WHITE PAPER

Key Issues in eDiscovery

An Osterman Research White Paper

SPONSORED BY

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 253 630 5839 • Fax: +1 253 458 0934 • info@ostermanresearch.com
www.ostermanresearch.com • twitter.com/mosterman

EXECUTIVE SUMMARY

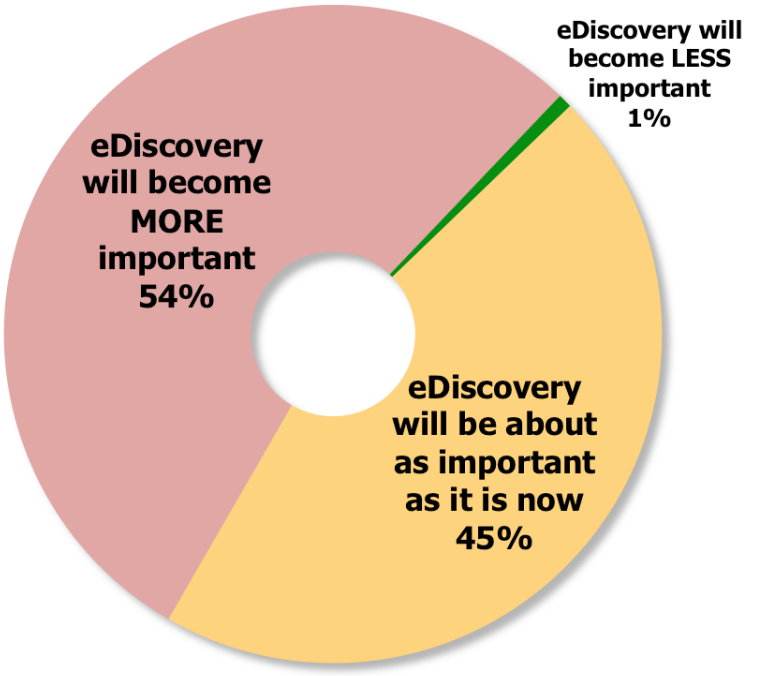
Discovery involves the preservation, search, analysis and production of relevant information that might play a role in civil litigation. Its importance can be summed up by the Zubulake standard:

> "[A] party has a duty to preserve all evidence, including electronically stored information ('ESI'), that it knows, or should know, is relevant to any present or future litigation."

What this means for every business is that it must retain all of its relevant electronic content – emails, files, databases, social media posts, instant messages and the like – and do so systematically and following a set of procedures that will allow it to satisfy all of its legal obligations.

While the formal process of discovery has been a key element of civil litigation for decades, eDiscovery has become much more important over the past 10-15 years as the proportion of electronic content in most organizations has become more voluminous and more difficult to manage than information on paper. As evidenced by the following figure, businesses and other organizations believe that eDiscovery will remain just as important over the next 12 months as it is today, or it will become more important.

Anticipated Importance of eDiscovery During the Next 12 Months



KEY TAKEAWAYS

- The consequences of poor data management practices – inadequate archiving, no ability to implement legal holds, lack of competence, etc. – include significant legal judgments, loss of corporate reputation, and an increased level of overall risk.

- Poor eDiscovery results in poor decision-making because those charged with managing litigation – as well as the overall organization – do not have sufficient insight about what is happening within their organization.

Poor eDiscovery results in poor decision-making because those charged with managing litigation – as well as the overall organization – do not have sufficient insight about what is happening within their organ-ization.

- Good eDiscovery results in lower direct costs because of the reduced number of person-hours that must be invested in the collection, processing and review of information; and lower indirect costs because of reduced corporate risk.

ABOUT THIS WHITE PAPER

This white paper discusses the important practices and technologies that any organization should implement in order to improve eDiscovery and drive its cost as low as possible. The paper also presents the results of a primary market research survey conducted specifically for it that highlights the key problems that organizations have with current eDiscovery practices. Finally, a brief overview of Micro Focus, this paper's sponsor, is included.

SHOULD YOU CARE ABOUT eDISCOVERY?

DEFINING TERMS

Discovery is the critical process of searching for information that may be relevant for use as evidence in a trial or in pre-trial activities. It can include any sort of communication, document, metadata, advertisement, statement or other information that might be useful to prove a plaintiff's or defendant's case in a civil action.

"eDiscovery" is simply the extension of this well-established process to any Electronically Stored Information (ESI) that an organization might possess – email messages, presentations, spreadsheets, word processing files, tweets, Facebook posts and any other communication or information that might be useful in a civil legal action. By extension, eDiscovery can extend to any platform on which ESI is stored: desktop computers, laptops, smartphones, tablets, backup tapes, servers, and even employees' home computers and other personally owned devices.

ENORMOUS GROWTH IN THE AMOUNT OF ELECTRONIC DATA UNDER MANAGEMENT

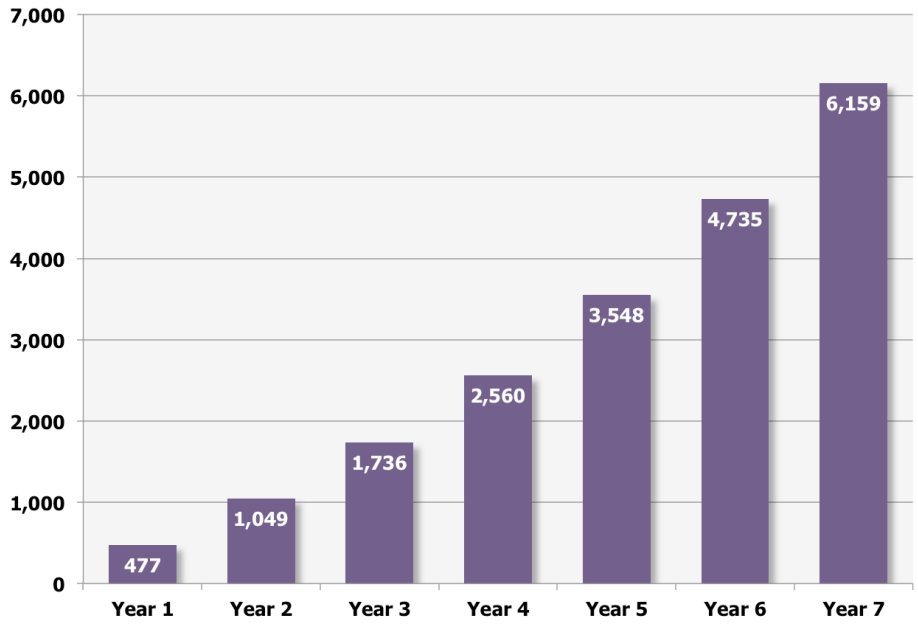
Organizations of every size create, send, receive and store an enormous and growing amount of digital information. For example, the IDC Digital Universe study estimated that 1.8 zettabytes (1.8 trillion gigabytes) of information were created and replicated during 2011, a nine-fold increase from 2006 and more than doubling every two years[i]. Moreover, IBM estimates that each day 2.5 quintillion bytes of data are created[ii]. While much of this data is normally not subject to eDiscovery – e.g., television programming and the like – the enormous scale and growth of ESI is illustrative of the problem that organizations have, and will have, in finding and producing ESI in their organizations. As just a simple illustration of data growth in a mid-sized company, consider the figure on the following page that demonstrates the growth of content storage in a typical organization with 1,000 email users.

While discovery has focused traditionally on paper documents, over the past several years ESI has become a much more important component of discovery for the simple reason that a growing proportion of corporate content is electronic and never meets paper. Consider the following:

- ESI is normally stored in much greater volume than are hard copy documents.
- ESI can be modified quite easily.
- ESI is often not readable apart from the system(s) that created it.
- ESI contains information that is not normally displayed to users – metadata – that describes the context of the information and provides other useful and important information.

While discovery has focused traditionally on paper documents, over the past several years ESI has become a much more important component of discovery for the simple reason that a growing proportion of corporate content is electronic and never meets paper.

Seven-Year Archiving Requirements for a 1,000-Person Company
Gigabytes of Content Storage



ESI consists of a large number of data types, as noted earlier, that may be in any number of locations:

- Email systems
- Social media data stores in the cloud or stored locally
- Collaboration systems like SharePoint®
- Real-time communication systems like Sametime
- Repositories of structured and unstructured data
- Employees' home computers
- Corporate and employee-owned smartphones
- Tablet computers (e.g., Apple iPad, Dell Streak, etc.)
- Corporate wikis and blogs
- Desktop computers
- Laptop computers
- File servers
- USB storage devices (e.g., flash memory sticks, iPods, etc.)

While email is often the most important single source of content in most organizations, there are many other content types – and locations in which it might be stored – that organizations must include among their discoverable content sources.

Preservation of this content without a true archiving system is a challenge for many organizations for a number of reasons:

- They must then determine where all of their content is located (no easy feat in any organization, let alone a distributed one).
- They must back up this data to a central location or have ready access to it when required.
- They must extract content from backup tapes or disk – an arduous task for IT even under good circumstances.

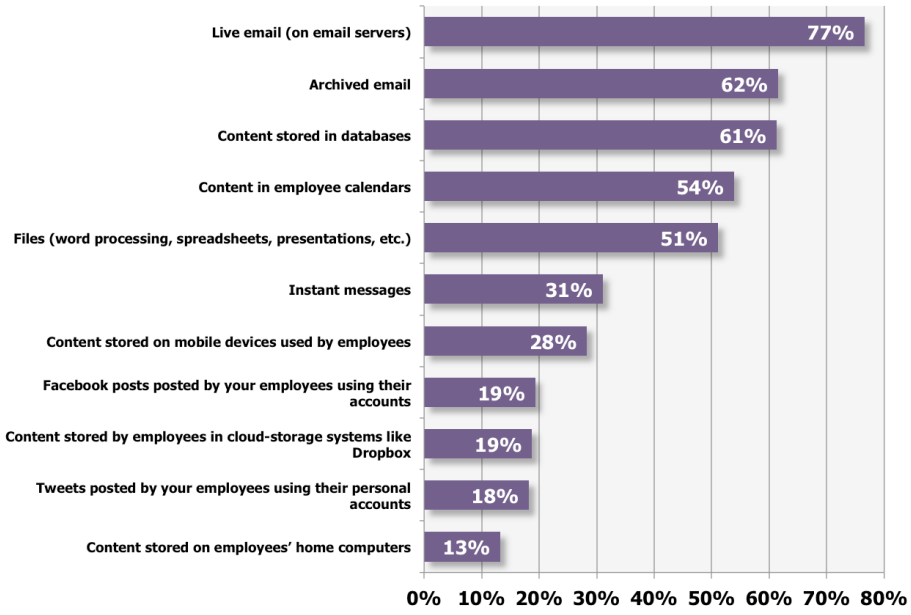
While email is often the most important single source of content in most organizations, there are many other content types – and locations in which it might be stored – that organizations must include among their discoverable content sources.

WHERE ARE WE WITH eDISCOVERY TODAY?

ORGANIZATIONS ARE (SORT OF) PREPARED FOR BASIC eDISCOVERY, BUT NOT MUCH ELSE

Osterman Research has discovered that the vast majority of organizations believe they are reasonably well prepared to deal with searching for, finding and producing live email – i.e., content on email servers – in the context of eDiscovery. However, they are much less prepared to satisfy eDiscovery requirements for other types of content, particularly social media and cloud-based content repositories, as shown in the following figure.

Preparedness to Search, Find and Produce Various Types of Content
% Responding Prepared or Very Well Prepared

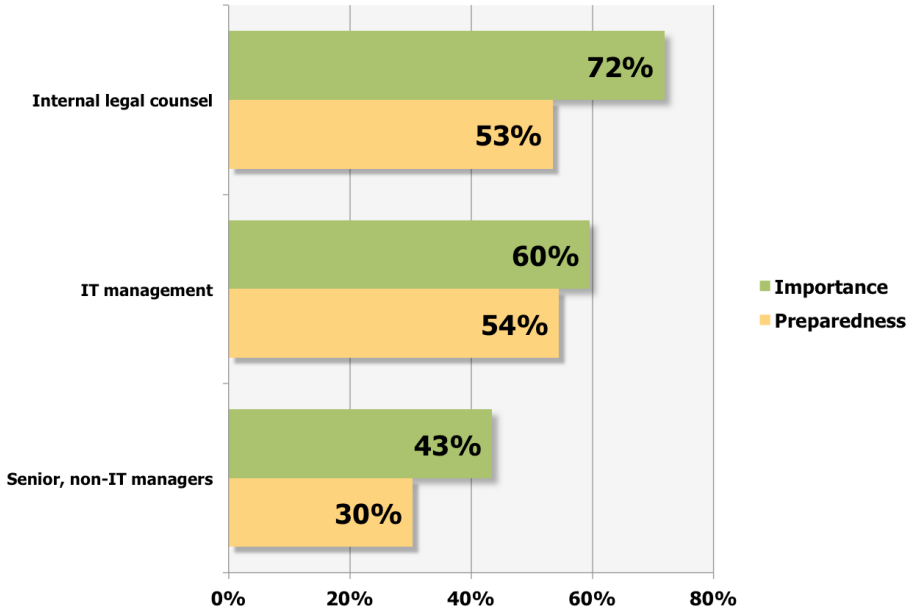


THE DISCONNECT BETWEEN IMPORTANCE AND READINESS

Our research also discovered that internal legal counsel and corporate management believe eDiscovery is important, but they are not as prepared for it as they need to be. For example, nearly three-quarters of internal legal counsel considers that eDiscovery is important or extremely important to their organizations, yet only slightly more than one-half of them are prepared or very well prepared to deal with the issues presented by eDiscovery. Similarly, both IT management and senior, non-IT managers place greater importance on eDiscovery than they do on their preparedness to deal with the issues presented by it.

Nearly three-quarters of internal legal counsel considers that eDiscovery is important or extremely important to their organizations, yet only slightly more than one-half of them are prepared or very well prepared to deal with the issues presented by eDiscovery.

Importance of and Preparedness for eDiscovery by Various Groups
% Responding Important or Extremely Important
% Responding Prepared or Very Well Prepared



THE GROWING IMPORTANCE OF PREDICTIVE CODING

Traditional eDiscovery relies on linear document review – the process of manually reviewing and coding potentially relevant and privileged content. While this process works well for relatively small data sets, the review of large data sets makes linear document review inefficient and time-consuming. Moreover, it contributes significantly to the growing cost of eDiscovery because of both the multiple reviews of the same content that often must take place, as well as the production of content that ultimately will not be useful. Underscoring the enormous cost associated with reviewing documents during eDiscovery are the findings of a Rand analysis that found the review phase of eDiscovery accounts for 73% of the costs of producing electronic documents[iii].

A much more efficient approach for document review is predictive coding, also known as computer-assisted review. This technique employs an expert's review of key documents, followed by computer review of potentially relevant content, assigning a rating to each document based on how closely documents match the expert-reviewed documents. Predictive coding generally results in more accurate coding, as well as faster document review and lower costs of eDiscovery.

While predictive coding is not yet widely used, the technology was given a significant boost by a federal judge in the case of *Da Silva Moore v. Publicis Groupe et al*[iv]. The judge in this case ordered the adoption of a protocol that includes predictive coding.

THE BASICS OF DISCOVERY

THE FEDERAL RULES OF CIVIL PROCEDURE

The Federal Rules of Civil Procedure (FRCP) consist of a set of rules that are focused on governing procedures for managing civil lawsuits in the United States district courts. While the United States Supreme Court is responsible for overseeing the FRCP, the United States Congress must approve these rules and any changes made to them.

A much more efficient approach for document review is predictive coding, also known as computer-assisted review. Predictive coding generally results in more accurate coding, as well as faster document review and lower costs of eDiscovery.

Several important changes to the FRCP went into effect in December 2006. The modifications represented many years of debate at various levels and had a major impact on electronic discovery within U.S.-based organizations. Many companies have responded to these changes by improving their information management and eDiscovery practices, although many have not.

Among the key elements of the FRCP changes are the following:

- An expansion of discoverable material to include all ESI that might be relevant in a legal action [Rule 26(a)].
- A schedule conference to discuss eDiscovery and other issues must be held within 120 days after a legal action is initiated [Rule 16(b)].
- Within 99 days after a legal action commences, the parties must come to an agreement about the protocols and procedures that will govern the eDiscovery process [Rule 26(f)].
- When a party requests information as part of eDiscovery, they can specify the format in which they would like it to be provided [Rule 34(b)].
- Sanctions can be avoided with the court's blessing if ESI is lost because of good faith deletion practices that were not intended to destroy evidence [Rule 37(f)].

In summary, these changes reflect the fact that discovery of email and other ESI is now a routine aspect of most litigation. As a result, decision makers need to keep in mind that ESI is treated differently than paper-based data; the FRCP rules now require early discussion of, and attention to, eDiscovery as an integral component of any legal action; organizations should address the inadvertent distribution of privileged or protected materials; organizations must now focus on a two-tiered approach to discovery in which they must first deal with reasonably accessible information and then later focus on less accessible data; and, finally, the rules can provide a safe harbor from sanctions by imposing a good faith requirement.

KEY ELEMENTS OF A SOUND eDISCOVERY SYSTEM

As part of an overall eDiscovery strategy, there are several things that any organization must ensure it can satisfy well in order to minimize the risk of problems during legal actions. While these apply specifically to eDiscovery, the general principles involved largely apply to satisfying regulatory obligations, as well:

- **Respond quickly to eDiscovery requests**
  FRCP Rule 26(a)(1) requires that organizations have a solid understanding of their data assets and that they are able to discuss these issues ahead of the initial pre-trial discovery meeting – FRCP Rule 16(b) requires that this meeting take place within 99 days from the commencement of a legal action. Organizations that have not planned ahead for such an eventuality may face a variety of negative consequences, not least of which is the enormous expense and disruption that eDiscovery can create for the unprepared.

  Sometimes, however, organizations have much less time than this to produce the required information. For example, in the case of *Best Buy v. Developers Diversified Realty*[v], the judge in the case ruled that the latter had to produce electronic content within just 28 days[vi].

- **Impose legal holds when necessary**
  If a litigation hold – i.e., a suspension of any deletion of content that might be relevant during a legal action – is required, it is imperative that an organization preserve all relevant data, such as emails, word processing documents that may contain business records, financial spreadsheets, etc. Serious consequences can result from failure to preserve potentially relevant evidence. Courts have discretion to impose a variety of sanctions, including monetary fines, adverse

Serious consequences can result from failure to preserve potentially relevant evidence. Courts have discretion to impose a variety of sanctions, including monetary fines, adverse inferences, additional costs for third parties to review or search for data, or even criminal charges.

inferences, and additional costs for third parties to review or search for data, or even criminal charges. At a minimum, an organization that cannot produce data as a result of deletion may suffer a damaged corporate reputation.

- **Identify what is and is not accessible**
  Each party to a civil litigation must also determine what it can and cannot reasonably produce. If the evaluation determines that certain electronic content cannot be produced because it is not reasonably accessible or it is too expensive to produce, FRCP Rule 26(b)(2)(B) of the FRCP still requires that information about this content must be forthcoming. This might include, for example, information describing content on backup tapes that is in a format that can no longer be read because the equipment that could access the information is no longer in use. This further implies that ESI must be preserved even if it is not reasonably accessible.

- **Manage a growing number of data types and venues**
  Complicating the eDiscovery process further is the fact that there is a large and growing number of data types and platforms on which relevant data may be stored. For example, discoverable content will typically reside on corporate email servers, file servers, SharePoint databases and other IT-managed systems. However, it can also reside on corporate and personal smartphones and tablets, cloud-based data repositories like Dropbox, employees' home computers, USB sticks and a host of other on-premise and cloud-based platforms. One of the more important downsides of the Bring Your Own Device (BYOD) trend, for example, is this proliferation of corporate content in locations that are not under IT's control.

IMPORTANT ISSUES TO CONSIDER

There are a variety of lessons that organizations can take from court decisions about what to do – and what not to do – in the context of eDiscovery. What follows are some notable cases that can shed light on best practices when considering how to plan for eDiscovery:

- **A failure to preserve ESI may lead to sanctions**
  In the case of *Pension Committee of University of Montreal Pension Plan v. Banc of America Securities, LLC*[vii], the Court issued sanctions against parties that did not adequately preserve ESI, citing the "gross negligence" of their actions. This ruling was made even though the judge found that there was no evidence of bad faith on the part of those who did not preserve the required ESI.

- **eDiscovery must be relatively specific**
  In the 2010 case of *Moulin Global Eyecare Holdings Ltd. v. KPMG* that adjudicated in Hong Kong, the court rejected plaintiffs' arguments a request for discovery of ESI that it considered too expansive. The court determined that allowing such broad access to the defendant's electronic information would be "tantamount to requiring the defendants to turn over the contents of their filing cabinets for the plaintiffs to rummage through.[viii]"

- **Backup tapes are not satisfactory for eDiscovery**
  The case of *Johnson v. Neiman*[ix] is a good example of why using backup tapes as the primary source of discoverable content is not a best practice. The defendant argued that it should not have to produce emails that were stored on 5,880 backup tapes, because accessing this information would allegedly have required 14,700 person-hours to catalog and restore, and that an additional 46.7 days would have been required for the creation of .PST files. The defendant argued that this data was not reasonably accessible. Luckily for the defendant, the Court agreed with their position and did not require production of the data. However, a judge could easily have determined that this content should have been archived and ordered the defendants to produce the requested data.

Complicating the eDiscovery process further is the fact that there is a large and growing number of data types and platforms on which relevant data may be stored.

- **Cooperation between parties is essential**
  In *Digicel v. Cable & Wireless PLC*, the defendant made a unilateral decision not to search through their backup tapes for content. Further, the defendant determined the search terms it would use, a decision that the plaintiffs opposed. The British court that heard the case overruled the defendant's decision and ordered it to both restore employee emails that were stored on backup tapes, as well as add a few more search terms. The court was not willing to allow one party to the suit to make unilateral decisions regarding what content was discoverable.[x]

- **Social media content is increasingly part of eDiscovery**
  The case of *Lester v. Allied Concrete Company* is illustrative of the growing importance of social media content in legal actions[xi]. In this case, a personal injury attorney instructed his client to delete various photographs from his Facebook profile instead of placing a formal legal hold on these images, or at least instructing that the content not be deleted. In response, the Court ordered the attorney to pay $522,000 for this spoliation of evidence and required the client to pay $180,000, despite the fact that a jury awarded the plaintiff $8.6 million (later reduced by the Court to $4.1 million)[xii]. The ill-advising attorney no longer practices law.

- **eDiscovery must be managed competently**
  In *Green v. Blitz U.S.A.*[xiii], the Court sanctioned the defendant for a variety of failures, including their representative (who claimed to be computer illiterate) not putting a legal hold on relevant data, not coordinating his work with the defendant's IT department, and not performing keyword searches, all of which resulted in relevant documents not being produced. After key documents were not discovered in this case, but were discovered in another case one year later, the judge a) issued a $250,000 civil contempt sanction against Blitz, b) ordered the company to inform plaintiffs from the past two years about the sanction, and c) to include a copy of the sanction memorandum in every case in which it will be involved during the next five years.

- **Metadata may need to be produced**
  Judge Shira Scheindlin, who ruled in the landmark *Zubulake v. UBS Warburg* case, issued an important ruling in February 2011 that will have important ramifications for the use of metadata. In *National Day Laborer Organizing Network v. U.S. Immigration and Customs Enforcement Agency,*[xiv] Judge Scheindlin a) stressed the importance of metadata in her ruling that "certain key metadata fields are an integral part of public records," and b) that counsel must "make greater efforts to comply with the expectations that courts now demand …with respect to expensive and time-consuming document production."

- **Home computers may constitute part of your discoverable content**
  In *Orrell v. Motorcarparts of America, Inc.*[xv], the Court ordered the production of a plaintiff's home computer for forensic examination because it contained information that allegedly had been wiped from the plaintiff's company-supplied laptop computer.

HOW CAN YOUR ORGANIZATION BENEFIT FROM PROPER eDISCOVERY?

BE PROACTIVE INSTEAD OF REACTIVE

All organizations should deploy sound eDiscovery capabilities that include the ability to index content, search for it, allow it to be tagged or classified, and impose legal holds quickly. Moreover, these tools should be sufficient so as to provide decision makers confidence that all relevant data is being held, and that all archived information that is relevant to a case has been discovered (e.g., data on mobile

Good eDiscovery and related tools, policies and practices can help avoid legal actions altogether by ensuring that, through the use of good search capabilities and analytics, corporate policies are being followed on a continual (and, perhaps, near real-time) basis.

devices). The right eDiscovery capabilities can help an organization to be proactive in two important ways:

- Good eDiscovery and related tools, policies and practices can help avoid legal actions altogether by ensuring that, through the use of good search capabilities and analytics, corporate policies are being followed on a continual (and, perhaps, near real-time) basis. This allows an organization to monitor employee behavior on an ongoing basis to look for potentially actionable statements or activities, and to adjust corporate policies on-the-fly to minimize the potential for legal action.

- In situations where a legal action has already begun, robust eDiscovery capabilities can help in early case assessment so that decision makers can understand their legal position early on, at times to an organization's advantage over the opposition. This might include reviewing the likelihood of victory early in a case, allowing an organization either to settle quickly and avoid significant legal fees or an adverse judgment; or giving decision makers confidence that they can prevail and thereby reduce the likelihood of an adverse judgment. Having the right tools lets decision makers focus on the merits of a case instead of the process, and reduced costs lets an organization devote more resources toward resolving the case instead of spending significant amounts on the eDiscovery process itself.

In short, being proactive will help decision makers to make better and more well informed decisions. This will help minimize the negative impact of a legal action and can lead to lower legal fees, the reduced likelihood of court-imposed sanctions, and reduced disruption to normal business operations.

IMPROVE THE EFFICIENCY OF LITIGATION

The right eDiscovery systems, services and tools can help an organization respond to legal actions more effectively. The appropriate tools will help organizations to understand what content they have available and what is not reasonably accessible. These tools can also streamline the eDiscovery process and help organizations respond more quickly and at a lower cost.

LOWER COSTS

Good eDiscovery capabilities can also help an organization reduce the overall costs of managing email content, records and the business itself. These benefits include:

- Avoiding many of the costs associated with outside counsel expenses by reducing the subset of data that has been flagged for legal review.

- Reducing the length of the eDiscovery process, which can result in hard cost savings of internal staff time.

- Reducing other costs, including legal judgments, fines, and public relations damage from negative press.

- Reducing the cost of backing up content by moving older, unstructured data such as email, to content archiving systems.

From an IT perspective, one of the benefits of good eDiscovery is its ability to reduce storage management problems for email and other types of business records. Osterman Research has found in numerous surveys that most of the serious problems involved in managing email systems are storage-related, including problems like large attachments sent through email, growing use of attachments itself, and storing large volumes of older content on primary storage systems connected to live email servers. These are benefits that can be realized in the management of other types of records as well, since this content can also be migrated to less expensive archival storage. The right archiving, litigation hold and related solutions can significantly reduce

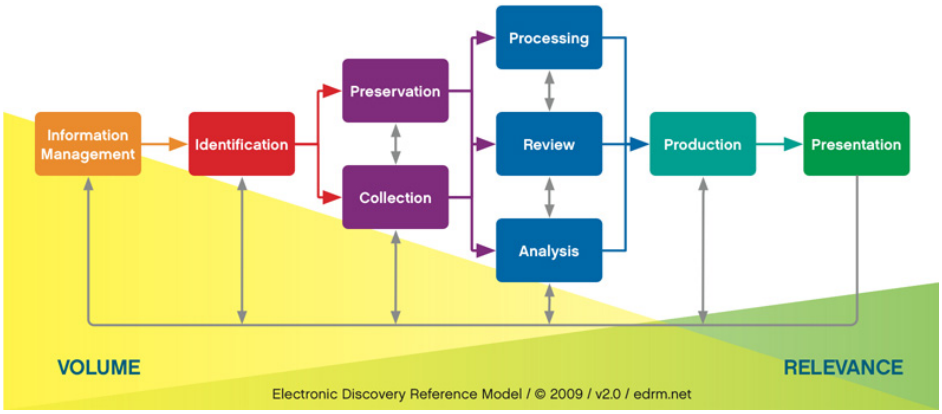
From an IT perspective, one of the benefits of good eDiscovery is its ability to reduce storage management problems for email and other types of business records.

storage costs and provide a number of other email management benefits well beyond just eDiscovery.

ELECTRONIC DISCOVERY REFERENCE MODEL

The Electronic Discovery Reference Model (EDRM), diagrammed in the following figure, was a response to the relatively few standards and lack of generally accepted guidelines for the process of eDiscovery that existed prior to its development. The team that developed the EDRM was facilitated by George Socha (Socha Consulting LLC) and Tom Gelbmann (Gelbmann & Associates), and included 62 organizations, among whom were software developers, law firms, consulting firms, professional organizations and large corporations.

Electronic Discovery Reference Model[xvi]



Begun in May 2005, the goal of the EDRM Project was the creation of a framework for the "development, selection, evaluation and use of electronic discovery products and services". The EDRM, which was placed into the public domain in May 2006, is designed to help organizations manage the process of eDiscovery from the initial stages of managing electronic information through to its presentation.

The EDRM's development was important because it represented a major step forward in the standardization of the eDiscovery process. Standardization is important for eDiscovery for a variety of reasons, most notably because of the growth in the quantity and diversity of ESI, as well as the large number of entities that will need to process this data (internal and external legal counsel, senior managers, archiving solution vendors, cloud-based IT managed services, outside forensics firms and others).

Following development of the EDRM was the EDRM XML project in the 2006-2007 timeframe. The goal of this project was to "provide a standard, generally accepted XML schema to facilitate the movement of electronically stored information (ESI) from one step of the electronic discovery process to the next, from one software program to the next, and from one organization to the next. The EDRM XML 2 project continued the development of the EDRM XML schema for metadata, developing protocols for the number of electronic files that are preserved in their native format, and developing a compliance validation tool, among other projects.

KEY ELEMENTS OF THE EDRM

The EDRM is divided into nine sections that focus on the process of managing an eDiscovery effort:

The EDRM, which was placed into the public domain in May 2006, is designed to help organizations manage the process of eDiscovery from the initial stages of managing electronic information through to its presentation.

- **Information Management**
  This phase focuses on managing electronic content in such a way that an organization can prepare for eDiscovery should that become necessary. The goal of Information Management in an EDRM context is to minimize the risk and cost associated with the entire process of eDiscovery. Managed properly, this step can dramatically reduce the effort required in the subsequent phases of the EDRM process.

- **Identification**
  Understand the "inventory" of ESI that might be relevant in a particular legal action and that might have to be presented during discovery. At this point in the process, discovery demands, disclosure obligations and other pertinent claims and demands are reviewed and considered. The goal at this stage of the process is to understand the universe of information that might be required in order to respond to appropriate eDiscovery requests and then determine the subset of information that will be relevant for further processing.

- **Preservation**
  This is a critical step that ensures that ESI is protected from spoliation and modification, such as through the imposition and enforcement of a legal hold on all relevant ESI. If spoliation does occur, the consequences can be expensive. For example, in the case of *Leon vs. IDX Systems Corporation [2006 U.S. App. LEXIS 23820 (9th Cir. Sept. 20, 2006)]*, the plaintiff deleted 2,200 files from the laptop computer his employer had issued to him. The court dismissed the case and awarded the defendant $65,000 for the spoliation.

- **Collection**
  During this phase, all relevant ESI is collected from the various sources that contain it, including messaging archives, backup tapes, file servers, desktops, laptops, employees' home computers, smartphones and other sources.

- **Processing**
  At this point, collected data is indexed and, thus, made searchable. The data should also be de-duplicated in order to reduce the amount of data that must be reviewed during subsequent phases of the discovery process. Collected data should also be prioritized into a) content that will likely be relevant later in the process and b) content that will likely not be relevant. At this point, decision makers may want to convert ESI into a form that will permit the most efficient and thorough review of its contents.

- **Analysis**
  This phase involves a variety of activities, including determining exactly what the ESI means in the context of the legal action at hand, developing summaries of relevant information, determining the key issues on which to focus, etc.

- **Review**
  The review phase includes evaluating the content for its relevance, determining if specific items are subject to attorney-client privilege, redacting ESI as appropriate, etc.

- **Production**
  The production of data involves delivering the relevant ESI to any parties or systems that will need it. It also includes the activities focused on delivering ESI in the appropriate formats (e.g. in native or image format) and form(s), including DVDs, CD-ROMs, paper, etc.

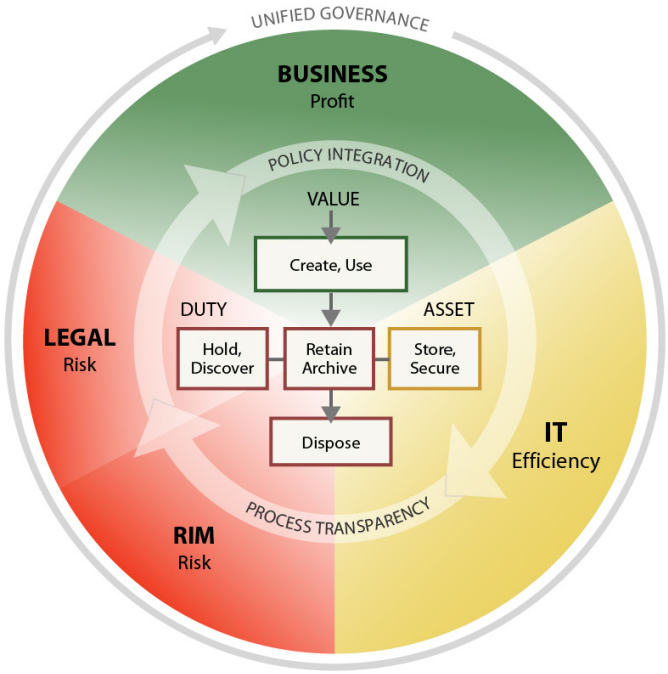
- **Presentation**
  The presentation of ESI is a key consideration at various points of the eDiscovery process – as information is reviewed, analyzed, produced, etc. The specific forms of presentation for ESI will vary widely depending on the content; how, where and by whom the content will be presented; and other factors.

The purpose of the Information Governance Reference Model (IGRM) is to "provide a common, practical, flexible framework to help organizations develop and implement effective and actionable information management programs.

THE INFORMATION GOVERNANCE REFERENCE MODEL

The purpose of the Information Governance Reference Model (IGRM) is to "provide a common, practical, flexible framework to help organizations develop and implement effective and actionable information management programs."[xvii] Its goal is essentially to bring together various stakeholders within an organization and provide them with a common framework for discussing and acting on the Information Management node of the EDRM. The IGRM fills an important void because it attempts to integrate the records management, archiving and retention obligations across an entire organization.

Information Governance Reference Model[xviii]



Duty: Legal obligation for specific information

Value: Utility or business purpose of specific information

Asset: Specific container of information

OTHER ISSUES

FEDERAL RULES OF EVIDENCE

Enacted in 1975, the Federal Rules of Evidence (FRE) are a set of requirements that determine how evidence is presented during trial in the U.S. federal courts. These rules are focused mostly on the initial presentation of evidence during trials. Individual states may use these rules as the basis for their own rules of evidence, or they may adopt a different set of rules for presenting evidence at trial. It is important to note that for purposes of presenting evidence, a printed or otherwise human-readable version of electronic evidence is considered to be an original and can be presented at trial according to FRE Rule 1001(3).

Authentication is a key part of the eDiscovery process because its goal is to prove that a document is what its presenter claims it to be – a true and verifiable representation of an electronic document. Authentication for electronic content is even more critical than for paper-based documents, since electronic documents are more easily altered. For example, the process of copying data from one location to

Enacted in 1975, the Federal Rules of Evidence (FRE) are a set of requirements that determine how evidence is presented during trial in the U.S. federal courts.

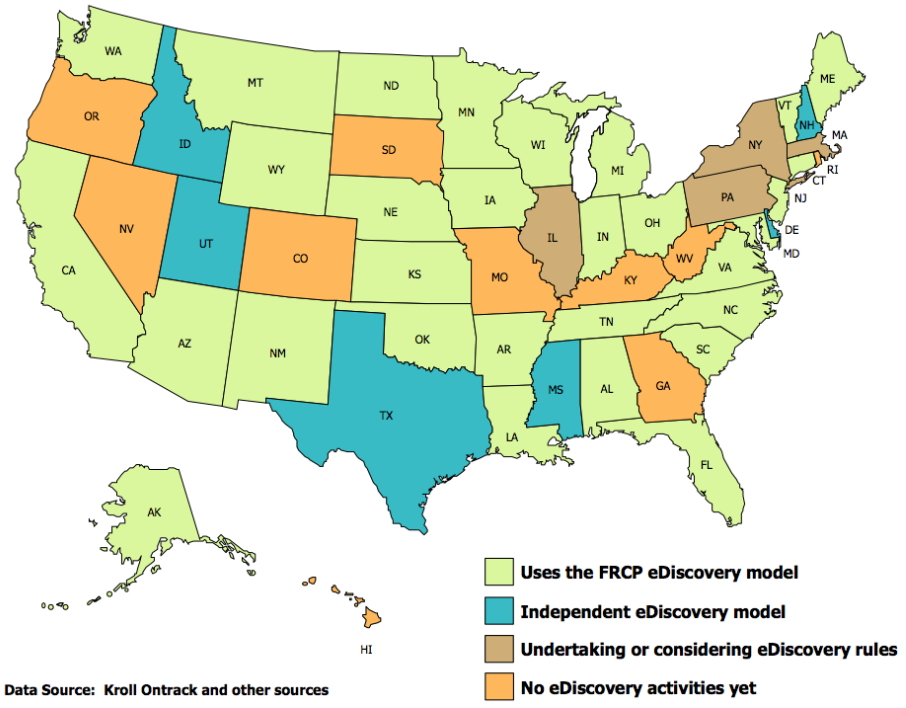
another may actually alter the metadata of that data and call into question its authenticity. When the authenticity of a piece of evidence has been called into question, an attorney may need to depose a witness who can verify the chain of custody of an electronic document, a signature block in an email can be used to provide authenticity, or each party in a legal action can agree to stipulate that electronic records will be considered authentic. Atkinson-Baker has written a good overview of the authentication requirements for electronic records[xix].

Proving the authenticity of electronic records is a major issue that many organizations have not completely resolved. A classic case in point is *Vinhnee vs. American Express Travel Related Services Company, Inc.* In this case, American Express sought payment for more than $40,000 in charges on two credit cards from a California resident who had filed for bankruptcy protection. However, because American Express could not prove the authenticity of the electronic statements it presented during trial, it lost the case even without the plaintiff being present. Another important case, *Lorraine v. Merkel*, saw the Court deny the admissibility of electronic evidence simply because it could not be authenticated[xx]. In Lorraine v. Merkel, the chief magistrate presiding over the case wrote:

> *"…there are five distinct but interrelated evidentiary issues that govern whether electronic evidence will be admitted into evidence at trial or accepted as an exhibit in summary judgment practice. Although each of these rules may not apply to every exhibit offered…each still must be considered in evaluating how to secure the admissibility of electronic evidence to support claims and defenses. Because it can be expected that electronic evidence will constitute much, if not most, of the evidence used in future motions practice or at trial, counsel should know how to get it right on the first try."*

> *"computerized data ... raise unique issues concerning accuracy and authenticity ... The integrity of data may be compromised in the course of discovery by improper search and retrieval techniques, data conversion, or mishandling."*

Status of U.S. States' Adoption of FRCP Requirements



The most useful archiving solutions will provide a verified audit trail showing who accessed archived content and when it was accessed, preventing an original of a document from being altered after the fact and minimizing the potential need to address chain-of-custody issues.

The ability to provide the authenticity of content, as well as the chain of custody for content relevant to a legal action, is one of the more important benefits of an archiving solution. The most useful archiving solutions will provide a verified audit trail showing who accessed archived content and when it was accessed, preventing an original of a document from being altered after the fact and minimizing the potential need to address chain-of-custody issues.

STATE FRCP-RELATED LAWS

The FRCP is but one of the key issues with which litigators and others involved in the eDiscovery must deal. As shown in the figure on the preceeding page, many U.S. states have already passed, or will soon pass, their own version of the FRCP for civil litigation that takes place within their respective state court systems.

eDISCOVERY IN OTHER JURISDICTIONS

Owing to the somewhat fairly litigious nature of society in the United States, U.S. eDiscovery practices are more advanced and requirements more specific than in most other nations. For example, in most of Europe organizations are not required to produce content that runs counter to the claims they make in a legal action. Requirements in the United Kingdom, however, can compel organizations to produce damaging content, but only after a court order[xxi].

While eDiscovery in American legal proceedings is difficult, laws in other parts of the world can significantly complicate eDiscovery (often referred to as "e-disclosure" outside of the United States). For example:

While eDiscovery in American legal proceedings is difficult, laws in other parts of the world can significantly complicate eDiscovery (often referred to as "e-disclosure" outside of the United States).

- At present, courts in England and Wales may or may not require some type of standard disclosure – namely, the disclosure that a document "exists or has existed". The recipient of the disclosure has a right to inspection of the documents, albeit subject to a variety of restrictions[xxii]. However, in April 2013 the UK Civil Procedure Rule 31.5 will go into effect, permitting courts much more discretion when ordering disclosure. Some of the rules are similar to the FRCP in the United States, such as the requirement to disclose relevant documents and the applicability of the Rule to electronic content[xxiii].

- In 2010, Ontario amended its rules of civil procedure in order to accommodate the growth of electronic content as part of the discovery process. Rule 29.1.03(4) now reads "In preparing the discovery plan, the parties shall consult and have regard to the document titled 'The Sedona Canada Principles Addressing Electronic Discovery' developed by and available from The Sedona Conference."

- As is the case in many countries, Mexico does not have pre-trial discovery or disclosure requirements, but the courts will compel litigants and third parties to produce information if it is deemed necessary to the proceedings and if the documents are specifically identified.

- The European Commission Directive 95/46/EC, adopted in October 1995, was designed to standardize the protections for data privacy among all of the member states of the European Union and to protect individuals' right to privacy. The Directive focuses on the processing of individuals' data within the EU, but also applies to any entity outside of the EU to whom this data might be provided, such as during an eDiscovery exercise. The Directive does not permit data to be provided to anyone whose national laws do not adequately safeguard privacy rights.

  Moreover, the *Convention on the Taking of Evidence Abroad in Civil Matters* (the Hague Evidence Convention) – which the U.S. Senate ratified in 1972 – was designed to "establish a system for obtaining evidence located abroad that would be 'tolerable' to the state executing the request and would produce evidence

'utilizable' in the requesting state."

- France imposes even more stringent requirements than Directive 95/46. French Penal Code, Law No 80 – 538 imposes fines and/or jail time for those who seek, request or disclose information intended to develop evidence for foreign legal proceedings.

- Australia's Supreme Court of Victoria, in its Practice Note No. 1 of 2007 (February 2007), strongly suggested that parties to a legal action should consider using technology to improve the efficiency of legal proceedings, including eDiscovery tools. The Federal Court of Australia has gone further and developed eDiscovery rules similar to those contained in the new amendments to the FRCP. Moreover, the Australian Federal Court ruled in 2009 that all cases meeting minimum requirements must be managed only with digital content, not paper.

Blocking statutes, such as the French law noted above, have been in place for many years in various countries and were enacted specifically to block discovery proceedings. For example, blocking statutes exist in Ontario, Canada (Business Records Protection Act), the United Kingdom (The Shipping and Commercial Documents Act) and the Netherlands (Economic Competition Act). The key issue to keep in mind with regard to blocking statutes is that even though data has been found, it may not be usable.

A good analysis of eDiscovery outside of the United States is *E-Discovery Around the World*[xxiv].

WHAT SHOULD YOU DO NEXT?

ACHIEVING THE IT-LEGAL HANDSHAKE

In order to establish a robust eDiscovery capability in any organization, but particularly a larger one, it is essential to start with a "meet-and-greet" among the relevant internal parties. For example, does your IT management know the name of your organization's chief legal counsel? Does legal counsel know the name(s) of your senior IT managers? Are key stakeholders aware of who else would potentially be involved in eDiscovery planning?

Does your IT management know the name of your organization's chief legal counsel? Does legal counsel know the name(s) of your senior IT managers? Are key stakeholders aware of who else would potentially be involved in eDiscovery planning?

Establishing this "legal-IT handshake" is a critical first step toward developing an effective eDiscovery strategy. Having each group familiarize itself with the requirements of the other will go a long way toward helping an organization develop an effective eDiscovery plan. For example, while IT may perceive that all legal counsel needs is a robust search capability for electronic content, the reality is that the legal workflow is more complex than that, and includes search, creating internal workflows for content, review of the discovered content, marking up the relevance of records, exporting data sets for use in forensics analysis tools, sending to external counsel for review, and taking things to the point of production (such as going through the Bates numbering process to serialize a production set).

EMPLOY YOUR EMPLOYEES

While policies, practices, procedures and technologies are all vital, it is essential to educate employees, consultants and others in the organization about the importance of retaining important documents, using corporate communication and collaboration resources wisely, not deleting documents intentionally and the like. Employing users as this first line of defense can go a long way toward improving eDiscovery in virtually any organization.

THE IMPORTANCE OF GOOD PRACTICES

It is also essential to understand that eDiscovery is critical to any business or organization, not just enterprises or organizations that serve "litigious" markets. For example, the survey conducted for this white paper found that across all industries

and organization sizes, there was a median of 2.0 eDiscovery cases per 1,000 employees in the year ending mid-2012; this figure is expected to increase to 2.9 during the next year.

A variety of laws and other requirements, as well as common eDiscovery risks and scenarios, can apply to any business of any size in any industry. Moreover, every organization will have a unique mix of policies, processes, business operations, and technologies that may increase its particular risks in the context of civil litigation.

As a result, an accurate baseline snapshot of eDiscovery and corresponding expenditures today within an organization will help its decision makers to develop, priortize, and justify changes and investments moving forward.

FOCUS ON POLICIES

It is also important to establish data retention and deletion schedules for all content types, a practice that many organizations do not pursue with sufficient urgency. It is important for any organization to retain all of the electronic data that it will need for current and anticipated eDiscovery and other retention requirements. However, many organizations, either by overspecifying the amount of data they must retain and/or not establishing appropriate data deletion policies, retain more information than is necessary, creating greater and unnecessary liability. This can result in much higher eDiscovery costs because more data is retrieved and must be reviewed, as well as unnecessarily high storage costs. It is important for any organization to have its legal team work with IT to conduct a review and ensure compliance with regulatory and statutory requirements. Data classification here is a critical step – decision makers must define what needs to be retained, what can safely be deleted, and the disposition method to be used.

If a legal action is "reasonably anticipated", it is vital that an organization immediately begin to identify and preserve all relevant data. For example, a claim for a breached contract with a contractor might require preservation of emails and other electronic documents between employees and the contractor, as well as between employees talking about the contract or the contractor's performance. A properly configured eDiscovery and data archiving capability will allow organizations to immediately place a hold on data when requested by a court or regulator or on the advice of legal counsel, and retain it for as long as necessary.

Litigants that fail to preserve or hold ESI properly are subject to a wide variety of consequences, including reputational harm, additional costs for third parties to review or search for data, court sanctions, directed verdicts or instructions to a jury that it can view a defendant's or plaintiff's failure to produce data as evidence of culpability.

An adequate legal hold process must include technologies and practices that will enable these holds to be imposed, because relying on individuals to hold data may not be sufficient in many cases. In addition to the *Green v. Blitz* case noted earlier, *Jones v. Bremen High School District*[xxv] is illustrative of the importance of good legal holds:

- The plaintiff filed an Equal Employment Opportunity Commission charge in October 2007[xxvi]. The defendant did not issue a litigation hold, but did instruct three individuals in the District to search through email and save relevant messages. However, destruction of ESI continued and only one year after the case was filed did the District implement automated email archiving. Only in Spring 2009 did the defendant instruct its employees to retain emails that might be relevant to this case.

  The judge in this case did not issue an adverse inference instruction to the jury, but did instruct them that a lack of relevant emails was not evidence that they did not exist. Further, the District had to pay for the cost of court reports when witnesses were deposed about recently created emails, and they had to pay the plaintiff's costs associated with preparing a motion for sanctions.

An adequate legal hold process must include technologies and practices that will enable these holds to be imposed, because relying on individuals to hold data may not be sufficient in many cases.

IMPLEMENT THE RIGHT TECHNOLOGIES

Last, but certainly not least, deploy the storage systems and software tools, services or other capabilities – archiving, storage, predictive coding, etc. – that will enable proactivity in the context of eDiscovery. As discussed above, these capabilities will ensure that all necessary data is accessible and reviewable early in the lifecycle of a case. The right technology will help an organization classify data as it is created and then discover content wherever it exists. These can include, but are not limited to, email servers, file servers, local computers, and other sources like mobile devices. Good tools will also create a complete eDiscovery repository and deduplicate the data. For example, single-instance storage or file/block deduplication applications can reduce the size of some data stores and significantly streamline the entire eDiscovery process.

SPONSOR OF THIS REPORT

Micro Focus is a global software company with 40 years of experience in delivering and supporting enterprise software solutions that help customers innovate faster with lower risk. By applying proven expertise in software and security, we enable customers to utilize new technology solutions while maximizing the value of their investments in critical IT infrastructure and business applications. As a result, they can build, operate, and secure the IT systems that bring together existing business logic and applications with emerging technologies—in essence, bridging the old and the new—to meet their increasingly complex business demands.

www.microfocus.com
twitter.com/MicroFocus

+1 866 464 9282
+1 646 304 6250

---

[i] http://www.emc.com/collateral/about/news/idc-emc-digital-universe-2011-infographic.pdf
[ii] http://www-01.ibm.com/software/data/bigdata/
[iii] http://www.rand.org/content/dam/rand/pubs/monographs/2012/RAND_MG1208.pdf
[iv] http://pdfserver.amlaw.com/legaltechnology/Da_Silva_Moore_v_Publicis_Groupe_11-civ-1279_nysd_complaint.pdf
[v] 636 F.Supp.2d 869 (2009)
[vi] http://www.inboxer.com/downloads/Whitepaper_FRCP.pdf
[vii] 2010 WL 184312 (S.D.N.Y. Jan. 15, 2010)
[viii] http://www.clearwellsystems.com/e-discovery-blog/tag/case-law/
[ix] 2010 U.S. Dist. LEXIS 110496 (E.D. Mo. Oct. 18, 2010)
[x] Source: Kroll Ontrack
[xi] http://blog.x1discovery.com/2011/11/15/facebook-spoliation-costs-lawyer-522000-ends-his-legal-career/
[xii] http://www.readthehook.com/102207/not-over-both-sides-appeal-lester-v-allied-concrete
[xiii] http://civilprocedure.dbllaw.com/2011/08/past-eDiscovery-errors-result-in-sanctions/
[xiv] http://ralphlosey.files.wordpress.com/2011/02/ndlon-v-ice-10-civ-3488-metadata-foia_revised.pdf
[xv] 2007 WL 4287750 (W.D.N.C. Dec. 5, 2007)
[xvi] Source: EDRM (edrm.net)
[xvii] http://www.edrm.net/projects/igrm
[xviii] http://www.edrm.net/projects/igrm
[xix] http://www.depo.com/resources/aa_thediscoveryupdate/authenticating_email.html
[xx] http://www.wwpi.com/index.php?option=com_content&task=view&id=4092&Itemid=44
[xxi] http://www.legaltechnology.com/the-orange-rag-blog/guest-article-the-ediscovery-passport/
[xxii] http://www.justice.gov.uk/courts/procedure-rules/civil/rules/part31#IDAALICC
[xxiii] http://www.clearwellsystems.com/e-discovery-blog/tag/practice-direction/
[xxiv] http://www.mcmillan.ca/Files/ARTICLE_E-Discovery_Around_the_World_0110.pdf
[xxv] Dist. 228, 2010 WL 2106640 (N.D. Ill. May 25, 2010)
[xxvi] http://blog.legalholdpro.com/2010/06/10/northern-district-of-illinois-makes-its-own-way-with-opinion-echoing-need-for strong-legal-holds/