox on my desktop computer which should have the same information

Employer Owned and Operated System

- Why is the SCA not violated?
  - Section 2702 applies to persons or entities providing electronic communication service or remote computing service **to the *public***
  - *See Andersen Consulting v. UOP*, 991 F. Supp. 1041 (N.D. Ill. 1998) (SCA was not violated when UOP disclosed emails sent by Andersen Consulting employees on UOP's email system; UOP provided email to UOP and consultants not the general public)

Text or Email Residing Elsewhere

- What if you want to search a work email or text message where you are not providing the service?
  - **Remote computing services** can disclose texts to the **subscriber** (the City paying for the phone) without the consent of the sender
  - **Electronic communication services** cannot

Text or Email Residing Elsewhere

- Courts disagree whether text messages located on another service provider are RCS (accessible to the subscriber/employer) and/or ECS (not accessible to the subscriber/employer)
  - *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892 (9th Cir. 2008) (ECS)
  - *Flagg v. City of Detroit*, 252 F.R.D. 346 (E.D. Mich. 2008) (ECS or RCS)

Quon v. Arch Wireless Operating

- Arch Wireless provided the text messaging service to the City and only Arch Wireless had access to the messages
- The City was the subscriber
- Ninth Circuit concludes Arch Wireless provided ECS and not RCS
- Arch Wireless provided no "computer storage" or "processing services" (think of a virtual filing cabinet)
- But the reason the City asked Arch Wireless for the records was that Arch Wireless stored them right…but ECS doesn't include temporary or back up storage

Flagg v. City of Detroit

- Discovery case where SkyTel provided Detroit text messaging; plaintiff wanted messages sent by employees during a particular time period
- Court concludes service providers can be ECS or RCS depending on how they are functioning
- Back up protection (electronic storage)—ECS; archived (computer storage)—RCS
- In this case SkyTel had the only copy so this wasn't an instance of backup storage

Personal E-mail

- Courts agree that logging into an employee's personal email violates the SCA
- In *Van Alstyne v. Electronic Scriptorium*, 560 F.3d 199 (4th Cir. 2009) the court does not even bother explaining why a company president accessing an employee's personal email without consent violates Section 2701

Personal E-mail

- The following authors suggest that without violating the SCA employers may be able to view personal emails viewed or created at work by accessing temporary internet files on the employer's computer--Marjorie Peerce & Daniel Shapiro, The Increasing Privacy Expectations in Employees' Personal Email, Journal of Internet Law (Feb. 2010)
- Why? You don't need to log in to view these files which are stored on your computer system
- *See also Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F. Supp. 2d 548 (S.D. N.Y. 2008)

Pure Power Boot Camp v. Warrior Fitness Boot Camp

- Offers support for this theory (in dicta?)
- SCA violated because former employer directly logged onto former employee's personal email
- But the court indicates the outcome might have been different had the former employer found the former employee's emails accessed at work through examining the former employee's computer

Social Networking

- SCA applies to social networking too
- In *Pietrylo v. Hillstone Restaurant Group*, No. 06-5754, 2009 WL 3128420 (D. N.J. Sept. 25, 2009), the court upheld a jury verdict in favor of the plaintiffs on the SCA where a manager demanded an employee's password to MySpace.com

Compelling Disclosure from Providers

- Government entities, including political subdivisions of the state, may compel disclosure from providers using:
  - Subpoena—non-content information like length of service, means of payment
  - Subpoena with prior notice—open and sent email
  - Order—most account logs and transactional records
  - Order with prior notice—almost everything associated with an account except unopened email and voicemail stored for less than 180 days
  - Warrant—everything!

Compelling Disclosure

- Subpoena with notice
  - This rule allows access to content in *electronic storage* for more than 180 days and electronic communications held by RCS
  - Most courts have concluded that open and sent emails aren't in electronic storage
  - In the Ninth Circuit per *Theofel v. Farley Jones*, 359 F.3d 1066 (9th Cir. 2004) open emails are in electronic storage because they are "back up"
  - So in Ninth Circuit a warrant is required to get open and sent emails less than 180 days old from providers

Penalties

- If you break into an employee's personal email
  - Penalties under Section 2701 include a fine or imprisonment
  - Civil actions against employers and supervisors by employees alleging violations of Section 2701 are possible under Section 2707
    - Damages include: money damages no less than $1,000 per person, equitable or declaratory relief, and a reasonable attorney's fee plus other reasonable litigation costs
    - Willful or intentional violations can also result in punitive damages

Penalties

- Think twice before breaking into an employee's personal email!
  - Jury verdict in *Van Alstyne v. Electronic Scriptorium*
    - Supervisor: $150K compensatory, $75K punitive
    - Company: $25K compensatory, $25K punitive
    - Plus $135K jointly in attorney's fees and costs
  - 4th Circuit overturned compensatory damages because the plaintiff did not prove she sustained actual damages

Penalties

- What if you improperly seek an employee's email held by a service provider?
  - Penalties for violating Section 2702 are limited to service providers
    - In *Quon* Arches Wireless was liable for the SCA violation not the City of Ontario
    - In *Flagg* the plaintiff subpeonaed Detroit for SkyTel's records and Detroit filed a motion arguing that the SCA prevents it from requesting the records

Additional Resources

- Learning about the SCA from secondary sources is difficult because most article aren't written from a government employer's perspective
  - Jennifer Heidt White, Text Messaging Monitoring After Quon v. Arch Wireless, 5 Scidler J. L. Com. & Tech. 19 (2009)
  - Department of Justice, Searching & Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, Chapter 3, The Stored Communications Act (2009)