Information Governance Initiative

E-DISCOVERY IN A CLOUD-FIRST WORLD

USING INFORMATION GOVERNANCE TO PREPARE & PROTECT YOUR ORGANIZATION

information governance initiative

Compliments of Viewpointe

Information Governance Initiative • 1271 Avenue of the Americas • Suite 4300 • New York, NY 10020 • iginitiative.com

About the Information Governance Initiative

The Information Governance Initiative (IGI) is a cross-disciplinary consortium and think tank dedicated to advancing the adoption of Information Governance practices and technologies through research, publishing, advocacy, and peer-to-peer networking. The IGI publishes research, benchmarking surveys, and guidance for practitioners that is freely available on its website. Join the IGI Community, a place for practitioners from all facets of IG to come together and learn from each other. The IGI was founded by recognized leaders in the field of Information Governance, and is supported by leading providers of Information Governance products and services.

About this Publication

This publication was written by the Information Governance Initiative as part of our ongoing series exploring issues, strategies, and techniques related to information governance.

This publication was made possible by Viewpointe's support of the IGI. More information about Viewpointe is available at www.viewpointe.com.

E-Discovery in a Cloud-First World

Using Information Governance to Prepare and Protect Your Organization

Introduction

Electronic discovery (e-Discovery) is a downstream problem in the flow of your organization's information "river." Decisions made upstream have a tremendous impact on your ability to manage the cost and risk of e-Discovery. Poor information management, control, and security upstream will mean greater risk and costs during e-Discovery—both directly (actual costs of conducting discovery) and indirectly (the consequences, including sanctions, of not getting it right).

The picture grows even more complex in a cloud-first world. Now these upstream issues (information management, control, and security) involve a third party whose obligations to address them are based in contract and whose technical capability to execute are not in your direct control (except for what's spelled out in service-level agreements).

Due diligence with a focus on information governance is required when making the move to cloud. In the rush to the cloud, many organizations fail to consider the downstream complexity of searching, finding, and producing mountains of evidence—all under the watchful eye of a court or regulator. In fact, many fail to consider the holistic governance and use of their information at all.

In addition to the host of considerations that businesses need to make regarding the cloud service providers (CSPs) that they ultimately decide to go with—like contractual terms, the provider's physical location, compliance expertise and any technological capabilities—information governance practitioners also need to be aware that employees, driven by convenience, may choose to leverage their own rogue cloud services without conferring with IT.

All organizations must address information governance requirements as part of the process of evaluating, selecting, and integrating a cloud provider into their information environment. This paper explores the unique challenges and opportunities that cloud infrastructure creates for information governance and e-Discovery. It also provides advice on how practitioners can better prepare for both.

What Do You See in the Clouds?

> *"I don't need a hard disk in my computer if I can get to the server faster . . . . carrying around these non-connected computers is byzantine by comparison."*
>
> – Steve Jobs, founder of Apple, 1997
>
> *"Cloud computing is based on the time-sharing model we leveraged years ago before we could afford our own computers. The idea is to share computing power among many companies and people, thereby reducing the cost of that computing power to those who leverage it."*
>
> –David Linthicum, cloud computing expert

While the concept of cloud computing traces its roots back to the 1950s, it wasn't until the mid-2000s that the model truly began making noticeable mainstream inroads thanks to companies like *Salesforce*, *Amazon*, *Microsoft* and *Google*. Today, the cloud is everywhere, and providers now have the ability to do everything from hosting content to storing data to running systems and applications.

Chances are if you asked five people what the cloud is, you'd get five different answers. (And at least one of those answers would include something related to weather.) This, believe it or not, sort of makes sense, because cloud computing isn't just one thing.

For starters, when businesses move to the cloud, they must first consider one of the following deployment models:

- **Public cloud.** Businesses wishing to enjoy the cost savings and versatility that result from sharing computing assets with other companies may opt for public cloud deployments, choosing providers like Amazon and Google to host their technological infrastructure. According to the IDC, the global public cloud market stands at $45.7 billion today; it's expected to grow 23 percent annually through 2018. Still, public cloud deployments are not free from drawbacks of their own. For example, because computing assets are shared by numerous organizations in public cloud environments, it's not uncommon for one business' information to become entangled with another's, which could lead to substantial problems during the e-Discovery process.

- **Private cloud.** Some organizations choose to build and maintain their computing infrastructure in-house, moving forward with private cloud deployments. In these environments, the administration of computing assets generally falls under the purview of internal IT teams. In addition, these clouds can be hosted as a managed service, where the provider becomes an extension of the organization, removing the burden of administration, maintenance and expertise from in-house IT. Private clouds are completely customizable, allowing them to be configured to meet the specific needs of the business (e.g., security). Technology Business Research (TBR)

predicts that companies will increasingly adopt private cloud environments in the coming years, and as such, the market will reach $69 billion by 2018, growing 40 to 50 percent annually in the coming years. Organizations in highly regulated environments (e.g., financial, pharmaceutical, and legal) tend to gravitate toward private cloud infrastructure due to strict information governance requirements.

- **Hybrid cloud.** Private clouds can be resource heavy and expensive; they're not the right solution for every business or for every environment within a business. Some companies choose the best of both worlds, building hybrid cloud environments that offer the benefits associated with both public and private deployment models. For example, an e-commerce company might decide to manage and maintain all sensitive customer information in a private cloud while provisioning public cloud resources to accommodate significant user-related traffic spikes. TBR expects the hybrid cloud market will likely outpace both the public and private markets, growing 50 percent in 2015.

Beyond cloud deployments, chances are at least some employees will utilize software as-a-service (SaaS) solutions and cloud-based collaboration and storage applications. After all, these tools make their jobs easier—regardless of whether the IT team has signed off on any of them or is even aware they're being used. These applications—like Dropbox, Box and OneDrive—have grown in popularity in recent years because they enable a more seamless collaboration experience. With them, all team members can access pertinent data from any connected device thereby streamlining productivity. While these apps make life easier for employees, they can present significant challenges during e-Discovery.

Clearly it is only a matter of time before all organizations move at least a portion of their infrastructure to the cloud—if they haven't done so already. In fact many organizations (including the U.S. federal government, for example) are adopting "cloud-first" strategies that prioritize delivery of IT services using cloud capabilities.

Altogether, the cloud computing market is expected to triple to $235 billion by 2017, and for good reason. In addition to simply hosting content like the cloud providers of yore, today's CSPs can store data and run systems, networks and applications. Additionally, on the customer side, cloud computing provides enterprises with a wealth of benefits including cost savings, agility, scalability, and business continuity, among others.

But, the movement to the cloud is not without its risks. Just consider the recent cases of Anthem and Sony, both of which fell victim to serious hacks reportedly due to neglecting to ensure cloud environments were secure and that data was protected. These severe attacks—along with those affecting companies like Target, Home Depot and JPMorgan Chase—have led leaders in Washington to push for increased digital privacy (e.g., President Obama's plan to protect students from big data), serving as a reminder that it is time for cloud security to mature. As such, businesses need to move beyond simply applying the guards at the gate, so to speak, and instead wholly embrace information

governance—i.e., making sure information is protected—prior to cloud migration and throughout its lifecycle.

What's more, after migration, your company is now relying on a CSP, so at least some of your business operations, depending on the type of cloud deployment, are now dependent on an outside entity. So whether you like it or not, you two are in business together. You are now subject to the quality of their management and execution. Again, doing the due diligence up front to help ensure that you find a CSP that is a true partner—i.e., one who goes to bat on your behalf—is paramount to your organization's information governance success.

Cloud migration poses additional problems due to the sheer number and variety of CSPs that find their way into an organization—whether the organization knows it or not. For example, it is no longer atypical for an organization to use one or more providers for their web presence, another for email, several for CRM, a few more for project management, several for development, and an uncountable number of providers for messaging and collaboration. Managing this mess, which includes a complex mix of both trivial and critical information, is clearly a big challenge. Therefore, partnering with a CSP that has experience with cloud-to-cloud integration is also advisable.

To ensure that data is secure and that the river of information in your organization flows freely, it is essential that you develop purposeful strategies that address both business goals and legal requirements—*before* moving to the cloud. Experienced and trusted CSPs that become your partners can help you formulate these strategies to help ensure your information governance success. Remember, these strategies must be centered on information governance best practices that guarantee your organization maximizes the value, and minimizes the risk, of its cloud investment.

E-Discovery in the Cloud: A Primer

> *"Experts estimate that conducting an [e-Discovery] event may cost upwards of $30,000 per gigabyte."*
>
> – Minnesota Journal of Law, Science & Technology

Failure to develop an information governance and e-Discovery strategy prior to moving to the cloud could lead to a disaster down the road. The use of the cloud does not change the legal requirements for e-Discovery. However, it may fundamentally challenge an organization's ability to meet those requirements. E-Discovery in the cloud creates a host of new challenges:

- **A third party is involved in controlling your data.** Businesses that partner with CSPs have to recognize that instead of being able to conduct the e-Discovery process wholly in-house, third-party entities now play crucial roles in data storage and retrieval. So in addition to the quality of your internal processes, you need to ensure that the CSP you select cares as much about fast and thorough e-Discovery processes as you do. This may be the exception rather than the rule, so be sure to vet your CSP up front so you're on the same page in this area. According to a recent survey, 95 percent of CSPs were unsure of their clients' basic legal requirements and didn't see the importance in supporting e-Discovery in the first place. Although that statistic sounds discouraging, remember that there are CSPs that specialize in the information governance space and do understand compliance and e-Discovery. This simply points out the necessity to ask the right questions about data management and retrieval when choosing your CSP.

- **Your business is subject to your contract and the third party's ability to execute.** When you partner with a CSP, you're bound to what's written in the fine print of your contract. It is therefore crucial that you ask would-be providers questions about their ability to support your e-Discovery and information governance needs. Ask about their experience and subject-matter expertise. What does your CSP's service-level agreement (SLA) say about responsibility for data loss? Don't forget that you are bound to the cloud vendor's technology, too. So ask about your potential CSP's agility and its track record on downtime and disaster recovery. The time and effort required to export data from the CSP is another critical e-Discovery consideration.

- **You are not the CSP's only customer.** Public cloud vendors in particular are in the business of economies of scale. Specialized requirements, such as supporting the often frustrating, contradictory, and laborious e-Discovery protocols may not fit into your CSP's business model. Private cloud vendors may be better suited to cater to your specific needs for legal discovery.

Despite these challenges, a recent study concluded that only 16 percent of organizations put together e-Discovery plans prior to moving their data to the cloud. Rather than knowing where they would stand in the event the e-Discovery process began, these enterprises will have to keep their fingers crossed and hope for the best.

This, of course, isn't an optimal position to be in—particularly when considering that you're almost certainly going to be dealing with numerous CSPs thanks to specific business needs and rogue employees. But by proactively placing information governance at the center of your cloud transformation strategy before migration and deployment, you can rest comfortably knowing precisely where your organization stands in the event the e-Discovery process commences.

E-Discovery in the Cloud: A Closer Look

> *"[T]he average medium- to large-sized business actually using between 300 and 400 cloud apps."*
>
> – ZDNet

The combination of employer-sanctioned cloud services and those that employees choose to use without company permission creates a cacophonic virtual ecosystem that can be challenging to navigate during e-Discovery.

Digging further, let's take a look at how each step of that process is affected by the cloud when information governance is not built into the cloud environment from the outset.

1. **Possession, custody and control.**

   Ignorantia legis neminem excusat—ignorance of the law excuses no one. Failure to get a grip on your data won't free you from your responsibilities, as the courts have repeatedly ruled that data held by third parties still remains in the possession, custody and control of organizations. So no matter what, businesses are required to produce appropriate electronically stored information (ESI) as requested—even if it's not "physically" in their possession.

   Since that's the case, it's worth revisiting possible difficulties associated with information kept in the cloud if proper due diligence is not undertaken. For starters, contractual issues could impede your ability to access relevant data (e.g., a vendor that doesn't offer 24/7 support could leave you on your own during your time of need). A CSP's lack of the proper technology could also limit your ability to track down the right documents (e.g., a vendor that has a rudimentary disaster recovery plan). You might also encounter jurisdictional problems if your firm is located in a different state or country than the CSP.

   By rooting your cloud transformation in robust information governance strategies, you can proactively address these potential problems upstream—before they occur. To do that, make sure that contracts include provisions on access for e-Discovery, clearly state who owns the data and offer comprehensive customer support. Additionally, work with seasoned CSPs that offer high availability and redundancy, and pay attention to geographic location when choosing vendors.

2. **Identification and preservation.**

   Once it appears as though litigation or an investigation is about to commence, businesses have the responsibility to identify possible ESI locations and sources.

They must then work to isolate and preserve those documents, making sure they are protected in a legally defensible manner.

It can be difficult enough to implement a successful data retention policy inside the walls of your own company. When you add a third-party provider into the mix, the process can become needlessly more complicated. To ensure your organization is able to successfully complete the identification and preservation stages of e-Discovery, it's essential to partner with a CSP that takes data retention and access just as seriously as you do. Find a CSP that enables you to mimic your internal data retention policies in the cloud. Choose a vendor that is contractually obligated to help you gain hold of your data—not one that will leave you on your own if you call after 5 p.m. or on a weekend.

It's a lot easier to conduct e-Discovery on your internal network or a hard drive that lives on-premises. Depending on the type of cloud you have deployed, searches can be limited and relevant data can often be overlooked. To avoid such a fate, look for transparent vendors who invest in cutting-edge technologies that allow data to be selectively identified and preserved quickly. It's also worth considering whether the CSP has application programming interfaces (APIs) that can serve as alternative methods for tracking down relevant data.

Some vendors' service packages include automatic deletion provisions, so it's critical that you know up front what kinds of data can be preserved in your cloud environment. Believe it or not, even if you've made a prompt request to suspend automatic deletion on your account, you may still be held liable for lost data. To avoid such an unfavorable outcome, find out how well a hold can be implemented with your CSP, as well as which kinds of holds—like the case, custodian, source type and date range—are available.

Organizations must also consider who's responsible in the event that spoliation—the destruction of data—occurs in the cloud. While some courts have ruled spoliation only occurs if intentional wrongdoing is uncovered, others have concluded spoliation results from simple negligence. To sidestep any would-be headaches and sanctions, it's best to figure out which entity would be responsible for spoliation from both a contractual and legal perspective prior to cloud migration.

3. **Collection, review and processing.**

Once e-Discovery is initiated, businesses are required to produce all pertinent information in a timely manner. To ensure both compliance and long-term financial vitality, you need to be able to track down that data in a cost-effective and efficient way that meets legal deadlines. (This can be even trickier to accomplish

thanks to rogue employees using cloud services without IT's knowledge or consent.)

Due to the sheer volume of the information your company stores in the cloud, it can be practically impossible to find the files you need if the CSP lacks modern technology. Before migrating, you need to know whether the vendor has the tools necessary to execute targeted searches and collections. You also need to know whether these tools will preserve the integrity of your data.

To ensure portability of data, make sure to also ask the CSP how easily you will be able to migrate your data to a new environment should the need to do so materialize. By covering all of your bases prior to moving to the cloud, your business is far less likely to encounter any unforeseen obstacles during the process of collecting and reviewing ESI.

4. **Production.**

Businesses see the cloud as a cost-effective way to modernize their technological infrastructure, giving them the agility necessary to thrive in today's fast-paced digital world. But while it might be cost-effective to store data in the cloud, the e-Discovery process does not lend itself to similar economies of scale. A business might pay $100 to store a terabyte of data in the cloud. But in the process of e-Discovery, that same amount of data can cost $1 million to collect, process, review and produce.

Each instance of e-Discovery has its unique set of circumstances which lend themselves to their own acceptable forms of production. But just because accessing your hosted email account might be easy doesn't mean production of ESI during an investigation or lawsuit is similarly simple.

The courts, for example, have ruled that producing images of documents that are stripped of metadata and lack any indication of where records start and stop is an unacceptable form of production. So you can't just produce data any old way; you have to follow specific terms. You're less likely to encounter these kinds of unimagined roadblocks—and therefore less likely to face the associated sanctions or other penalties—if you agree with your CSP about which forms are used to store and produce data in the cloud ahead of migration.

Additionally, in public cloud environments, one company's proprietary data might be woven in with another's, making it that much more difficult to produce. In fact, if the contract doesn't call for it, CSPs might refuse to cooperate with your requests altogether. Remember, you wouldn't be out of the clear in the event that occurred, as courts have concluded businesses are still responsible for their data, even when

it's stored on third-party servers. It's therefore imperative to know precisely how CSPs store data before partnering with them.

By understanding the ins and outs of how your CSP operates and working with them to draft litigation plans prior to migration, these kinds of problems can be prevented altogether. Such plans should include timeframes for production, and they should also mention the physical location of the servers on which your data is stored so as to prevent any jurisdictional problems during the retrieval process

5. **Presentation.**

   For ESI to be admissible in e-Discovery inquiries, it must pass a number of hurdles, including whether it's relevant, authentic and original. It must also have value that outweighs unfair prejudice—just like most other evidence—and parties must prove an exception to the hearsay rule. But because ESI can be easily edited, altered or redacted, proving the authenticity of documents is that much more challenging: Think about how hard it could be to prove authorship of emails, instant messages and text messages (e.g., it's not too difficult to create a fake account and spoof someone else's identity). To make sure you're not scrambling to try and figure out how to prove authenticity, seek CSPs that offer extensive audit and reporting capabilities and log all changes made to ESI once it's moved to the cloud.

   In e-Discovery, businesses have the ability to produce ESI in native format, i.e., as it exists digitally, or image format, i.e., near-paper form. While it might cost less and be easier to produce things like emails and memos in image format; in the age of big data, spreadsheets and databases might better lend themselves to native format so presenters are able to better showcase the requested data.

   To ensure there aren't any downstream problems in presenting pertinent data in e-Discovery, you should choose a versatile vendor that will work with you to accommodate provisioning proper ESI formats for both unstructured and structured data. The more time you spend addressing presentation issues at the outset—when you begin the cloud migration process—the less you'll have to worry about having a difficult time procuring relevant data in whichever format makes sense for your specific situation.

It's important to note that in today's data-driven environment, we are no longer discussing cloud solely for review and production purposes. Rather, a CSP will now be used to manage, store and secure your most sensitive data—not simply to help with search, review, processing and production. Beyond that, IG-enabled CSPs can streamline the entire e-discovery process, minimizing the risks associated with over-preservation and over-retention of collections—problems many businesses have experienced with traditional third-party reviewers.

Using Information Governance to Prepare for the Unexpected

> *"Forewarned, forearmed; to be prepared is half the victory."*
>
> – Miguel de Cervantes

In addition to preparing themselves internally and collaborating to develop mutually agreeable contracts with CSPs, organizations also need to plan for factors over which they have no control. As you go about developing your information governance strategies ahead of cloud migration, it's important to consider the following truths:

- **Change is inevitable.** You won't have any control over your CSP's business operations. Whether through reorganization or mergers and acquisitions, your vendor's entire business might be restructured at any moment. To that end, so could yours. Business, technology and the regulatory environment continues to evolve and with that, change is inevitable. You can't stop any of these things from occurring or their outcomes. But you can put yourself in a position to be ready should you encounter them by drafting comprehensive contingency plans.

- **Disasters happen.** Manmade or otherwise, no one can prevent disasters from occurring. To make sure your data is ready to weather any storm or accident, look for trusted and proven vendors that offer high redundancy and high availability. That's the path to business continuity—and smooth e-Discovery—in most imaginable scenarios.

- **Understand and internalize your CSP's business model.** Once e-Discovery commences, you might think that your case is the most pressing in the world. For your organization, it might be. But chances are your CSP has a slew of other customers and at any given point in time, they may be dealing with other subpoenas or requests from different clients. It is important to understand the value your CSP places on customer service and how they handle such dilemmas.

Looking Ahead: Cloud Migration Is an Information Governance Opportunity

By choosing to be proactive and integrate a comprehensive information governance strategy into your organization's approach to the cloud, you can put the right safeguards in place upstream that help ensure e-Discovery requests can be competently addressed downstream in a timely and fluid manner.

Is your organization well positioned to conduct e-Discovery? If not, you wouldn't be alone. According to a recent survey, only 26 percent of businesses consider themselves "very prepared" to respond to e-Discovery requests. Still, 92 percent of them expect the frequency of such requests will stay the same or increase over the next year.

To protect an ever-increasing amount of proprietary data, and therefore help ensure that you're ready to promptly respond to e-Discovery inquires, it's essential that your organization incorporates intelligent information governance strategies into the cloud migration process. Seeking a CSP that provides information governance and e-Discovery services along with the expertise required can smooth this transition. In so doing, you can rest comfortably knowing your company's information assets are readily available and easily uncovered at a moment's notice, thereby simplifying your e-Discovery challenge.

Viewpointe

Delivering the Power and Promise of Information Governance™

Established in 2000, Viewpointe has a legacy of providing purpose-built, private cloud services for some of the world's most elite companies. Created by leaders in the financial industry to answer the most complex, information-centric challenges facing our data-driven world, Viewpointe has developed a unique business model that has led to its well-known and unmatched pedigree as an information governance Cloud Service Provider to regulated industries.

At Viewpointe, we know that getting to a place of information strength and power, requires experienced leadership and a consultative approach to catalyze forward progress. Our unique business model combines hardware, software and unsurpassed experience to deliver high-value, customized information governance solutions that bring true value and opportunity for your business.

Viewpointe is centered on the following elements of operation:

- **Trusted Provider:** First and foremost, Viewpointe is trusted by many of the world's most elite organizations. Viewpointe has tens of billions of sensitive documents stored in its private cloud. Selected to the FinTech 100 every year since 2006, Viewpointe is trusted by C-level executives to work as an exclusive partner to catalyze the most critical internal information governance initiatives that demand immediate progress.
- **Robust Security and Compliance:** A top priority for Viewpointe, the company's robust security and access control measures undergo rigorous annual testing and auditing, including SOC 1 and SOC 2 Type II audits (SSAE16), as well as FFIEC. Over 50 individual customer audits are conducted annually. Our multi-layered security infrastructure is at the foundation of our services.
- **Reliable Performance:** Viewpointe provides a multiple data center architecture that is highly redundant with built-in failover. Providing stringent SLAs that are continuously monitored, Viewpointe maintains the high availability of services demanded by regulated business.
- **Scalable Service:** The Viewpointe archive grows by hundreds of millions of items each month. It is architected to easily scale to match an organization's long-term growth requirements, as well as episodic growth periods. It also allows for easy cost allocation to departments based on use.
- **Extensible Cloud Service:** Viewpointe's service interfaces with external cloud environments, internal applications and all document types while providing a distributed environment. This environment provides the utmost flexibility and extensibility, allowing organizations to solve the most complex information governance challenges for unstructured and structured data.
- **Pay-for-Use Pricing:** With a predictable, easy-to-understand pricing model, Viewpointe helps companies control costs better and eliminate upfront investments in infrastructure and maintenance resources by providing a hosted, managed private cloud for information governance.
- **Committed Partner:** Solving information governance challenges requires a partnership based on trust and experience. Viewpointe considers every client a partner, and as a service-first organization, delivering a premier-level service that generates efficiency and value is the hallmark of our company.

A MESSAGE FROM IGI SUPPORTER VIEWPOINTE

- **Industry Commitment:** To help drive thought leadership and momentum of information governance in the industry, Viewpointe is a Supporter of the Information Governance Initiative and a proud and active member of the EDRM, ARMA and AIIM.

Viewpointe's information governance platform, OnPointe, leverages best-in-class content and records management, archiving, analytics, and eDiscovery technologies to harness information value. The OnPointe platform provides a unique opportunity for information governance to be actualized and have meaningful impact on improving business efficiency, effectiveness and compliance.

Uniquely designed as a foundational platform to handle petabytes of information, OnPointe provides a flexible deployment model so that information management, governance and storage challenges can be addressed based on your business priority. Providing a wide range of information governance services to enable and optimize the collection, archiving and governance of business content, OnPointe features the following components to deliver a comprehensive approach for unstructured and structured data across an enterprise:

- *OnPointe for Messaging*
- *OnPointe for File Shares*
- *OnPointe for Enterprise Applications*
- *OnPointe for Print Stream and Image*
- *OnPointe eDiscovery*
- *Viewpointe Professional Services*

Viewpointe can help bring your information governance strategy to life in our hosted, dedicated private cloud. To find out more about Viewpointe, our services and our solutions, visit viewpointe.com.

Viewpointe