TECHNOLOGY’S INCREASING ROLE IN ANTI-FRAUD EFFORT ELECTRONIC DISCOVERY IN A CLOUD COMPUTING ENVIRONMENT

Don’t get lost in the cloud! This session will arm you with an understanding of the intricacies of “Cloud Computing.” You will walk away with tools to help you overcome the challenges of navigating an examination that requires access to data hosted on these Internet-based, outsourced computer-networking services.

JAMES P. MARTIN, CFE, CMA, CIA
Managing Director
Cendrowski Corporate Advisors
Bloomfield Hills, Michigan

Jim Martin is Managing Director of Cendrowski Corporate Advisors (CCA). Jim specializes in providing comprehensive risk assessments, focusing on the evaluation of operating effectiveness of business processes, internal control structures, and the development of recommendations for improvement. Additionally, Jim has performed forensic examinations of numerous business arrangements to determine the accuracy of recorded transactions and financial statement presentations in the healthcare, durable equipment, real estate, automotive, and construction industries. Jim frequently performs litigation-support activities, focusing his efforts on fraud investigation and forensic accounting services. He is a detailed accounting technician, and has used his skills to uncover complex multimillion-dollar frauds and quantify business losses.

In addition to numerous articles in trade publications, he is co-author of The Handbook of Fraud Deterrence and Private Equity: History, Governance, and Operations, both published by John Wiley & Sons. He regularly presents at national and regional conferences on various aspects of risk and control, forensic accounting, transforming the internal audit function, and process redesign.

Jim is also active in numerous civic organizations. He is Commissioner of the Great Midwest Hockey League, Secretary of the American Collegiate Hockey Association (ACHA), and coach of the Michigan State University Men’s ACHA Hockey Team. He serves as a member of the Entertainment Committee for the American Cancer Society’s Relay for Life–South Lyon, MI.

Jim holds a B.B.A in accounting and a M.S. in accounting information systems from Eastern Michigan University. Jim has served on the faculty of Davenport University, Walsh College, and the University of Detroit-Mercy, where he instructed courses in Fraud Examination, Managerial Accounting, Internal Auditing, and Information Technology.

“Association of Certified Fraud Examiners,” “Certified Fraud Examiner,” “CFE,” “ACFE,” and the ACFE Logo are trademarks owned by the Association of Certified Fraud Examiners, Inc.
Cloud Computing is the marketing focus of many IT companies. Ads touting the benefits of cloud computing and the “cloud readiness” of software products are visible in airports, print media, and on TV, and surveys predicting the rapid adoption of cloud computing solutions appear regularly. Though many different definitions of cloud computing exist, the term is generally used to describe technologies that allow both applications and data and to be hosted on a computer external to a business’s own computing resources and firewall (a “remote computer”). In some cases, the remote computer may be owned and operated by a third party, in another part of the country, or even internationally. The large-scale movement of data, including stored communications, to remote computers will impact discovery during criminal investigations and civil litigation. Fraud examiners must be prepared to understand and face the changes driven by migration to the “Cloud.”

As with other forensic techniques, the need for available documents and information residing on internal or external systems will vary based on the specifics of the examination.

Cloud computing describes an IT model where computing resources can be obtained and utilized on an as-needed basis; this is why cloud computing is often referred to as “utility computing.” Cloud computing models generally allow for the reduction of costly IT assets, avoidance of software license costs, and removal of maintenance of software. The end user is provided a turnkey solution that is supported and maintained by the service provider at a remote location. Cloud computing is enabled by rapid, reliable Internet communications, and, in fact, the Cloud is a term referring to the pool of resources hosted on the Internet.

Outsourced computing services like cloud computing facilitate practical IT solutions for both businesses and
individuals. It is important to remember during the course of an investigation that an individual may have a separate agreement with a service provider for a hosted application—a common example would be an individual Gmail (Google’s e-mail service) account—but services could include online document processing or online financial accounting. Accounts pertaining to these services may have information that would be useful, and should be considered in the context of the investigation.

Cloud solutions often tout tremendous cost savings, including elimination of fixed hardware investments as well as lowering support costs. Many cloud applications may be accessed from personal computers as well as mobile devices; ease of access can provide additional benefits as increasingly powerful mobile devices are adapted. For these reasons, cloud solutions are expected to grow substantially over the foreseeable future. One recent study concluded that cloud computing will grow from a $3.8 billion market in 2010 to a $6.4 billion market in 2014.

Cloud computing has grown into a powerful marketing term and hardware and software companies have been quick to add the term to their product marketing efforts. Given the adoption of the term, the “cloud” moniker may be applied to a plethora of different implementations and configurations, and this will undoubtedly continue to evolve over time. Currently, there are three major approaches to implementing cloud solutions:

- Public cloud
- Private cloud
- Hybrid cloud

In a public cloud, applications and data are hosted by a third party on a remote, third-party-controlled host. In a
private cloud, applications and data are hosted on an internal host controlled within the entity. In a hybrid cloud, applications and data are hosted in a combination of internal and external resources, or hosted on internal resources with redundant external services or backup techniques.

In a public cloud environment, both data and applications are hosted on a remote computer managed by a third party. From a practical standpoint, this hosting technique complicates electronic discovery as it will be difficult, if not impossible, for the examiner to directly access the hardware hosting the data. Additionally, since the data is managed by a third party who also manages the data of other organizations, it is challenging to ensure the examiner has obtained all desired data. For example, under a traditional client-server environment hosting a Microsoft Exchange e-mail system, if an examiner wanted to collect all e-mail accounts for a company, he could access the internal e-mail server and obtain a backup of the system. This backup would generally include all e-mail accounts. Under a cloud model, the third-party provider may be running Microsoft Exchange, but the Exchange server would include e-mail accounts for different clients, and therefore would be reluctant to provide a copy of the entire server. Any request made for e-mail accounts would need to be reduced to include the e-mail accounts for a specific company. As such, it would be difficult for the examiner to independently verify that all materials had been produced.

E-mail is a fast-growing area for cloud services, both from corporate as well as personal perspectives. Yahoo! Mail, Microsoft Hotmail, and Google Gmail are popular e-mail systems for personal use; it is very common for a person to maintain a personal e-mail account with one of these services in addition to an e-mail account assigned at work.
Outsourced corporate e-mail solutions are also available. Gmail, for example, offers a corporate e-mail solution that will host to any domain name, for $50 per user. The virtualized services do not stop with e-mail. Google Documents and Microsoft Office 365 provide hosted applications for creating, editing, and storing office documents online, both for the individual and corporate versions.

When dealing with discovery issues, it is increasingly important to consider that a user or organization may have pools of data stored outside of their organization; the rapid adoption of cloud computing solutions will make this an increasingly imperative consideration in the future. The investigator should consider the possible locations of data, both inside and outside of the organization, and look for clues as to where data might exist. For example, when obtaining an image of a computer assigned to the subject of an investigation, the investigator should look for desktop links and Internet favorites that link to a hosted application. In a civil litigation setting, the investigator should consider increasing the scope of interrogatories to ask for identification of any hosted solutions that might be in use.

Understanding the IT Solution

For discovery, an understanding of a corporate or personal IT solution will involve identifying the type and locations of applications and data, considering applications on the local (aka “client”) computer hosted internally to the organization, and data and applications hosted externally by a third party. The relationship with a third-party provider may be through the organization (as would be the case in a corporate Gmail service) or through the individual (as would be the case if a person had a personal Gmail account), but this relationship will have a great impact on the ability to obtain data from that host. If the relationship
is through the organization, the organization should be able to provide permission to access the data; if the relationship is personal, the data would likely fall under the Stored Communications Act (which is covered later in this document), and the user would need to provide that permission. Obtaining such permission would need to be considered in the context of the objectives of the investigation.

Moving to a cloud computing solution does not remove an organization’s document retention requirements, and many cloud solutions tout their ability to help the organization meet statutory requirements. Offsite storage and retention of data, including system backup data is a popular solution. This means that any data stored in such a cloud computing solution should be available for the statutory retention period; additionally, this means the cloud solution should also be a part of any litigation hold requirements where the destruction of data is halted. The investigator should consider the availability of archive information held by a third party in the context of the investigation.

Even when data is stored in a third-party system, there may still be local storage of some data in the form of cached files, local storage files, or files downloaded to the local drive. For example, Gmail (both business and personal accounts) may be configured to read Gmail messages from a client or device that supports Post Office Protocol (POP), such as Microsoft Outlook or Netscape mail. If a user were to set up this service, the client or device would have a local copy of the mail, including inbox and sent messages. In other cases, depending on the particular cloud-based service, and the local browser, it is possible that local cached files exist that are downloaded to the client in the normal operation of the system. For these reasons, it is still important to acquire forensic images of local drives and
thoroughly examine the acquired data to determine if any local data is relevant to the investigation.

For virtualized applications stored on an internal server, the investigator should consider that there will be applications and data stored both on the server and any backup system. Files may be extracted from the server or backup media, including e-mail files. For network storage locations, the investigator should examine the security definition for the subject user to determine the areas on the server where that user was authorized to store files.

For third-party hosted applications and data with an entity relationship (i.e., where the third-party service is contracted by the organization), the organization should be able to obtain data associated with a user account, or a company administrator should be able to access the data directly. For example, with a Gmail App for business-hosted e-mail solutions, a company administrator is provided tools to set up accounts and review any information in any of that company’s account. For any hosted solutions, the service agreement with the vendor should define the ability of the company to access user information, and procedures to access such data. The investigator should identify the administrator contact within the organization to access data.

As part of the procedures to utilize a cloud service, an organization should develop procedures for accessing user account information, should it be necessary in an investigation. Additionally, organizations should consider if additional archiving procedures are required to ensure copies of virtualized content is available if required to support an investigation.

**Discovery and the Stored Communication Act**

Data hosted by a third-party service provider where the contracted service is arranged by the individual may be
covered by the Stored Communications Act (18 U.S.C. §§ 2701–12) (SCA). This act was included as Title II of the Electronic Communications Privacy Act of 1986, which also included amendments to the Wiretap Act and created the Pen Register and Trap and Trace Devices statute. The SCA states that “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.”

The SCA also regulates providers of Remote Computing Services (RCS) and Electronic Communication Services (ECS). In order for a service to be covered by the SCA, the service must be available to the public, even if a fee for service is involved. Many of the product offerings billed as cloud computing solutions could fall under the Stored Communication Act as an Electronic Communication Service, a Remote Computing Service, or both.

ECS providers offer users the ability to send or receive wire or electronic communications, including phone, e-mail, and text messages. For example, a hosted e-mail system, such as Gmail, would be considered an ECS provider. Contents in “electronic storage”¹ are defined as temporary, intermediate storage incidental to communication (such as an inbox) and storage of such communication for system backup purposes.

RCS providers offer computer storage or processing services by means of an electronic communications system; this allows a user to obtain computer services in essentially a time-sharing arrangement. An RCS provider would include servers that allow users to store data for later retrieval, or a hosted application providing document

¹ § 2510(17)(A)
editing and processing capabilities. Regarding RCS providers, the SCA states, “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 provider may offer ECS and an RCS services; the key is determining what role the provider has played—and is playing—with regard to the communication in question. For example, consider a Gmail-hosted e-mail account. When a communication is received for a user and stored in the inbox, Gmail is an ECS provider with respect to the message. Once the message has been opened, and assuming the user does not delete the message, Gmail becomes an RCS provider. It is also important to note that if the message is downloaded or copied to the user’s client computer, the restrictions of the Stored Communication Act would no longer apply.

The SCA defines three categories of information; each category has different requirements to obtain the information.

1. Basic subscriber and session information:
   a. Name
   b. Address
   c. Phone connection records or session duration information
   d. Length of service and service types
   e. Means and source of payments

2. Non-content records and other information pertaining to customer:
   a. Transactional records
   b. Logs

---

2 18 U.S.C. § 2702
c. Listing of e-mail accounts with whom subscriber communicated

3. Contents:
   a. Actual files stored in the account
   b. E-mail text, headers
   c. Voice mail
   d. Subject lines of e-mail
   e. Contents in “electronic storage” held by ECS providers
      i. Differs in the 9th Circuit
   f. Contents held by RCS providers

Section 2703 of the SCA offers five mechanisms that a “government entity,” including law enforcement, can use to compel a provider to disclose certain kinds of information. They are, in increasing order of power, a subpoena, subpoena with prior notice to the subscriber or customer, a § 2703(d) court order, a § 2703(d) court order with prior notice to the subscriber or customer, and a search warrant. Latter processes generally include access to information that cannot be obtained with former processes, and the additional work required to satisfy a higher threshold will often be justified because it can authorize a broader disclosure. The table below provides a summary of production processes and information that may be produced by these processes.
Certain procedural aspects are different when implementing production demands under the SCA.

First, §2711 (3) defines “court of competent jurisdiction” as 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 or a court of general criminal jurisdiction of a state authorized by the law of that state to issue search warrants. This means that the 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. The SCA is silent, however, on whether state courts may issue orders to providers outside their districts.
Second, the presence of an officer is not required for service or execution of a § 2703 warrant. Investigators typically do not directly search the computers for the information requested. Instead, the warrant directs the provider to produce all the content of the account or accounts desired, and the information produced is then reviewed by law enforcement for items that fall within the scope of items to be seized.

While the SCA generally prohibits voluntary disclosure of information by a third-party provider of services, there are several notable exceptions. If the provider does not provide services to the public, the SCA does not apply. For example, consider a consultant who is provided an e-mail account by a company where they are assigned for work. Court decisions have determined that the company providing such an e-mail account is not covered by the SCA, as they do not provide services to the public.

Consent will allow production of records as well. RCS content may be provided with the consent of the subscriber. ECS content may be provided with the consent of the originator, addressee, or recipient. For civil litigation, consent may be strongly encouraged by the Court; in criminal matters, forcing consent could be considered a violation of the suspect’s Fourth Amendment rights.

The SCA was primarily written to protect the end user of computing services from government surveillance. In civil litigation, some courts have concluded that contents of communications cannot be disclosed to litigants even when presented with a civil subpoena. In a recent decision, the court noted that a subscriber could grant permission for the

---

3 18 U.S.C. § 2703(g)  
4 See Juror No. 1 v. California, 2011 U.S. Dist. LEXIS 16834  
5 See O'Grady v. Superior Court, 139 Cal.App.4th 1423, 1448
provider to release contents, or could not grant such permission, and the contents would not be provided. Therefore, the court reasoned that the information held by the provider was under the control of the subscriber, and therefore the party had an attendant duty to exercise this control and retrieve the content.\(^6\)

The role of the SCA will continue to grow in importance as more and more companies adopt cloud computing solutions. Courts continue to evaluate aspects of the law, and case law continues to build around these issues. Investigators attempting to access information held by a third party will need to evaluate an appropriate course of action depending on the type of information received, as well as the relative cooperation of the subscribing party.

---