Electronic Discovery and Cloud Computing
Association of Certified Fraud Examiners
June 14, 2011
Agenda

- What Is Cloud Computing?
- Discovery in a “Cloud” Environment
- Discovery and the Stored Communication Act
- Obtaining Information Held by 3rd Party
- Interesting Cases
What is Cloud Computing?
Cloud Computing Defined

• “Cloud Computing” is used as a marketing term by technology companies
  – SAAS – Software as a Service
  – IAAS – Infrastructure as a Service
  – PAAS – Platform as a Service
  – “Utility Computing”

• Technologies in this area are rapidly changing

• The information in this presentation may become rapidly outdated due to advances in technologies, applications, and platforms

• The information is in this presentation for educational purposes – an attorney should be consulted regarding matters discussed herein
Cloud Computing Defined

- Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

National Institute of Standards and Technology (NIST)
Cloud Computing Defined

- Applications and data management outsourced to a service provider
- Promise of reduced maintenance, licensing issues, support
- Technology enabled by rapid communication over Internet to remote servers
- Applications and data reside “in the cloud” (i.e., the actual location of the server and storage is not known, and is practically irrelevant)
- Details are abstracted from the end user, who no longer needs expertise in (or control over) the IT infrastructure
- Enables computing on demand, rapid addition or subtraction of resources or applications
Practical Implications

- Data resides in a remote, 3rd-party computer
- Data may reside in multiple data centers, in multiple countries
- Organizations may outsource certain functions or applications
- Requires identification of outside service providers
- Data acquisition may not allow recovery of deleted data
- Difficult to assess if data acquisition complete
- Data acquisition may be covered by constraints of:
  - Electronic Communications Privacy Act (18 U.S.C. § 2510)
"Both public and private cloud will shape the server market through 2014. Cloud will grow from a $3.8 billion opportunity in 2010, representing over 600,000 units, to a $6.4 billion market in 2014, with over 1.3 million units."

Katherine Broderick, research analyst, IDC's Enterprise Servers and Datacenter Trends, *Datacenter and Cloud Computing Survey*
"Traditional" Client/Server IT Model

**Internal Server:**
- E-mail Server (e.g. MS Exchange)
- Shared Applications
- User Document Storage
- Data Backup

**Local Applications (e.g. MS Office)**
Local Data
E-mail Client (e.g. MS Outlook)

**Web Servers**
- Public Content
- Public Data

**Internet**
"Traditional" Client/Server IT Model – Discovery Points

Internal Server:
- E-mail Server (e.g. MS Exchange)
- Shared Applications
- User Document Storage
- Data Backup

Local Applications (e.g. MS Office)
Local Data
E-mail Client (e.g. MS Outlook)

Image Local Drives

Obtain Backup
Copy Files
Copy E-mail

Web Servers
- Public Content
- Public Data

Copy Files
Copy E-mail

Internet
"Cloud Computing" Model

Internet Appliance:
- Connectivity to Internet resources
- Browser
- Possible local applications
- Web history files

Web Service Provider:
- Public Content
- Public Data
- Applications
- E-mail Content
- Stored Files
- Documents
Types of “Clouds”

• “Cloud computing” model may be deployed in a number of different ways

• Public Cloud
  – Applications and data hosted by off-site 3rd-party service provider
  – Open to all (with payment of fees)

• Private Cloud
  – Applications and data hosted via virtualized services thru internal IT resources on internal hardware
  – Does not avoid fixed IT costs and support costs

• Hybrid Cloud
  – Combination of both internal and external virtualized services
  – Internal resources with external services and replication
Rapid Adoption of Cloud

- 38% of SMBs with fewer than 20 employees use or plan to use cloud solutions in next 6 months
- 17% of SMBs with 20–99 employees
- 22% with over 100 employees
- 34% in the tech sector plan to adopt cloud solutions

Spiceworks survey of small and medium businesses (SMBs) with fewer than 1,000 employees
Common Cloud Applications

- Social networking
- Cloud storage
- Backup and recovery
- Secure e-mail processing
- Anti-spam/anti-phishing
- E-mail service
- Office applications
Sample Office Applications

- Gmail and Google Apps
  - user@gmail.com
  - Document, spreadsheet, presentation, drawing
- Hotmail and Office Online
  - User@hotmail.com, user@live.com
  - Word, Excel, Powerpoint, OneNote
- Corporate Gmail and Google Apps
  - $50 per year, per user
  - Document, spreadsheet, presentation, drawing
- Exchange Online
  - From $10 per user per month
  - Office 365 set to release later this year
Discovery in a “Cloud” Environment
Understand IT Solution

Local Computer

Hosted Applications

Internally Hosted

Externally Hosted

Entity Relationship

Non-Entity Relationship
Understand IT Solution

• Essential to understand the type and location of applications
  – Hosted or local
  – Local applications will likely have data on the local drive, or a shared network drive

• Essential to identify the host of the application
  – Internal or 3rd party
  – Internal applications are hosted on an internal server

• Essential to understand the relationship between the 3rd party and the account holder
  – Who would need to provide permission to access the data?
  – If the relationship is a corporate contract, the entity should be able to grant permission to access the data
  – If the relationship is personal, discovery would likely fall under the Stored Communications Act
- Document retention requirements must still be met in a hosted environment
- Certain entities are statutorily required to maintain documents and/or e-mail correspondence for a specified time period
  - Also must suspend destruction under certain circumstances
- Organizations must perform IT planning, including planning of archival methods, to meet these requirements
- When moving data to the Cloud, these organizations must consider the impact of the hosted environment on these requirements and plan accordingly
Discovery Points – Local Computer

- Local storage of application data
- Local drive may include cached copies of documents
  - Depends on source and browser
  - Likely difficult to find and analyze
- Hosted documents may have been exported to the local drive by the user
- User may use POP mail to retrieve content to local client
  - Local e-mail client (like Outlook) used to receive internet hosted mail
  - Mail content replicated on local machine
- Google Desktop will create ‘snapshots’ of opened files, even if they are deleted
- Image of computer drive would allow retention of the local data
  - Possible recovery of ‘deleted’ files
Discovery Points – Internally Hosted

- Internal server with hosted applications
- Internal server storing documents
- Internal server receiving and storing communications
- Files may be extracted from server, including e-mail storage files
- System backups may also hold information of interest that may be recovered
- Extent of files may be derived from security permissions
  - Identify folders to which the user had permission to write
  - Personal folders, shared folders
- Copy of e-mail server must typically be accomplished when mail server is offline
Discovery Points – Externally Hosted

- Externally hosted applications with an entity relationship (i.e., the 3rd party provides service to a user through a relationship with an entity)
- Entity policies would define relationship of data to the user
  - E-mail content remains the property of the employer
- Contract, service agreement may specify terms of access by subscriber
- Entity may provide permission to the 3rd-party provider to copy or access the stored data
- Service agreement should define the ability of the organization to access their hosted data
• 2.4 **End User Consent.** Customer's Administrators may have the ability to access, monitor, use, or disclose data available to End Users within the End User Accounts. Customer will obtain and maintain all required consents from End Users to allow: (i) Customer's access, monitoring, use and disclosure of this data and Google providing Customer with the ability to do so and (ii) Google to provide the Services.

Gmail Apps for Business Online Agreement, 4/4/2011
• **2.7 Third Party Requests.** Customer is responsible for responding to Third Party Requests. Google will, to the extent allowed by law and by the terms of the Third Party Request:
  – (a) promptly notify Customer of its receipt of a Third Party Request;
  – (b) comply with Customer's reasonable requests regarding its efforts to oppose a Third Party Request; and
  – (c) provide Customer with the information or tools required for Customer to respond to the Third Party Request.

• Customer will first seek to obtain the information required to respond to the Third Party Request on its own, and will contact Google only if it cannot reasonably obtain such information.

Gmail Apps for Business Online Agreement, 4/4/2011
Discovery Points – Externally Hosted

• Accessing current content does not ensure that deleted content is also accessible
• “Deleted” content in some mail systems available for a period of time
• System tools are available to archive e-mail content, and allow access to the data should it become necessary
• Careful planning is essential to ensure data is available for analysis during an investigation
Planning for Discovery

- Identify all storage locations for data
  - Internal
  - External
- Identify all 3rd party service providers and data they host
- Obtain service agreements for all 3rd-party providers
- Identify if:
  - Service available to the public
  - Conditions exist demonstrating entity ‘control’ over the data
  - Retention of backup copies/recovery of deleted data is addressed
  - Local copies of the data may also exist
Discovery and the Stored Communications Act
Stored Communication Act

- The Stored Communications Act, 18 U.S.C. §§ 2701–2712 ("SCA") sets forth a system of statutory privacy rights for customers and subscribers of computer network service providers.
- The SCA was included as Title II of the Electronic Communications Privacy Act of 1986 ("ECPA").
- The ECPA also included amendments to the Wiretap Act and created the Pen Register and Trap and Trace Devices statute.
- "Stored Communications Act" appears nowhere in the language of the statute.
“Oct. 21, 1986 To amend title 18, United States Code, with respect to the interception of certain communications, other forms of surveillance, and for other purposes.”

ECPA 1986

Regulates:
- Providers of Electronic Communication Services (ECS)
- Remote Computing Services (RCS)

Services must be available to the public, after paying any fees
(a) Prohibitions

(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—

- (A) 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;
- (B) 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
Stored Communication Act

- Providers of Electronic Communication Service (ECS)
  - Provides users the ability to send or receive wire or electronic communications
    - Phone companies, e-mail services, text message services
  - Contents in “electronic storage” held by ECS § 2510(17)(A)
    - Temporary, intermediate storage incidental to the communication
    - Storage of such communication for backup purposes
    - E.g., an e-mail received by the provider but not opened by the recipient

- Providers of Remote Computing Service (RCS)
  - The provision to the public of computer storage or processing services by means of an electronic communications system
    - Use computer services in essentially a time-sharing arrangement
    - Server that allows users to store data for later retrieval
    - Services must be available to the public, after paying any fees
• Service may be an ECS and an RCS
• Key is determining what role the provider has played and is playing with respect to the communication in question

• The potential importance of distinguishing between an ECS and an RCS lies in the different criteria for establishing an exception to the general rule against disclosure.
• The provider of an RCS may divulge the contents of a communication with the “lawful consent” of the subscriber to the service, while the provider of an ECS may divulge such a communication only with the “lawful consent of the originator or an addressee or intended recipient of such communication.” 18 U.S.C. § 2702(b)(3)
• Example: e-mail service provider
  – E-mail is sent to my personal Gmail account
  – Inbox = temporary intermediate storage
  – Gmail is an ECS with respect to the message
  – I open the message; it is available for retrieval later in my inbox
  – Gmail becomes an RCS with respect to the message*
  – Gmail remains an ECS with respect to copies of any backup of the in-transit message
  – I copy the message to my personal computer – SCA does not apply

* Note: the 9th District in Theofel would disagree
"Electronic Storage"

- Ninth Circuit decision created a split between two interpretations of “electronic storage”
  - *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004)

- Traditional definition of “electronic storage” § 2510(17)(A) refers only to:
  - Temporary storage made in the course of transmission
  - Storage ‘for purposes of backup protection of such communication’
  - Backups of such intermediate communications made by the service provider to ensure system integrity

- The Ninth Circuit rejected the narrow definition of “electronic storage”
"Electronic Storage"

- *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004)

- Court did not dispute that once opened, the message is no longer in temporary storage.
- E-mail messages are in “electronic storage” regardless of whether they had been previously accessed.
- Retrieved e-mail falls within the backup portion of the definition of “electronic storage.” *Id.* at 1075–77.
- Such a message “functions as a ‘backup’ for the user.” *Id.* at 1075

- This interpretation sets a higher standard to obtain previously opened e-mail content.
Obtaining Information Held by 3rd Party
Information in three categories:

1. Basic subscriber and session information
   1. Name
   2. Address
   3. Phone connection records or session duration information
   4. Length of service and service types
   5. Means and source of payments

2. Non-content records and other information pertaining to customer
   1. Transactional records
   2. Logs
   3. Listing of e-mail accounts with whom subscriber communicated
Information in three categories:

3. Contents
   1. Actual files stored in the account
   2. E-mail text, headers
   3. Voice mail
   4. Subject lines of e-mail
   5. Contents in “electronic storage” held by ECS
      - Differs in the 9th Circuit
   6. Contents held by RCS
Section 2703 offers five mechanisms that a "government entity" can use to compel a provider to disclose certain kinds of information:

1. Subpoena
2. Subpoena with prior notice to the subscriber or customer
3. § 2703(d) court order
4. § 2703(d) court order with prior notice to the subscriber or customer
5. Search warrant

Greater process generally includes access to information that cannot be obtained with lesser process.

Additional work required to satisfy a higher threshold will often be justified because it can authorize a broader disclosure.
Two situations where a subpoena is not required:

- When investigating telemarketing fraud, law enforcement may submit a written request to a service provider for the name, address, and place of business of a subscriber or customer engaged in telemarketing.
  - 18 U.S.C. § 2703(c)(1)(D)

- The government may compel a service provider to disclose non-content information pertaining to a customer or subscriber when the government has obtained the customer or subscriber’s consent.
  - 18 U.S.C. § 2703(c)(1)(C)
Subpoena

- Any information that is outside the scope of the SCA
- Basic subscriber and session information defined in 18 U.S.C. § 2703(c)(2):
  - Name
  - Address
  - Local and long distance telephone connection records, or records of session times and durations
  - Length of service (including start date) and types of service utilized
  - Telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address
  - Means and source of payment for such service including any credit card or bank account number
Subpoena with Notice

- Administrative subpoena authorized by a federal or state statute or a federal or state grand jury or trial subpoena
- Subpoena and *either* prior notice to the subscriber *or* compliance with the delayed notice provisions of § 2705(a) may obtain:
  1. Basic subscriber and session information
  2. “The contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days.”
     18 U.S.C. § 2703(a)
  3. “The contents of any wire or electronic communication” held by a provider of remote computing service “on behalf of . . . A subscriber or customer of such remote computing service.”
     18 U.S.C. § 2703(b)(1)(B)(i), § 2703(b)(2)
- Outside the Ninth Circuit this third category will include opened and sent e-mail
Subpoena with Notice

• Notice may be delayed for 90 days “upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result.”

• An adverse result is:
  – Endangering the life or physical safety of an individual
  – Flight from prosecution
  – Destruction of or tampering with evidence
  – Intimidation of potential witnesses
  – Otherwise seriously jeopardizing an investigation or unduly delaying a trial
  – 18 U.S.C. § 2705(a)(2)
§ 2703(d) Order

- A court order under 18 U.S.C. § 2703(d) may obtain:
  - Basic subscriber and session information
  - All “record[s] or other information pertaining to a subscriber to or customer of such service (not including the contents of communications)” 18 U.S.C. § 2703(c)(1)
  - Most account logs and transactional records

- Requires:
  - Specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation”
  - “In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State” 18 U.S.C. § 2703(d)
§ 2703(d) Order

- §2711 (3) defines “court of competent jurisdiction”
  A. any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals that has jurisdiction over the offense being investigated
  B. a court of general criminal jurisdiction of a State authorized by the law of that State to issue search warrants

- SCA permits federal judges to issue 2703(d) orders compelling providers to disclose information even if the judge does not sit in the district in which the information is stored

- SCA is silent on whether state courts may issue orders to providers outside their districts
§ 2703(d) Order with Notice

• A court order under 18 U.S.C. § 2703(d), and either prior notice to the subscriber or comply with the delayed notice provisions of § 2705(a), may obtain:
  1. Basically, everything except for unopened e-mail or voice mail that have been in the account for 180 days or less
  2. Except in the 9th Circuit, where the § 2703(d) order may be used to obtain communications in “electronic storage” for over 180 days
Search Warrant

- A search warrant may obtain anything (all content and non-content) associated with an account
- There is no requirement to notify the customer or subscriber
- Warrant may be issued by a federal court with jurisdiction over the offense under investigation, even for records held in another district
- State courts may issue warrants, but the SCA does not provide for the warrant’s effect outside the court’s territorial jurisdiction
Search Warrant

- The presence of an officer is not required for service or execution of a § 2703 warrant
  - 18 U.S.C. § 2703(g)
- Investigators typically do not directly search the computers for the information
- The warrant directs the provider to produce all the content of the account or accounts
- The information produced is then reviewed by law enforcement for items that fall within the scope of items to be seized
<table>
<thead>
<tr>
<th>Basic subscriber, session, and billing information</th>
<th>Subpoena; 2703(d) order; or search warrant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other transactional and account records</td>
<td>2703(d) order or search warrant</td>
</tr>
<tr>
<td>Retrieved communications and the content of other stored files#</td>
<td>Subpoena with notice; 2703(d) order with notice; or search warrant</td>
</tr>
<tr>
<td>Unretrieved communications, including e-mail and voice mail (in electronic storage more than 180 days)</td>
<td>Subpoena with notice; 2703(d) order with notice; or search warrant</td>
</tr>
<tr>
<td>Unretrieved communications, including e-mail and voice mail (in electronic storage 180 days or less)</td>
<td>Search warrant</td>
</tr>
</tbody>
</table>

Source: Searching and Seizing Computers, 3rd Edition 2009, CCIPS Criminal Division
Voluntary Disclosure - Exceptions

- The SCA generally prohibits voluntary disclosure of information by a 3rd party provider of services to the public
  - If an RCS or ECS provider does not provide services to the public, the SCA does not apply
- Non-content records may be freely provided to another party other than a government agency
  - 18 U.S.C. §§ 2702(a)(3), (c)(6)
- RCS content may be provided with consent of the subscriber
- ECS content may be provided with consent of the originator, addressee, intended recipient
- In emergency situations related to the commission of a crime, death, or serious physical injury
- Submitted to the National Center for Missing and Exploited Children
• Contents of communications may not be disclosed to civil litigants even when presented with a civil subpoena.
  – *O'Grady v. Superior Court*, 139 Cal.App.4th 1423, 1448
• At least one court has held that a pre-trial discovery subpoena issued in a civil case pursuant to Fed. R. Civ. P. 45 is inadequate. See *FTC v. Netscape Communications Corp.*, 196 F.R.D. 559, 561 (N.D. Cal. 2000) (holding that civil discovery subpoena did not fall within the meaning of “trial subpoena”)
• Case law continues to build in this area
• Discovery issues in litigation frequently bump into the provisions of the Stored Communications Act
• There is essentially no case law addressing services provided by “cloud” service providers
• Many cases reveal issues that have not been presented previously
• Earlier precedent may not exactly fit the facts of the current case
• The application of the SCA will continue to evolve as more and more content is transmitted through and stored by 3rd-party providers
O’Grady v. Superior Court

- Apple Computer, Inc. (Apple), alleged persons unknown caused the wrongful publication on the Internet of Apple’s secret plans to release a device that would facilitate the creation of digital live sound recordings on Apple computers
- Apple sought and obtained authority to issue civil subpoenas to the publishers of the websites where the information appeared and to the e-mail service provider for one of the publishers
- Publishers moved for a protective order to prevent discovery
O’Grady v. Superior Court

- Trial court denied the motion for protective order on the grounds that the publishers had involved themselves in the unlawful misappropriation of a trade secret
- Court of appeals held that this was an error because a subpoena to the e-mail service provider cannot be enforced consistent with the plain terms of the federal Stored Communications Act
- Protective order was allowed
Beluga Shipping v. Suzlon

- In Australian Federal Court, Suzlon brought cross claims for fraud and breach of fiduciary duty against former employees
- Suzlon believed that they used Gmail accounts to perpetrate the fraud
- In its §1782 petition, Suzlon sought leave to issue subpoenas to Google to obtain all e-mails sent or received by the former employees using specific Gmail accounts
  - Records establishing when those Gmail accounts were created
  - The name provided to Google by the user of each account
  - Country in which each account was created
  - How Google stores or saves e-mails in its Gmail accounts
  - How information regarding when e-mails sent to and from a Gmail account is recorded and stored
Beluga Shipping v. Suzlon

- Google argued that under the SCA, consent of the individual account holders is required to comply with subpoena.
- Because Google and its servers are located in the United States, the district court concluded that the SCA was applicable.
- District court denied Suzlon’s petition to subpoena the e-mails.
- Court did direct Google to produce:
  - When the specific Gmail accounts in question were created
  - The actual names of the e-mail account holders
  - Countries from which the specific Gmail accounts were created
- The court further directed Google to continue to preserve the e-mails contained in the specific Gmail accounts in question pending a showing of consent by the account holders.
• *Juror No. 1 v. California*, 2011 U.S. Dist. LEXIS 16834
  • Juror No 1, serving as Foreman, occasionally posted updates to his Facebook wall
  - Still on jury duty
  - Bored by cell phone evidence
• After trial, several jurors became “friends on Facebook”
• Juror No. 5 reported the posts to counsel for defendants
• Evidentiary hearing held, Juror No. 1 questioned extensively
• February 4, 2011, Judge issued order requiring plaintiff “within 10 days from the date of this order ... execute a consent form sufficient to satisfy the exception ... allowing Facebook to supply the posting made by Juror No. 1 during trial”
• Threatened by contempt finding if consent is not provided
Juror No. 1 v. California

- Juror No. 1 asserts a right of privacy in posting
- Asserts Fifth Amendment right not to disclose the postings as they may be used against him to assert perjury charges in evidentiary hearing
- Juror No. 1 states order compels him to waive his Fifth Amendment rights
- February 10, 2011, appellate court denies request for stay
Thayer v. Chiczewski

- Thayer v. Chiczewski, No. 07 C 1290, 2009 WL 2957317 (N.D. Ill. Sept. 11, 2009)
- Civil rights case vs. the City of Chicago
- March 19, 2005, Thayer arrested for participating in a anti-war march for which a permit was denied
- At deposition, Thayer admitted sending e-mails about the events of the day, claimed older e-mails were deleted
- July 9, 2009, City issued revised subpoena to AOL for messages from Thayer’s account
- July 31, City filed motion to compel production
- AOL objected
- Court order on September 11, 2009, granting leave to commence discovery on AOL
“The Stored Communication Act does not Prevent the City from Discovering Relevant Documents”

City’s subpoena is targeting documents that Thayer would need to produce had he not deleted them

SCA permits disclosure if account holder grants permission

The issue becomes the length to which the Court can go to compel Thayer to assist the city in recovering the e-mail

Thayer had allowed AOL to release one e-mail; did not indicate he would later object to producing all e-mail
Flagg v. City of Detroit

- Involved charges of conspiracy among city officials
- Plaintiff believed text messages sent on city-issued devices would be relevant to the case
- Defendant claimed production in a civil case prohibited by SCA
- Court rejected this noting it would permit:
  - “a party to defeat the production of electronically stored information created by that party and still within its control — information that plainly is subject to civil discovery, see Fed. R. Civ. P. 34(a)(1) — through the simple expedient of storing it with a third party”
Flagg v. City of Detroit

• § 2702 lacks any language that explicitly authorizes a service provider to divulge the contents of a communication pursuant to a [civil] subpoena or court order
• Ordinary Fed. R. Civ. P. 34 request for production
  – Documents and various other categories of items that are “in the responding party’s possession, custody, or control.” Fed. R. Civ. P. 34(a)(1)
  – May include electronic information
• Control:
  – “Legal right to obtain” documents found in contractual provisions
  – Documents in the possession of a party’s agent
• Court concluded that the Defendant City of Detroit had “control” over the text messages preserved by third party
Flagg v. City of Detroit

- City’s present motion is **premised** upon such control, first asserting that the City has the **ability** to consent to production of the text messages at issue, but then stating that it is **unwilling** to do so.

- If the City can **block** the disclosure of messages by **withholding** its consent, it surely follows that it can **permit** the disclosure of these communications by **granting** its consent.

- This acknowledged power readily qualifies as a “legal right to obtain” the messages held by SkyTel, and hence constitutes “control” within the meaning of Rule 34(a)(1).

- A party has the attendant duty to take the steps necessary to exercise this control and retrieve the requested documents.

- Plaintiff directed to issue subpoena to the defendant, rather than to the 3rd-party provider.
• Questions?
Contact us:

Chicago
205 West Wacker Drive
Suite 1750
Chicago, IL 60606

Bloomfield Hills
4111 Andover Road
West 3rd Floor
Bloomfield Hills, MI 48302

866.717.1607  |  www.cca-advisors.com

cca@cendsel.com