Proliferation of "Electronically Stored Information" (ESI) and Reimbursable Private Cloud Computing Costs

Michael R. Arkfeld
Attorney, speaker and author of
Arkfeld on Electronic Discovery and Evidence (3rd ed.)

LexisNexis®

TABLE OF CONTENTS

"It is change, continuing change, inevitable change, that is the dominant factor in society today. No sensible decision can be made any longer without taking into account not only the world as it is, but the world as it will be … This, in turn, means that our statesmen, our businessmen, our everyman must take on a science fictional way of thinking."

—Isaac Asimov

Executive Summary

As novelist William Gibson once observed, "The future's already arrived; it's just not evenly distributed yet."

It has been almost five years since the courts introduced rules addressing the discovery of electronically stored information (ESI). Since this time, technology has advanced to the level where data that may be relevant to a case may be found in countless mediums and in numbers that seem impossible to narrow down. Data is no longer stored in banker's boxes, but in digital technology—communication is almost entirely done through emails and tweets to Facebook® and instant messaging. Transitioning from paper to a digital "form" has resulted in the proliferation of ESI, doubling your client's data every three years.

Law firms and in-house counsel have to face a harsh reality that their usual modus operandi must advance and assimilate with advancements in the industry to keep up with the ever-increasing data load with corresponding cost increases. Even further, litigation and regulatory actions are on the rise and courts are more stringent on sanctions resulting from failure to adequately identify, preserve and process ESI. For a law firm to surmise that it can effectively manage data in-house with their current IT infrastructure, without leveraging proper outside e-discovery resources, is to expose itself to needless increasing, and sometimes unrecoverable, costs; and clients to possible ineffective representation.

The wise investment is to turn to trusted industry partners that can simplify a firm's automated litigation support process by taking the data and litigation technology load off the firm's shoulders and into a secure and safe environment for storage and processing—into the cloud.

"Private cloud computing" is a new term in the legal vernacular, but it will soon become the imperative when it comes to ESI management. Major businesses and government organizations have already moved to hosting in the cloud, and more are following. Private cloud computing offers a scalable design to grow with your case, dedicated resources, additional customization and control, predictable costs, 24/7 accessibility, self-service and security.

As with any storage system concerning client information, a lawyer must ensure that a trusted provider is selected to prevent any breach of confidentiality, security and reliability of the system. With proper due diligence and reasonable care, attorneys can utilize the benefits of cloud computing within ethical standards.

Recovering your IT costs within ethical constraints is mandatory. By treating the processing and storage of ESI as an "overhead" expense, your firm will gradually weaken as more dollars are diverted to the IT department. The firm's dollar will be spent ensuring compliance with client mandated security and court directives regarding the use of IT in litigation and regulatory matters. Fortunately, this road has already been traveled by several firms taking the approach of recovering their IT costs from their clients.

Just as firms were reimbursed for photocopies in the paper era, law firms will be reimbursed for ESI storage and processing in the digital era.

To change your client expectations, and the lawyers in your firm, will require communication and education. Even though clients do not want to pay for something they did not have to in the past, and the lawyers want to remain competitive and not lose clients, the writing is on the wall. The ever-increasing amount, storage and processing of ESI along with the rise of litigation result in costs that have to be addressed within the firm. The failure to do will end up draining a law firm's resources.

Lawyers and law firms will need to re-engineer themselves, again. Private cloud computing can be an enabler of their client's and firm's strategy. The goal is be the best lawyer you can be and cloud computing can work for you, only if you are willing to take the first step.

PART I—Revolutionary Changes and Volume in Discovery Data—"Electronically Stored Information" (ESI)

Transition to Digital and the Internet

The ubiquitous use of computers for creating electronic information has changed discovery and admission of case information dramatically. Whether in business, government, or at home, information is most often created in an electronic format. "According to a University of California study, 93 percent of all information generated during 1999 was generated in digital form, on computers. Only 7 percent of information originated in other media, such as paper."[1] Not only is this change pervasive, but it occurred quite rapidly.

It only took a short period of time for technology, computers, and the Internet to change the way we create and transmit and store information. In 1975, the first microcomputer was introduced replicating the power of larger computers into a small, compact computer. Over the next 35 years, computers have found their way into millions of households and businesses. Couple this with the introduction of the Internet, it is now easy to transmit voluminous amounts of information created in electronic format to a worldwide audience in seconds.

Today, technology has advanced to the level where relevant ESI to a case may be found in numerous storage media, devices and locations.

Proliferation of ESI

New electronic information that may have some relevance to litigation is experiencing exponential growth. Through normal routine use and the immense storage capabilities of today's computers, there are millions of new electronic and possibly evidentiary items created on a daily basis. Consider the following:

The total amount of digital information created grew from 494 billion gigabytes in 2008, to 800 billion gigabytes (900 exabytes or 0.8 zettabytes) in 2009 or a 62 percent increase, to 1.2 billion gigabytes (1,350 exabytes or 1.2 zettabytes) in 2010.[2]

To put this into perspective, the Library of Congress, which houses 17 million books, would only equal 136 terabytes of information. Five exabytes of information would be equivalent to information contained in 37,000 new libraries the size of the Library of Congress book collections. So in 2010 the amount of information created (1,350 exabytes) would equal 9,990,000 new libraries.[3]

We have entered a world where the definition of "volume" is changing and what is really considered a lot of information is really just the tip of the electronic iceberg.

1. *In re Bristol-Myers Squibb Securities Litigation*, 205 F.R.D. 437, 440 n.2 (D.N.J. 2002).
2. Wikibon Blog, *Information Explosion and Cloud Storage*, http://wikibon.org/blog/cloud-storage/ (last visited April 4, 2011).
3. Peter Lyman & Hal R. Varian, *How Much Information*, University of California at Berkeley, School of Information Management and Systems (Oct. 27, 2003), http://www.sims.berkeley.edu/how-much-info-2003 (last visited on June 1, 2011).

Client Data is Doubling Every Three Years

This exponential ESI growth is being reflected in your client's creation and storage of ESI. It is now estimated that enterprise data is doubling every three years.[4]

But what type of enterprise data is doubling every three years?

> *"IDC estimates that by 2020, business transactions on the Internet business-to-business and business-to-consumer will reach 450 billion per day."*[5]

Email alone, which accounts for 60 – 70 percent of the information being exchanged, is growing with corporate users now receiving on an average 112 emails a day. [6]

Client Retention Policies

Though it would benefit an organization not to retain ESI that is no longer needed and not related to any anticipated litigation, organizations rarely delete ESI.

This revolutionary change in the "form" of discovery from paper to digital and the exponential increase in volume pose many challenges to a law firm in the handling and processing of ESI. A new way of thinking is required to meet these challenges.

PART II—The Problem: Increasing Number of Cases and ESI Volume Are Causing E-Discovery Risks and Costs to Accelerate

Not only do law firms face the challenge of an increasing ESI volume, they also have to contend with:

- Increased Regulatory and Litigation Workload
- Court- and Regulatory-Imposed ESI Federal and State Rules and Case Law
- Court-Imposed Responsibility to Monitor Client's ESI Systems and Sanctions for Failure to Disclose
- Capability of In-House IT Systems and Administrative Costs
- Recovering IT Costs in Compliance with Ethical Rules

Increased Regulatory and Litigation Workload

Coupled with the proliferation of ESI, litigation and regulatory matters are on the rise.

Fulbright's annual survey revealed that, though declining in 2006 and 2007, lawsuits and regulatory matters have increased from 2008 through 2010. Specifically, "[corporate counsel] expect that contracts and labor/employment actions will continue to consume litigation resources. Regulatory concerns have replaced bankruptcy concerns: 42 percent of energy respondents, 48 percent of financial services respondents and 39 percent of health care respondents list regulatory as the type of action that most concern their company. Looking ahead, one-quarter of all respondents—and one-third of respondents from energy, health care and insurance—expect the number of regulatory proceedings their companies face to increase in the coming year." [7]

From a law firm's perspective, this increase in workload was welcomed in light of the decline that occurred in 2006 and 2007. However, with this increase, they are confronted with issues of how to effectively manage, process and store the increased ESI.

Court- and Regulatory-Imposed ESI Federal and State Rules and Case Law

To address the myriad ESI issues, a whole new body of case law and procedural rules has been formulated into what is now referred to as "electronic discovery."

Electronic discovery has been described as the "disclosure or discovery of electronically stored information [ESI], including the form or forms in which it should be produced . . ." [8]

4. *Big Data Explosion & Emerging Business Patterns*, **http://tinyurl.com/3apmc9p**, (last visited April 4, 2011).
5. Wikibon Blog, *Information Explosion and Cloud Storage*, **http://wikibon.org/blog/cloud-storage/** (last visited April 4, 2011).
6. *Email Archiving Market*, 2010 – 2014—August 2010, The Radicati Group, Inc
7. *Fulbright's 7th Annual Litigation Trends Survey Report*, http://www.fulbright.com/litigationtrends21 (last visited April 4, 2011).
8. *Junk v. Aon Corp.*, No. 07-4640, 2007 U.S. Dist. LEXIS 89741, at *2 n.2 (D.N.Y. Nov. 30, 2007).

On December 1, 2006, the federal courts amended the Federal Rules of Civil Procedure and mandated the disclosure of "electronically stored information" (ESI). ESI includes email, word-processing documents, spreadsheets, voice mail, text messaging, databases, deleted ESI and any other type of digital information. Even prior to the passage of the 2006 amendments, the courts held that the definition of "documents" under Rule 34 includes "paper" and all types of computer data, as well as "deleted" data.[9]

Among the primary driving forces behind the implementation of the amended FRCP electronic discovery rules, which have been copied in over 15 state rules, were:

- The volume of ESI is significantly greater than paper;
- Systems that create, store, and transmit ESI are often complex;
- ESI may need to be preserved, restored, or processed before it can be reviewed for privilege, trade secrets, or responsiveness.

Court-Imposed Responsibility to Monitor Client's ESI Systems and Sanctions for Failure to Disclose

Duty to Monitor

During this transition from paper to digital information, the courts have imposed heightened and affirmative responsibilities on counsel to monitor their client's electronic discovery efforts to ensure the proper disclosure of ESI. In *Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422, 432 (S.D.N.Y. 2004) the Honorable Shira Scheindlin stated:

> *"[I]t is not sufficient to notify all employees of a litigation hold and expect that the party will then retain and produce all relevant information. Counsel [both in-house and outside counsel] must take affirmative steps to monitor compliance so that all sources of discoverable information are identified and searched."*

Sanctions

The failure to monitor and disclose responsive ESI can often lead to sanctions.

Litigation is one of the riskiest and costliest events a business can encounter. This has become increasingly so with the proliferation of ESI. There are many cases where the courts have not hesitated to impose sanctions, default judgment or spoliation instructions for failure of a party to preserve electronic information or to disclose electronic information in their possession. Organizations are being routinely sanctioned for failing to properly identify, preserve and disclose ESI. Below is a sampling of these cases.[10]

Jail Time

"For such clearly contemptuous behavior, a very serious sanction is required. Accordingly, I order that [defendant's] ... acts of [ESI] spoliation be treated as contempt of this court, and that as a sanction, he be imprisoned for a period not to exceed two years, unless [defendant pays] ... attorney's fees and costs ..."[11]

Plaintiffs Sanctioned

Plaintiffs sanctioned with an adverse inference instruction for failing to preserve ESI when they reasonably anticipated bringing an action against the defendants.[12]

Compliance Officer Sanctioned

SEC sanctioned securities company and compliance officer $100,000 for failing to preserve and produce the personal email and personal computer of independent securities contractor. Contractor barred from employment in securities area for two years.[13]

The use of cloud computing will reduce the staff and technological issues surrounding the storage and security of your ESI and permit the firm to focus on the legal ESI issues that oftentimes result in sanctions for your client.

9. *Kleiner v. Burns*, No. 00-2160, 2000 U.S. Dist. LEXIS 21850, at *11-12 (D. Kan. Dec. 22, 2000).
10. *See also*, Willoughby et al, *Sanctions For E-Discovery Violations: By The Numbers*, Duke University Journal (Nov. 15, 2010).
11. *Victor Stanley, Inc. v. Creative Pipe, Inc.*, 2010 U.S. Dist. LEXIS 93644 (D. Md. Sept. 9, 2010).
12. *Pension Comm. of the Univ. of Montreal Pension Plan v. Banc of Am. Secs*, No. 05-9016, 2010 U.S. Dist. LEXIS 1839, at *14 (S.D.N.Y. Jan. 15, 2010).
13. *In the Matter of vFinance Investments, Inc.* (July 2, 2010), http://www.sec.gov/litigation/opinions/2010/34-62448.pdf (last visited May 24, 2011).

Over the last several years, the courts have imposed sanctions in hundreds of cases as a result of the improper identification, preservation and collection of ESI.[14]

Reallocating resources to these critical client areas will better assist the firm and reduce the pressure of increasing your hourly fee due to technological issues.

Capability of In-House IT Systems and Administrative Costs

The law firm is faced with several issues in this changed discovery environment. It must be able to effectively manage and store this ever-increasing volume of ESI and, at the same time, recover its technological disbursements within the constraints of ethical standards.

Technological disbursements for in-house IT systems are diverse and can be expensive. Law firms need to take into consideration increasing costs for facilities (rent, power, cooling and physical security), hardware (application servers, domain controllers, switches and routers, and maintenance and support), storage hardware (SAN, NAS, tape systems and maintenance and support), software (operations and storage management, replication, backup, security from hacking antivirus and other support), WAN and remote access (telecommunications services, Citrix® servers and software and maintenance and other support), and general operations cost (staff salaries and benefits, onsite and offsite tape cartridges and other operating costs).

For example, if enterprise data is doubling every three years then it should be assumed that the same amount of ESI will double for litigation and regulatory matters. In that case, are the high costs of storage and other operational costs being recovered from your client or do they consider this as part of your overhead and, therefore, "free"?

It is important to note that, for any particular matter, the risks to a law firm due to increasing ESI volume in a litigation or regulatory matter exist for additional reasons.

First, with the global economy growing, many multinational companies generate large amounts of ESI which may be stored in multiple countries. Though a request pursuant to Fed. R. Civ. P. 34 must be directed to documents or electronically stored information "in the responding party's possession, custody, or control … ," the focus is on the party's legal right to custody or control of the documents in question, even if the party is not in possession of the documents.[15]

Second, a case's ESI may increase from the court adding additional "claims or defenses," additional parties, enlargement of the scope of the search by adding additional searches or by adding additional custodians.

Third, it is difficult to predict ESI storage requirements, not anticipated just a few short years ago, due to the immense growth of social and business networking data. It is estimated that Facebook processes 10 terabytes each day and Twitter® processes 7 terabytes of data every day.[16] In addition, "more than one-quarter of corporate counsel now say their company uses LinkedIn®, while 22 percent of respondents use Twitter and 17 percent use Facebook."[17]

14. Willoughby et al, *Sanctions For E-Discovery Violations: By The Numbers*, Duke University Journal (Nov. 15, 2010).
15. *United States v. International Union of Petroleum and Industrial Workers*, AFL-CIO, 870 F.2d 1450, 1452 (9th Cir. 1989).
16. *Big Data Explosion & Emerging Business Patterns*, **http://tinyurl.com/3apmc9p**, (last visited April 4, 2011).
17. *Fulbright's 7th Annual Litigation Trends Survey Report*, **http://www.fulbright.com/litigationtrends21** (last visited April 4, 2011).

Evidence demonstrates that there is no alternative to handling large amounts of ESI other than using automated litigation support systems with corresponding computer systems.

With an increased workload and amount of ESI, a firm must invest in more of these systems or in alternative solutions, such as cloud computing.

In the sampling of cases, the courts are mandating that a lawyer use automated litigation support systems to host, hyperlink, and search for responsive ESI.

- *In re Instinet Group, Inc.*, 2005 Del. Ch. LEXIS 195, at *9-10 (Del. Ch. Nov. 30, 2005)(Court rejected the notion that the conversion of ESI to paper was a "paradigm of efficient litigation.")
- *El-Amin v. George Wash. Univ.*, No. 95-2000, 2008 U.S. Dist. LEXIS 85009, at *1-4 (D.D.C. Oct. 22, 2008) (Court ordered the parties "to create a system whereby all existing documents are hyper-linked to fields in a database that will permit the instantaneous retrieval from within the database of the information offered by plaintiffs in support of any factual proposition.")
- *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309, 318 n.50 (S.D.N.Y. 2003)("[b]y comparison [to the time it would take to search through 100,000 pages of paper], the average office computer could search all of the documents for specific words or combination[s] of words in a minute, perhaps less.")
- *Rhoads Indus. v. Bldg. Materials Corp. of Am.*, 254 F.R.D. 216 (E.D. Pa. 2008)(pursuant to FRE 502 plaintiff had not waived privilege protection for approximately 800 electronic documents that were disclosed inadvertently after electronic screening).
- *Spieker v. Quest Cherokee*, LLC, 2009 U.S. Dist. LEXIS 62073 (D. Kan. July 21, 2009)(Court found that estimated attorney fees of $250,000 for a privilege and relevance review by counsel was excessive and could be reduced by utilizing FRE 502).

Traditionally, law firms and other organizations have invested large amounts of money to manage litigation or regulatory ESI in-house using a client/server computing model. Client/server networking is not a recent phenomenon. It has been used by universities and governments for decades and by other organizations since the 1980s.

The problem is that this type of model requires purchasing and upgrading servers and software, hiring administrative and IT personnel and absorbing other IT system costs. With every hard drive or backup tape added to store and ensure the availability of clients' data, the costs increase.

In addition, an important issue is raised whether a firm's resources should focus on the search, review and analysis of ESI, and have the processing and storage outsourced to a cloud computing service provider. This question is posed due to the range of technical issues involved and with the constantly evolving ESI types and devices such as instant messaging, video, Windows® 7, and iPad® (and associated metadata with all three).

For example, this issue is especially important in light of the recent enactment of Federal Rule of Evidence 502 and the explanatory note suggestion that if one uses "reasonable" screening procedures—"advanced analytical software and linguistic tools"—that the inadvertent disclosure of privileged ESI will not result in its waiver. A firm must ensure that the search software being utilized meets this criterion.

Other problems with client/server systems may occur such as the commingling of client ESI.[18] Many law firms have treated these costs as "overhead" and have not directly recovered these expenses from their clients since it is not "billable" work. Unfortunately, this also means that needed upgrades and other IT costs may go unfunded depending upon the profitability of the firm.

18. *Oxxford Info. Tech., Ltd. v Novantas LLC*, 2010 NY Slip Op 8363, 2 (N.Y. App. Div. 1st Dep't Nov. 16, 2010)(Court upheld "confidentiality agreement" requiring a law firm to destroy all of the client's confidential business information even though there was substantial cost in deleting it from law firm's backup copies).

The client/server computing model is changing with the strong emergence of host services or "cloud" computing. Cloud computing is a term that describes the option of using hosted services over the Internet for delivery of products and services—such as automated litigation support solutions for the processing, storage and review of ESI.

Recovering IT Costs in Compliance with Ethical Rules

One of the issues for a law firm is whether the costs for these automated litigation support systems, including increased storage needs, are recoverable from a client and not in contravention of ethical rules.

There are several ethical issues that a lawyer must address pertaining to whether it is appropriate to seek disbursement costs from a client for investments in a hosted or "cloud" solution to manage the ever-increasing ESI volume through automated litigation support systems.

In this upcoming section we will address whether these costs are merely "overhead" costs or whether they are "disbursement" costs, permitting recovery from a client under certain conditions. In addition, "hosted" or cloud computing raises separate client confidentiality and security ethical issues, which can be minimized utilizing "private cloud" computing.

Finally, and most importantly, we will address how to meet clients' expectations that these costs are not "overhead" expenses but a recoverable cost to ensure the quality processing and storage of their ESI.

Presently, an attorney's hourly fee is covering the cost of this increasing overhead expense.

PART III—The Solution: Using Hosted Litigation Services or the "Cloud" from a Trusted Provider to Recoup Expenses and Manage Litigation Within Ethical Parameters

As noted, there are many IT and legal issues facing law firms in this transition to the new digital form of e-discovery, especially in light of the increasing volume and workload. The answer to many of these issues is the recent strong emergence of "hosted" litigation services commonly referred to as "private cloud" computing.

Primer on Hosted Litigation Services and "Cloud" Computing

What is "cloud" computing?

Cloud computing is a term that describes the option of using hosted services (computing platforms and software run by third parties) over the Internet for delivery of products and services, instead of maintaining, processing and storing ESI in-house.[19]

Cloud Computing services are generally divided into three service models: Infrastructure-as-a-Service (IaaS) Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS).

These are defined by the National Institute of Standards and Technology (NIST)[20] to be:

- Cloud Software-as-a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a Web browser (e.g., Web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

19. *Rearden LLC v. Rearden Commerce, Inc.*, 597 F. Supp. 2d 1006, 1021 (N.D. Cal. 2009) ("'Cloud Computing'—a term used to describe a software-as-a-service (SAAS) platform for the online delivery of products and services").
20. SP 800-145, DRAFT A NIST Definition of Cloud Computing, **http://tinyurl.com/4dmorxe** (last visited on April 26, 2011).

- Cloud Platform-as-a Service (PaaS). The capability provided to the consumer is the ability to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application-hosting environment configurations.

- Cloud Infrastructure-as-a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

When choosing an SaaS application, you would contact a third-party cloud provider such as Yahoo!® or Gmail™ for Internet-based e-mail. To maintain marketing information, you could use Salesforce.com®. Other cloud providers or ASPs provide online computer applications for litigation support, legal holds, centralized databases, timekeeping and billing, banking, benefits administration, payroll interface, compensation analysis, compliance tools and more.

These service models provide opportunities for a firm to leverage the IT expertise of the provider with the office and litigation support applications of the firm's choosing.

For example, a firm may decide to host a litigation support application that they subscribe to such as Concordance® or CaseMap®. The firm would contract with the private cloud provider who would manage this application on dedicated servers located outside of the law firm. However, the control, supervision and management of the litigation software would be under the auspices of the firm. As a result, the firm would reduce their in-house IT operational and equipment costs and be protected against scalability issues involving ESI growth. Additionally, they would gain access to IT expertise, enhanced security, backup and disaster recovery and other supplemental services.

Who is Moving to the Cloud?

Many of your client organizations—business or government—have already moved to the cloud environment or are strongly considering the transition.

The reason? Businesses want to increase sales and lower IT costs. Many companies are moving away from the old computer archetype (client/server) where computers and all data storage are located onsite to ensure control of data. The list of enterprises on the cloud are vast and include: *The New York Times*®, Nasdaq®, MAJOR LEAGUE BASEBALL® and many others.[21]

One of the most significant cloud computing converts is the federal government. In a must-read report, the chief information officer of the United States published a policy document entitled "Federal Cloud Computing Strategy."[22] In the report, which targets a 20 billion dollar investment in cloud computing, it states:

21. *Top 10 Enterprises in the Cloud,* http://tinyurl.com/5nmgyf (last visited April 26, 2011).
22. *Federal Cloud Computing Strategy*, http://www.cio.gov/documents/Federal-Cloud-Computing-Strategy.pdf (last visited on May 23, 2011).

> *"By leveraging shared infrastructure and economies of scale, cloud computing presents a compelling business model for Federal leadership. Organizations will be able to measure and pay for only the IT resources they consume, increase or decrease their usage to match requirements and budget constraints, and leverage the shared underlying capacity of IT resources via a network. Resources needed to support mission critical capabilities can be provisioned more rapidly and with minimal overhead and routine provider interaction ...*
>
> *To effectively provision selected IT services, agencies will need to rethink their processes as provisioning services rather than simply contracting assets. Contracts that previously focused on metrics such as number of servers and network bandwidth now should focus on the quality of service fulfillment."*

The reason cloud computing has become popular is because a cloud provider has the proper resources to provide myriad computer services supported by a large-scale IT environment allowing many users to share the same IT expertise and infrastructure. These services are important and range from scalability, flexibility, enhanced security, backup and disaster recovery and other supplemental services. The provider can easily analyze the law firm's computing needs and can, for example, purchase additional servers and spread the cost of managing the servers over all of its users. Ultimately, law firms are free to focus on the practice of law and not the IT infrastructure.

What Are the Reasons to Use Cloud Computing?

Depending on the type of cloud computing you use, there are many issues to consider when deciding whether to contract for hosted or cloud computing services to mange, process and store ESI.

- Scalability issues are easier to resolve

Cloud services are scalable so they can be increased or decreased depending upon your ESI or other applications' need. Reputable cloud service providers have the capacity to scale up if your case ESI increases due to the addition of parties, additional claims or defenses, additional search terms, etc. The user does not need to know their exact upfront computer needs and can request additional storage and additional resources on demand.

As previously noted, your client's ESI growth will double in the next three years, which will impact your computing needs. Therefore, it is wise to determine now if cloud services are needed in your firm.

- Predictable Costs and Expense Savings

A cloud offers several cost advantages over the traditional client/server in-house IT environment.

The firm's litigation support applications can be installed on the private cloud and your existing litigation support staff would still manage the software and client data, including the ESI responsive to the case. Therefore, the investments already made in the software and modifications, training and other services associated with your firm's litigation support systems would remain intact. The applications would be transferred to a secure private cloud, but the control and management of the litigation software and other applications would be retained by the firm. The headaches of maintaining the scalability issues, security, disaster recovery, backups, and ensuring IT expertise would be the responsibility of the cloud provider.

Cloud services provide a predictable budget expense since hosted solutions typically charge based on users per month, Internet activity or storage requirements (such as a gigabyte).

Cost savings would result due to no "up front" capital investment in hardware or software (depending on your needs), design and setup, nor administrative expenses (including consultants). Additionally, the firm would not be burdened with having to address IT issues involving improper design of the system.

Since cloud solutions are managed by a hosting provider, organizations can free up their own IT staffs for other important tasks.

Other savings would result from reduced need for office space, less power consumption, no cooling requirements, and no installation and cabling.

- Access and Available—24/7 from anywhere, anytime

Conveniently, a lawyer or other legal professional only needs a personal computer and Internet access to utilize cloud services. They would be able to store, access and retrieve ESI at any time, from anywhere.

A legal professional can work from home, office or even while traveling, through use of myriad devices including a desktop, laptop, iPhone® or iPad. In fact, law firms could easily open new offices since there is no need for an IT infrastructure. Since reputable cloud systems are usually up and accessible 99 percent of the time, a lawyer would not have to deal with the downtime of an in-house system due to power failures, hardware malfunctions and other unforeseen problems. Some cloud providers guarantee uptime in their contracts.

- Security, Redundancy and Backups, and 24/7 Support

Security

Regardless of being in a paper or paperless environment, security and confidentiality of ESI and other client data remains a major concern in using an in-house IT system or cloud computing. With paper, not only do you need to ensure that your office is physically secure against theft or fire, but you must consider other security issues such as whether an offsite paper storage facility is secure.

With in-house systems you have to guard against outside hackers, employee theft and possible violations of client confidences.

As Professor Richard Susskind noted in his law firm technology predictions for 2011: [23]

> *"Many firms will move their data and processing to the cloud. Confidentiality concerns are being addressed and, in any event, it is probable that a first-rate outsource provider will offer better security than many firms can provide for themselves. This applies to litigation as much as to other things—much litigation data is either price-sensitive or very personal; how many firms can say in a post-WikiLeaks world that they are truly confident of their own security?"*

Law firms are now being required by their clients to comply with ISO® 27000 standards as they pertain to their client's data stored on the law firm's servers. "The [ISO 27000] series provides best practice recommendations on information security management, risks and controls within the context of an overall Information Security Management System … The series is deliberately broad in scope, covering more than just privacy, confidentiality and IT or technical security issues. It is applicable to organizations of all shapes and sizes.

23. *eDisclosure Information Project*, http://tinyurl.com/2cs84av (last visited April 26, 2011).

All organizations are encouraged to assess their information security risks, then implement appropriate information security controls according to their needs, using the guidance and suggestions where relevant. Given the dynamic nature of information security, the ISMS concept incorporates continuous feedback and improvement activities, summarized by Deming's "plan-do-check-act" approach, that seek to address changes in the threats, vulnerabilities or impacts of information security incidents." [24]

In addition, the private cloud site is usually physically more secure than a typical office building in protecting against theft as well as natural disasters.

There are numerous other examples of security breaches of ESI data. There was a recent insider trading scandal where an associate lawyer was able to "browse" the headings of documents in a document management system to discover when mergers were going to occur.[25] This internal work product should have been sealed off from other associates just like litigation ESI should be secure to protect against breaches of client confidences.

Finally, in a recent study, at least 60 percent of data theft or loss occurred as a result of portable computing device theft or malicious insiders.[26]

Law firms should not be in the business of risking exposure of their client's data to hackers and others; instead security and its increasing complexity should be outsourced to a private cloud.

Redundancy

Cloud service providers should be able to provide redundancy services. This service would ensure that ESI is backed up and located at more than one location to guard against any disaster that would wipe out data stored all at one location.

Backups

Reputable cloud service providers usually have multiple backup features to guarantee data preservation in the case of power failure and other emergencies. As an extra measure, the data is often encrypted while being sent and while in storage.

Support

There are many technological issues (operating and application software, accessibility and other issues) that confront law firms as we rapidly transition into a more complex IT environment. Private cloud computing allows 24/7 support for these issues and, depending upon whom you choose, a trusted partner for the firm to rely on for their IT expertise at any time.

- Faster, More Timely Solution Upgrades

Depending on the cloud service you select, you may be provided a seamless upgrade path to the latest versions of litigation support software or other applications on the cloud. In-house systems present special problems with software upgrades, especially with firms that have multiple offices. These solutions deployed in the cloud can be utilized more uniformly to users in various geographic locations.

24. Wikepedia, *ISO/IEC 27000-series*, **http://en.wikipedia.org/wiki/ISO/IEC_27000-series** (last visited on May 20, 2011).
25. *SEC Charges Corporate Attorney and Wall Street Trader In $32 Million Insider Trading Ring*, **http://www.sec.gov /litigation/litreleases/2011/lr21917.htm** (last visited April 22, 2011).
26. KPMG 2010 *Data Loss Barometer Report*, **http://tinyurl.com/6jjnrxc** (last visited on April 26, 2011).

Other Law Firms Are Generating Revenue Storing and Processing ESI

Several major law firms are processing and handling ESI and, in the process, generating revenue for the firm.[27]

In this article, several firms noted that they process ESI for their clients and for other law firms and have even considered spinning off an e-discovery company to avoid conflict of interest problems. Some of the reasons for not using an outside vendor are that it permits a firm to retain control over their work and it ensures timely processing.

One firm noted that their cost of processing ESI was approximately $250 per gigabyte and were charging $1,200 per gigabyte to their client.

However, one law firm noted that though it can be a huge income stream in the short term—"clients are happier if you keep costs to a minimum, and happy clients are what give a law firm long-term success."

Overhead or Disbursable Costs and Ethical Issues

There are several ethical issues that a lawyer must address pertaining to whether it is permissible to outsource a client's ESI to a "cloud" computing platform. This includes such issues as: client confidentiality, overhead and disbursement costs.

As you know, a lawyer is obligated to adhere to various codes and rules of conduct that are adopted by the state(s) where they are licensed to practice, including any ethical obligations set forth in applicable case law or statute. It is suggested that a lawyer check with their bar association regarding the various issues with "hosted" or "cloud" computing and overhead and disbursable expenses.

Initially, the question to consider is whether it is it permissible to outsource the processing, handling and storage of your client's ESI through the use of a host or cloud computing platform ("cloud" computing).

Outsourcing to a Cloud Computing Platform

Generally, ethics opinions find that counsel may use cloud computing as long as reasonable care is taken in the selection of a provider and that precautionary measures are in place to ensure the security of confidential client information. Opinions hold that a lawyer must confirm that the technology adequately protects client confidences and that the service provider has in place reasonable measures to prevent unauthorized access to client data.[28]

For example, the New York State Bar Association concluded that:

> *"A lawyer may use an online data storage system to store and back up client confidential information provided that the lawyer takes reasonable care to ensure that confidentiality will be maintained in a manner consistent with the lawyer's obligations under Rule 1.6. In addition, the lawyer should stay abreast of technological advances to ensure that the storage system remains sufficiently advanced to protect the client's information, and should monitor the changing law of privilege to ensure that storing the information online will not cause loss or waiver of any privilege."*

Overhead and Disbursements Analysis

Another recurring ethics concern is whether you can pass on to your client the charges for online services provided by a "hosted" or cloud computing provider.

27. *The Data Boom: Can Law Firms Profit?*, http://www.law.com/jsp/llf/PubArticleLLF.jsp?id=900005481542 (last visited April 26, 2011).
28. NY Ethics Opinion 842 (9/10110) , http://tinyurl.com/2b6hdu6 (last visited on April 26, 2011); Cal. State Bar Form. Op. 2010-179 (2010), http://tinyurl.com/5rj9ame (last visited on April 26, 2011); Arizona Committee on the Rules of Professional Conduct Opinion 05-04, http://www.myazbar.org/Ethics/pdf/05-04.pdf (last visited on May 31, 2010) (must ensure confidentiality of ESI preserved); Nev. St. Bar Standing Comm. on Ethics and Professional Resp. Formal Op. 33, http://www.nvbar.org/ethics/opinion_33.pdf (last visited on May 31, 2010).

One of the most oft-cited ABA opinions in this area has analyzed this issue by dividing the costs (other than professional fees) into three areas: general overhead; disbursements; and in-house provision of services.[29] In the absence of an agreement, a client can reasonably expect overhead expenses to include mortgage or rental costs for the location of the law firm space, professional malpractice insurance, and utilities expenses; thus, all included as part of the professional fee charged by counsel.[30]

Presently, an attorney's hourly fee is covering the cost of this increasing overhead expense.

Disbursements, Other Than "Overhead" Costs, Present Special Issues

As a general rule, in addition to charging a client professional fees for their services (including overhead charges), lawyers may also charge their clients for additional expenses referred to as "out-of-pocket, disbursements or additional charges."[31] In the context of this paper, the issue is whether a firm can bill the cost of private cloud computing services to a client as a disbursement.

At the initial stage of representation, counsel will generally disclose in writing their professional fees and costs for certain items that are to be passed on to the client. These may include deposition costs, travel expenses, photocopy charges, costs of service of a complaint and other items, which are generally "disbursement costs."

In ABA Formal Opinion 93-379, supra[32], when discussing professional fees and disbursements, the ethics committee clearly stated that if the disbursements are disclosed to the client, and the client consents, then it is permissible to charge what the law firm chooses as long as it is reasonable. For example, the opinion specifically approves an agreement between the client and the attorney to charge for photocopying at 15 cents per page and messenger service at $5.00 per mile. The committee noted that:

> *"On the other hand, in the absence of an agreement to the contrary, it is impermissible for a lawyer to create an additional source of profit for the law firm beyond that which is contained in the provisions of professional services themselves."*

What this means is that, in the absence of disclosure and consent of the client, the prevailing view is that a lawyer may only charge the "actual" costs of an in-house service plus a reasonable allocation of overhead expenses directly associated with the service (i.e., allocated cost of librarian for managing online research and actual online research costs). The committee recognized that the actual cost and allocation of overhead expenses was an accounting issue.

It would seem that the same analysis should hold true for the reimbursement or charges for a "hosted" or "cloud" computing system based on a charge per gigabyte of storage or a similar measure. If a client understands and agrees to the charge per gigabyte, then such charges may be passed along to the client.

29. ABA Formal Opinion 93-379 Dec. 6, 1993), http://tinyurl.com/65unc4q (last visited on April 26, 2011).
30. Restatement 3d of the Law Governing Lawyers, § 38.
31. ABA Formal Opinion 93-379, supra; Alabama Ethics Opinion Number: 2005-02, http://www.alabar.org/ogc/fopDisplay.cfm?oneId=402 (last visited on April 25, 2011).
32. *See also*, Model Rule 1.5(b)("the basis or rate of the fee and expenses shall be communicated to the client, preferably in writing, before or within a reasonable time after commencing the representation, except when the lawyer will charge a regularly represented client on the same basis or rate").

Recovering the Cost of Processing and Storing ESI

It is a bit ironic that, during the "paper" era, the cost of photocopying was passed on to the client as a separate charge, and now in the "digital" era, the cost of storage and other processes concerning ESI may be passed on to a client.

For years, law firms have generated revenue from photocopying services for their clients. In this article, which discusses the costs of operating a photocopier, the author suggests using the following engagement letter in disclosing recoverable costs:

> *"It is our policy to utilize the personnel who can most efficiently handle the task to be accomplished. In addition to our hourly rate charges, which are billed in quarter (1/4) hour task increments, we will bill for all out-of-pocket expenses incurred on your behalf, including all charges for photocopying, long-distance telephone calls, postage, word processing, telecopier, court filing fees, court reporter fees, mileage and travel costs, parking charges, file storage fees, office supply fees, consultation fees for outside professionals, exhibit and witness fees, delivery fees, service of process fees, subpoena fees, and all other necessary and incidental expenses incurred on your behalf."*[33]

As noted, ABA Model Rule 1.5 provides that for costs such as telephone or copying charges or other out-of-pocket expenses, lawyers can charge a reasonable amount to which the client agrees in advance or an amount that reflects costs incurred by the lawyer.[34]

Further guidance is provided in the Restatement of the Law (3d) of The Law Governing Lawyers, § 38, Subsection (3)(a) which provides that, "unless the contract construed in its circumstances provides otherwise, a lawyer may not recover from a client payment in addition to the agreed fee for items of general office and overhead expense such as secretarial costs and word processing. A client lacking knowledge of the lawyer's usual practice cannot be expected to assume that the lawyer will charge extra for such expenses. The lawyer may, however, charge separately for such items if the client was told of the billing practice at the outset of the representation or was familiar with it from past experience with the lawyer or (in the case of a general billing custom in the area) from past experiences with other lawyers."

In the digital era, an engagement letter should include "hosting services for the processing and storage of ESI will be billed at $___ per gigabyte."

Changing Client Expectations and the Law Firm Culture

As the volume of data grows, the need to recover costs to handle e-discovery processing and storage becomes more and more critical. However, what about clients and law firm members who are used to these "overhead" charges and do not want to change?

Client Expectations

Let's face it, clients do not want to pay for something that they didn't have to pay for in the past. However, we have already seen many other firms charging for this processing and storage service. These firms' profitability increased because of the charges for e-discovery processing and storage services, which were not part of their overhead expense.

33. James Wirken, *Using Your Photocopier as a Profit Center*, http://www.mobar.org/4a06ac73-6e7e-424f-826e-00422ea9b4fc.aspx (last visited April 26, 2011)
34. See also ABA Formal Opinion 93-379 (approves an agreement between the client and the attorney for charging copying at 15 cents per page and messenger service at $5.00 per mile).

However, it is necessary to provide the supporting documentation and increasing costs in the handling and management of ESI to your clients. Otherwise, the profitability of your firm will decrease as you attempt to continue to absorb these costs as part of your overhead. By using private cloud computing for your software platform applications, while maintaining your current IT and staff infrastructure, you are actually saving the client more money than if the firm completely outsourced the hosting and management services.

Law Firm Culture

In addition, law firms want to maintain their competitive edge and do not want to pass along their cloud computing expense if they could lose clients.

Oftentimes, the question asked is, "How much can cloud computing save on my IT budget?" A cloud ROI calculation can be hard to pin down. However, you can attempt to measure the cloud ROI based on server reduction, savings on new server provisioning, reduced operating expenses and the payback period from new IT spending.

As previously noted, technological disbursements for in-house IT systems are diverse and can be expensive. Law firms need to take into consideration increasing costs for facilities (rent, power, cooling and physical security), hardware (application servers, domain controllers, switches and routers, and maintenance and support), storage hardware (SAN, NAS, tape systems and maintenance and support), software (operations and storage management, replication, backup, security from hacking antivirus and other support), WAN and remote access (telecommunications services, Citrix servers and software and maintenance and other support), and general operations cost (staff salaries and benefits, onsite and offsite tape cartridges and other operating costs).

Maybe the question that should be asked is, "How many more matters can I handle when using cloud computing; how much more efficient will we be in processing, storing and reviewing ESI for disclosure? In addition, will my legal obligations under the rules such as FRE 502 be met by using the search software of a reputable provider?"

Education and Communication

Part of the solution to these difficult issues is to educate and communicate with your clients and law firm partners. There are several methods of providing your client and firm members with the necessary information to justify a cost recovery approach regarding the processing and storage of ESI. These methods include seminars (with both partners and management in attendance), white papers, case law and other materials.

Information Provided Should Include:

- Background history of law firm's handling of ESI
- Review the ABA opinion (ABA Formal Opinion 93-379, Dec. 6, 1993)
- Present the current status of your firm's billing procedure/policy re ESI
- Educate regarding the value of data storage, risks and the cost
- Present different ESI processing and storage scenarios
- Provide statistics reflecting the proliferation of ESI
- Present cost figures for processing and storage of ESI (both internal costs and outside provider costs)
- Provide information on how the firm is structured and the risk of continuing to absorb this cost in the overhead category
- Ask the clients or law firm members to argue the other side
- Provide information as to the value of cloud computing and how other companies (maybe their own clients), agencies and other firms are using it to reduce and track costs and ensure security

Trusted Provider—Confidentiality, Security and Reliability

When selecting a cloud computing provider, you will want to ensure the provider has a sustainable business that you'll be able to depend upon in the long term. In fact, several ethics opinions require that a lawyer perform due diligence when selecting a provider.

Topics to Investigate Should Include:

- How long have they been in business?
- How many customers and employees does it have?
- Is it profitable? (failure to answer should serve as a warning)
- What happens if the provider goes bankrupt?
- What is its privacy policy?
- What is the procedure to transfer ESI to a different provider?
- If you choose to leave the cloud service, can you easily take your data with you?
- Is it possible to export your data in a useable form, and if so, is there an associated cost?
- What type of search capability does the system have?
- Does its search capability comply with FRE 502?
- How often is the data backed up?
- What are its redundancy policies and at what physical locations?
- What is the disaster recovery plan?
- Will the provider provide physical backups of the data to store offsite?
- How reliable is the service regarding online availability?
- When were the last five times the system "crashed" or was down for repairs?
- Does the system maintain data integrity?
- What security is provided against hackers and other unauthorized access?
- Does it follow any particular industry standards for security?
- Are their employees screened and background checks performed?
- Can the data be shared across competing cloud platforms?
- Is the system scalable?
- Is there 24/7 support?
- Where are the data centers located—in the United States or out of the country?
- Does the agreement provide that you own all of the data uploaded or entered into the cloud provider's service and it will not be re-used for any purpose other than providing you access to the service and your data?
- Who's liable for stolen data? Does the service provider disclaim liability?
- Will the provider provide an indemnification provision for losses that are the fault of the cloud provider?
- Will the data remain in a form that can be used by your in-house computer applications?
- What are the procedures or notice provisions to alert you if a provider is served with a legitimate government order or subpoena for access to your ESI?
- Are there any issues with EU privacy laws and the location of the data?

CALLOUTS

Automated Litigation Support (ALS)

ALS generally refers to technology operations that support legal functions in litigation. These functions include an overall plan, document indexes, witness depositions and indexes, correspondence and deposition management, ESI control, interrogatory control, production document control, admissions, pretrial orders, substantive motion preparation, opening statements, closing arguments, and so on.

ASP

ASP is an acronym that stands for Application Service Provider, a technology company that provides software or service "application" through the Internet directly to your computer. Instead of the software or service application residing on your computer or network, it resides on a "mainframe" or "server" computer at a remote location and you connect to the software application or service through the Internet. These providers are sometimes referred to as "cloud" providers.

Client/Server

A type of computing that divides tasks between clients and servers. Client/server networks use a dedicated computer called a server to handle files, print, and perform other services for client users. The client (usually the less powerful machine) requests information from the servers. Cloud computing or Software-as-a-Service (SaaS) is a term that describes the option of using hosted services over the Internet for delivery of products and services.

Electronically Stored Information

(ESI) is digitally stored information. Fed. R. Civ. P. 34.

Cloud Computing

Is a term that describes the option of using hosted services (computing platforms and software run by third parties) over the Internet for delivery of products and services, instead of maintaining, processing and storing ESI in-house.

FRE 502

(Federal Rule of Evidence 502) applies to inadvertent disclosure of privileged information, and the explanatory note suggestion that if one uses "reasonable" screening procedures—"advanced analytical software and linguistic tools"—that the inadvertent disclosure of ESI will not result in its waiver.

Private Cloud Computing

Is a term that describes the implementation of using cloud hosted services (computing platforms and software run by third parties) that are dedicated to your organization. With private cloud computing you get many of the same benefits of public cloud computing with additional control and customization available from dedicated resources. This private structure provides the scalable design to grow with your case load, predictable costs, 24/7 accessibility, self-service and security. These systems can have dedicated servers for a firm and be logically separate from other customers data.

About the Author

Michael R. Arkfeld is an attorney, speaker and author who is involved on a daily basis in the discovery and admission of electronic information. Among his writings are the *Arkfeld on Electronic Discovery and Evidence* (3rd ed.) treatise, *Arkfeld's Best Practices Guides for Electronic Discovery and Evidence, ESI Pretrial Discovery—Strategy and Tactics, Legal Hold and IT Primer for Legal Professionals* available from Law Partner Publishing (**www.lawpartnerpublishing.com**) and also from LexisNexis (**www.lexisnexis.com/store**). He is also the author of *The Digital Practice of Law: A Practical Reference for Applying Technology Concepts to the Practice of Law*. Michael is a member of the State Bar of Arizona and the recipient of the national 2004 E-Evidence Thought Leading Scholar Award. His websites at **www.arkfeld.com** and **www.elawexchange.com** feature additional electronic discovery and evidence materials and resources.

As a former assistant United States Attorney for the District of Arizona, Michael handled cases involving personal injury, medical malpractice, wrongful termination and a host of other tort claims. He has appeared before both federal and state appellate courts and has extensive experience in jury (over 30 trials) and bench trials. Since 1985, Michael has incorporated personal computers extensively in his legal practice. He lectures and consults throughout North America and internationally on the impact of technology on the practice of law and the discovery and admission of electronic evidence. Michael can be reached by e-mail at **Michael@Arkfeld.com** or by phone at **602-993-1937**.
