WHITE PAPER

Key Issues for E-Discovery and Legal Compliance

An Osterman Research White Paper

Published March 2017

ARCHIVE360
POINT. CLICK. MIGRATE. STORE.

OSTERMANRESEARCH

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 206 683 5683 • info@ostermanresearch.com
www.ostermanresearch.com • @mosterman

EXECUTIVE SUMMARY

Good electronic discovery (e-discovery) practices and processes, as well as the technologies that enable them, are an essential best practice for any organization because:

- They enable organizations to preserve content, place content on litigation hold, and prevent this information from being deleted prematurely.
- They enable the retention, protection, search and production of relevant content in support of an organization's litigation efforts.
- They minimize risk by significantly reducing the likelihood that a court's or regulator's request for information in the appropriate form and in a given timeframe cannot be satisfied. Without good e-discovery, organizations that are subject to court orders or regulatory obligations to produce information run the significant risk of sanctions, fines or other penalties.
- They enable organizations to index, classify, search for and produce business records and other information for reasons other than an e-discovery order, such as satisfying a regulatory requirement to produce information, enabling managers to perform an early case assessment, or gathering information for a Freedom of Information Act (FOIA) request.

Consequently, pursuing and implementing best practices around e-discovery should be a very high priority for any organization, but for many it is not.

Good electronic discovery (e-discovery) practices and processes, as well as the technologies that enable them, are an essential best practice for any organization.

KEY TAKEAWAYS

- The majority of managers in mid-sized and large organizations are at least somewhat worried that their organizations will be sued at some point, but most constituencies within these organizations are not adequately prepared to deal with e-discovery issues.
- The volume of electronic content that organizations generate, receive and store is growing rapidly. As new content types increasingly become part of the discoverable content that organizations must manage, coupled with the rapid growth in data from "Internet of Things" devices, the rate at which the volume of electronic content increases in the typical organization will accelerate.
- At least 70 percent of organizations can retain, find and produce email that is up to six months old. However, for other content types that are increasingly the subject of e-discovery, this percentage falls off dramatically.
- Most organizations are not adequately prepared to address key requirements included in the Electronic Discovery Reference Model.
- There are a number of best practices that decision makers can implement that will help their organizations to satisfy the growing number of e-discovery requirements and significantly reduce their corporate risk.

ABOUT THIS WHITE PAPER

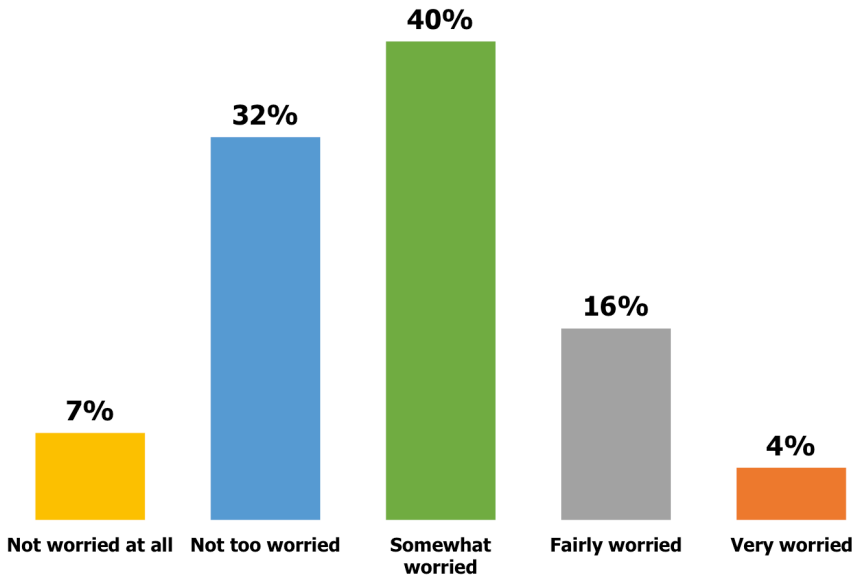
This white paper presents an overview of key e-discovery issues, and presents some of the results from an in-depth survey of decision makers and influencers at mid-sized and large organizations, primarily in North America.

This white paper was sponsored by Archive360 – information about the company is provided at the end of this paper.

WHY FOCUS ON E-DISCOVERY?

E-Discovery and legal compliance are top-of-mind issues for business and IT decision makers for two simple reasons: organizations are frequently involved in litigation, either as defendants or as involved third parties; and most decision makers are worried about the potential for being sued. For example, the research conducted for this white paper found that the organizations surveyed received a mean of 75 e-discovery requests during the past 12 months and more than three in five decision makers are "somewhat", "fairly" or "very" worried about their organization's potential for being sued, as shown in Figure 1. Moreover, we found that 40 percent of organizations anticipate an increase in the number of e-discovery requests they will receive during the next 12 months and 45 percent anticipate no decrease.

Figure 1
Extent to Which Managers are Worried Their Organizations Will be Sued



Source: Osterman Research, Inc.

HOW TO VIEW DISCOVERY

The overall process of "discovery" can be viewed in a couple of different ways:

- As a strict set of legal obligations focused on searching for and producing content that might be relevant for use as evidence during a trial or in pre-litigation activities. Viewed this way, discovery can include the search for and production of any sort of document or other data that might be useful to prove a plaintiff's or defendant's case in a civil action or, in some cases, a criminal action.

- In a broader context, however, "discovery" could be viewed as the ability to search for and produce content not only for court-ordered discovery activities, but as a means of finding information that might somehow be relevant for any sort of litigation- or compliance-related activity. These activities might include senior managers performing an informal early case assessment to determine if a potential lawsuit has merit, mid-level managers searching for content in their employees' email or social media posts that might indicate they are planning to leave a company, a compliance manager satisfying a FOIA request, searching for information about customer in a particular geography, or line-of-business managers looking for social relationships within a company.

WHAT IS DISCOVERY AND E-DISCOVERY?

"E-Discovery", then, is simply the use of well-defined discovery processes to any Electronically Stored Information (ESI) that an organization has available, such as email messages, CRM data, presentations, social media posts, voicemails, word processing files, spreadsheets, and any other relevant communication or information that might be useful in a legal action. E-Discovery can occur on any platform where ESI is stored: desktop computers, laptop computers, file servers, smartphones, tablets, backup tapes, and even employees' home computers and other personally owned devices.

The ability to find, hold and produce information when requested by a court or regulator is a critical responsibility present in one form or another in every jurisdiction. It is also a responsibility that, if not performed adequately, can cost an organization in the form of fines, sanctions, penalties, lost revenue, or higher legal costs. An effective and compliant e-discovery or compliance process is dependent on a well-managed information governance capability, along with clear communication with internal IT departments along with outside third parties like law firms and service providers. The costs and risks of e-discovery and compliance skyrocket when an organization does not have control of their enterprise data and when they cannot find all of the information requested for a legal action within the timeframe allowed by the court. E-Discovery and other legal costs are also impacted by over- or under-collecting data.

ELECTRONIC CONTENT VOLUMES ARE GROWING RAPIDLY

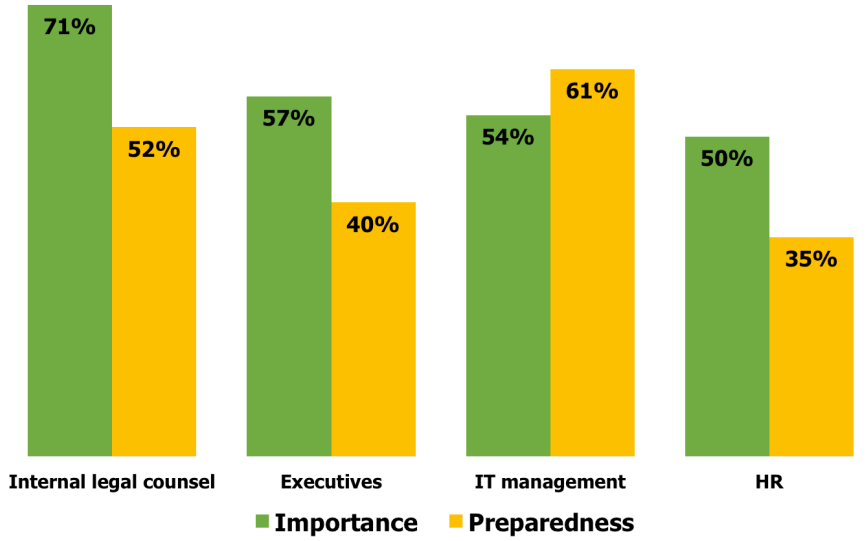
ESI is accumulating rapidly. For example, an Osterman Research survey conducted during 2016 found that organizations store a mean of 49.3 gigabytes of email data per user, and that total messaging-related storage during the previous 12 months had increased a mean of 18 percent. Based on even this relatively modest rate of growth, 49.3 gigabytes per user in 2016 will increase to 133 gigabytes per user by 2022, an increase of 354 percent in just six years. Even small organizations are experiencing rapid growth in their storage of ESI if they are retaining it as they should.

Although email is the most common type of ESI that is called upon for e-discovery and related purposes today, other types of ESI are becoming more relevant and will increasingly be relevant in the context of e-discovery and litigation holds. For example, electronic files stored on file shares and other endpoints, content in SharePoint repositories, social media posts, structured data (e.g., content stored in databases), CRM data, text messages, voicemails and other content types will need to be retained and stored in archiving systems for litigation support purposes.

The research conducted for this white paper found that most of the key groups in an organization, with the exception of IT, are not adequately prepared to deal with e-discovery issues. As shown in Figure 2, only IT management's preparedness meets or exceeds the importance that it places on e-discovery.

Most of the key groups in an organization, with the exception of IT, are not adequately prepared to deal with e-discovery issues.

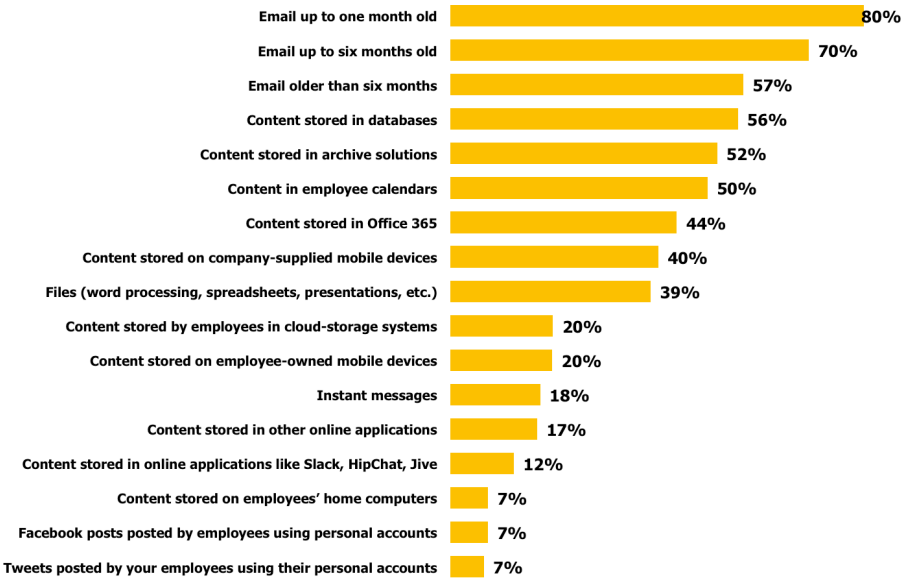
Figure 2
How Various Groups Perceive the Importance of e-discovery and Their Preparedness for It
Percentage Responding "Important" or "Extremely Important"
Percentage Responding "Well Prepared" or "Very Well Prepared"



Source: Osterman Research, Inc.

Part of the reason that many decision makers may perceive that their organizations are underprepared for e-discovery is that they are unable to produce potentially discoverable content. For example, as shown in Figure 3, the vast majority of organizations surveyed can preserve, find and produce email that is up to six months old in response to an e-discovery request. However, for older email and other data types, this ability falls off dramatically.

Figure 3
Preparedness to Retain, Find and Produce Various Content Types
Percentage Responding "Well Prepared" or "Very Well Prepared"



Source: Osterman Research, Inc.

WHAT IS DRIVING THE GROWING IMPORTANCE OF E-DISCOVERY?

There are a number of important drivers for e-discovery, although the importance of the various drivers will depend on an organization's size, the industries in which it participates, the regulatory environment in which it operates, its management tolerance for risk, and other factors.

THE FEDERAL RULES OF CIVIL PROCEDURE

The Federal Rules of Civil Procedure (FRCP), established in 1938, are a set of rules that constitute the basic guidelines for civil litigation in the United States. The FRCP was updated significantly in 2006, most notably to codify the concept of ESI, and again in 2015. The primary impacts of the 2015 changes to the FRCP, among others, are shorter and more limited discovery periods, the requirement for litigants to be better prepared for e-discovery quickly once the litigation process starts, and a requirement for attorneys' readiness to address claims and proportionality issues in the context of e-discovery.

Key changes to the rules in 2015 include the following:

- While the changes to the FRCP in 2006 focused on the *provision* of ESI, the 2015 changes adapt the focus more to *preservation* of ESI. The FRCP now imposes "curative" measures when ESI is lost or absent [FRCP Rule 37(e)(1)], which might make an inability to produce requested content during e-discovery more expensive and consequential.

- The discovery process is now more limited than it was so that the pain it imposes on all parties to litigation can be minimized.

- The parties under the previous FRCP rules could simply object to a request to produce content. However, the new rules require the objecting party to state the specific reasons for any objection and the party "must state whether any responsive materials are being withheld on the basis of that objection".

OBLIGATIONS THAT ALL ORGANIZATIONS MUST SATISFY

Any sound e-discovery strategy should include several elements to ensure that it can satisfy an organization's litigation obligations and to lessen the risk of difficulties during legal actions. While this applies specifically to e-discovery, the general principles involved apply generally to satisfying regulatory obligations, as well:

- **Relevant data must be preserved**
  All organizations must preserve their relevant ESI, even those that are not in heavily regulated industries like financial services, healthcare, energy or life sciences. These records include interactions with clients, purchase orders, contracts, employee records, policy statements and any other content that might be relevant for litigation, regulatory compliance, or simply any best practices that management or legal determines are necessary.

- **Litigation holds are a critical requirement**
  A litigation hold requires an organization to suspend any content deletion processes or practices for relevant data before a legal action commences if it can be reasonably determined that litigation is probable. Because organizations must retain all relevant data for a litigation hold, continuing to delete content can result in serious consequences. Courts have the discretion to impose a variety of sanctions on organizations that fail to implement proper litigation holds, including adverse inference instructions, fines, additional costs for third parties to review or search for data and, in some cases, criminal charges. At a minimum, an organization that deletes data improperly may suffer harm to its corporate reputation.

All organizations must preserve their relevant ESI, even those that are not in heavily regulated industries.

- **Content that can and cannot be accessed must be identified**
  The parties to civil litigation must determine the information that it can and cannot reasonably produce. If an evaluation finds that specific ESI cannot be produced because it is not accessible or would be too expensive to produce, FRCP Rule 26(b)(2)(B) of the FRCP still requires that information about this information must be made available. For example, a party that has potentially relevant data on backup tapes that is in a format that is no longer supported may have to report this fact.

- **Information requests must be addressed quickly**
  FRCP Rule 26(a)(1) obligates litigants to have a good understanding of their data assets. Moreover, they must be able to discuss these issues in advance of the initial pre-trial discovery meeting. FRCP Rule 16(b) requires that this meeting occur within 99 days (sometimes sooner) from the commencement of a legal action, and so all parties should have solid e-discovery capabilities in place prior to litigation.

- **More data types must be managed for e-discovery**
  As noted above, the e-discovery process is becoming more complicated because of the need to produce new data types from a growing number of platforms where that data may be stored. For example, social media content from official, corporate accounts and personal accounts that contain business records that might be relevant during litigation must be produced. Corporate information stored on employee-owned devices must also be produced even though it resides on devices that often are not under direct (or any) corporate control.

E-DISCOVERY REQUIREMENTS AND COMMON MISTAKES

Decision makers would be well advised to learn from court decisions about what they should and should not do with regard to managing the e-discovery process. Here are a few cases that are illustrative of best (and worst) practices:

- **Emails <u>and</u> attachments must be produced**
  In *Skepnek v. Roper & Twardowsky, LLC*[i], the defendant was ordered to produce relevant emails, but did so in PDF format without the attachments that were part of the original emails. The defendants argued that the plaintiffs had never stated in their original request the form of the emails to be produced, but the judge in the case did not agree, stating that "*…defendants were required under Rule 34(b)(2)(E)(ii) either to produce the e-mails and attachments in the form (1) in which they are ordinarily maintained, or (2) 'in a reasonably usable form.' Defendants failed to produce the attachments at all. Defendants also failed to show PDF format is the form in which their e-mails and attachments are ordinarily maintained.*" The judge ordered the production of the missing email attachments.

- **Litigation holds must be implemented promptly**
  In *Stinson v. City of New York*[ii], a case involving an accusation of police officers issuing summonses in violation of five amendments to the US Constitution, a litigation hold was implemented by the City – three years after the initial complaint had been filed. Not only was the litigation hold issued long after it should have been, but the Court determined that it had not been communicated effectively to the relevant parties. Moreover, the New York Police Department allows individual officers to delete email that should be subject to litigation holds, the Court determined that no effort was made to preserve relevant text messages between officers, relevant emails had been deleted, and that "*records were destroyed with a culpable state of mind.*"

- **E-discovery should be specific**
  Parties requesting content should be specific in their requests for information. For example, in the case *Tompkins v. Detroit Metro*[iii], the defendant sought the plaintiff's entire profile on Facebook. The court denied the request, ruling that "*…the Defendant does not have a generalized right to rummage at will through*

information that Plaintiff has limited from public view. Rather, consistent with Rule 26(b) and with the cases cited by both Plaintiff and Defendant, there must be a threshold showing that the requested information is reasonably calculated to lead to the discovery of admissible evidence."

In contrast, the requesting party in *Wilkinson v. Greater Dayton Regional Transit Authority*[iv] asked for "*[A]ny notes, diaries, logs, journals, letters, electronic mail, text messages, calendars, Facebook postings, tweets, or other social media messages that relate or refer to your employment with the GDRTA, your alleged serious health condition, or your activities on days when you requested FMLA leave.*" In this case, the Court granted the request because it defined specific information that was relevant to the case.

- **Backups are generally not appropriate for e-discovery**
  Backups are a poor method for preserving discoverable content because the search and production of relevant content from backups is much more time-consuming and expensive than when using an archiving system, and it may not produce all of the necessary information. In the case of *Johnson v. Neiman*[v], the defendant argued that it should not be required 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 needed for the creation of .PST files. Further, the defendant argued that this data was not reasonably accessible, a position with which the Court ultimately agreed and did not require production of the data, luckily for the defendant.

  In short, an appropriate archiving capability can make the search for data during early case assessments, e-discovery, regulatory audits, or even informal searches dramatically easier than if this content is stored on backup tapes.

Backups are a poor method for preserving discoverable content.

- **Coming to an agreement about discoverable content is essential**
  In *Digicel v. Cable & Wireless PLC*, the defendant decided not to search through their backup tapes without first consulting the plaintiff. Further, the defendant defined the search terms it would use despite the fact that the plaintiffs did not agree with them. The Court overruled the defendant's decision and ordered it to restore employee emails that were stored on backup tapes, as well as add additional search terms.[vi]

- **Only appropriate material should be used**
  Many employers use social media from prospective employees in the recruiting and candidate evaluation process. However, there are limits about the types of content that they can evaluate. For example, an employer must not consider a candidate's race, religion, sexuality or certain other types of information. If an employer uses social media as part of the candidate evaluation process, it should archive the content it used about candidates so that it can demonstrate it did not evaluate material that should not be considered. A failure to do so – and an employer's failure to demonstrate its good faith evaluation of this information during e-discovery – could result in damaging consequences. Relevant regulations in this regard include the Americans with Disabilities Act, the Age Discrimination in Employment Act, the Civil Rights Act of 1964 and Executive Order. No. 11,246[vii].

NON-LEGAL DRIVERS FOR E-DISCOVERY

While e-discovery is most often associated with satisfying specific legal obligations, such as court orders to produce ESI, there are a number of applications for e-discovery outside the context of litigation. For example:

- The European Union's (EU) General Data Protection Regulation (GDPR) is applicable to almost every organization around the world that collects or processes data on residents within the EU, including permanent residents, visitors and expatriates. Compliance is thus predicated on the geographical

location of the individuals about whom an organization holds personal data, not the domicile of registration for the organization. An organization that violates the provisions of the GDPR, which goes into effect in May 2018, may be subject to a fine of up to €20 million or four percent of their annual revenue.

- Strict regulatory obligations to search for and produce information exist in a wide range of industries. For example:
    - Financial services firms governed by the Financial Industry Regulatory Authority (FINRA) must preserve various types of information and perform supervision of broker-dealers and certain others to ensure that these individuals' communications are in compliance with Securities and Exchange Commission (SEC) requirements.
    - Insurance providers are subject to a range of regulations, including the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), and the Health Information Technology Act (HITECH), among other federal and state requirements. These regulations impose a variety of obligations on insurance companies, including records preservation, auditing and immutability of content.
    - Healthcare providers must satisfy a growing array of obligations, including HIPAA's Privacy and Security Rules and HITECH, requiring them to preserve and produce information of various types.
    - Energy providers subject to Federal Energy Regulatory Commission (FERC) rules must preserve and periodically produce information of various types, such as email, instant messages, CRM systems, and Voice-over-IP systems.
    - Most government agencies are subject to FOIA, open-records or "sunshine" laws that obligate them to search for and produce information they possess in response to requests from press organizations, individuals or other government agencies.
- As discussed elsewhere in this report, managers, legal teams and others should perform early case assessments to determine their organization's position before litigation begins or when litigation is even remotely suspected.
- Of growing importance is the need for decision makers to understand what actually takes place in an organization through unofficial or informal channels, what may be called internal investigations. For example, the ability to search for information that will enable decision makers to find abusive managers, employees who are contemplating leaving the company, or individuals who are sending content to competitors can be useful in discovering and remediating problems as early as possible.

The same e-discovery capabilities that can help an organization to satisfy a court order can be useful in helping decision makers to address all of the non-legal use cases identified above.

HOW WILL E-DISCOVERY CHANGE OVER THE NEXT FEW YEARS?

One of the more fundamental changes in the e-discovery market will be the sheer volume of the market and its substantial rate of growth. For example, IDC noted that the combined e-discovery services and software market is now in excess of $10 billion worldwide and will grow at nearly 10 percent per year through 2019[viii]. Zion Market Research has an even more aggressive forecast, predicting that the worldwide e-discovery market will grow at the rate of nearly 16 percent per year between 2016 and 2021, to $18.5 billion by 2021[ix].

Another fundamental change in e-discovery, as noted earlier, will be the expansion of the practice and process of e-discovery to virtually all types of ESI. While many firms today are not yet even archiving email – the most commonly discoverable electronic content in litigation – they will be required to archive, search for and produce a wide range of data types, including text messages, social media posts, files, data in collaboration tools, voicemails and other information. In short, any electronic information that contains a business record, regardless of the tool that was used to create it or the venue in which it is stored, will potentially be subject to e-discovery. The amendments to the FRCP in 2006 and 2015 have, for all intents and purposes, made anything from any source potentially subject to e-discovery.

As a corollary to the point above, data generated by Internet of Things (IoT) devices will increasingly be subject to e-discovery. For example, content from an Alexa-enabled Amazon Echo device has been sought in a 2015 murder investigation[x]. At least five US states now use data from automobiles' vehicle event data recorders to determine the speed at which cars were traveling when they were involved in an accident[xi]. Vendors of communication and collaboration solutions are increasingly integrating their solutions with tools like Alexa, Apple's Siri, Microsoft's Cortana and Google's Assistant. As the proportion of electronic content shifts primarily from documents created by humans to data generated by things, we anticipate a growing proportion of discoverable content will come from the latter.

Another important trend will be the use of machine-learning assistants, such as IBM Watson, in conjunction with visual analytics to assist in the e-discovery process. For example, as noted by David Horrigan of kCura[xii], email threading in conjunction with analytics visualization will help paralegals and attorneys to dramatically reduce the time required to review email content in their effort to discover the most relevant content.

Another fundamental change in e-discovery… will be the expansion of the practice and process of e-discovery to virtually all types of ESI.

Finally, the cloud will have a significant impact on e-discovery in two ways:

- First, a growing proportion of discoverable content will be stored in the cloud, such as in Microsoft OneDrive and SharePoint repositories for the growing number of Microsoft Office 365 customers; in the Google Cloud for customers of G Suite; in the myriad other cloud-based communications and collaboration tools that are replacing on-premises solutions; and in cloud-based archiving and storage systems that are replacing on-premises solutions. While Office 365 and G Suite are widely used, there are hundreds of other communication and collaboration tools that contain information subject to e-discovery – decision makers must focus on the entirety of their cloud-based information stores for purposes of e-discovery.

  Moreover, e-discovery capabilities will need to adapt not only to the shift in venues where data may be found, but also to any limitations that may be imposed by the cloud on e-discovery efforts, such as the speed of search from cloud-based data repositories that are accessed from Internet connections that may not always be adequate to the task at hand.

- Second, there are a growing number of cloud-only vendors that offers e-discovery, archiving and other capabilities. These solutions have the potential for changing e-discovery practices by enabling easier access to discoverable information by a larger number of parties.

It is important to note, however, that organizations continue to bear the complete responsibility for their compliance, e-discovery and related obligations for their data even when stored in the cloud, despite whatever compliance capabilities a cloud provider might offer. Information owners that store content in the cloud are not absolved of their responsibilities with regard to storing data securely, applying litigation holds when necessary, or satisfying their e-discovery or regulatory compliance obligations simply because their data is stored with a third party.

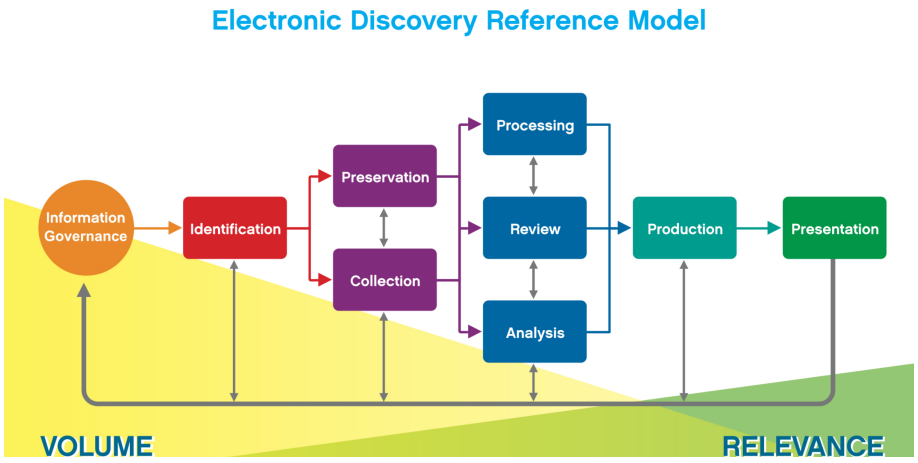
IMPORTANT E-DISCOVERY ISSUES AND THEIR IMPACT

THE ELECTRONIC DISCOVERY REFERENCE MODEL (EDRM)

Placed into the public domain in May 2006, the Electronic Discovery Reference Model (EDRM) was developed as a response to the relatively few standards and lack of generally accepted guidelines for the process of e-discovery that was the norm prior to its development. George Socha (Socha Consulting LLC) and Tom Gelbmann (Gelbmann & Associates) facilitated the team that developed the EDRM, which included 62 organizations, among which were law firms, software developers, consulting firms, professional organizations and large corporations.

The EDRM Model is shown in Figure 4.

Figure 4
Electronic Discovery Reference Model[xiii]



Source: Electronic Discovery Reference Model, ©2014, v3.0, edrm.net

The EDRM is important because it represents a useful tool for the standardization of the e-discovery process. Because of the growth in the quantity of ESI, the growing number of data types subject to e-discovery, and the large number of entities that need to process data during the normal course of e-discovery, standardization in the process is essential.

There are nine sections in the EDRM that focus on the process of managing an entire e-discovery effort:

- **Information Governance**
  This section focuses on managing electronic content in such a way that an organization can prepare for e-discovery if it should become necessary. The goal of information governance, which includes preservation of ESI, is to minimize the risk and cost associated with the entire process of e-discovery. Managed properly, this step can dramatically reduce the effort required in the subsequent phases of the EDRM process.

- **Identification**
  Understanding the ESI that might be relevant in a particular case and that might have to be presented during discovery is critical. At this point in the process, discovery demands, disclosure obligations and other relevant claims and demands are reviewed and considered. The goal is to understand the totality of information that might be required in order to respond to appropriate e-discovery

requests and then determine the subset of information that will be relevant for further processing. Archiving solutions are an essential tool in this process as the primary enabler of proper data retention.

- **Preservation**
  Preservation is an essential step that ensures that ESI is protected from spoliation and modification, such as through the imposition and enforcement of a litigation hold on all relevant ESI. If spoliation occurs, the consequences can be damaging. For example, in the case of *Hart v. Dillon*[xiv], the plaintiff was terminated by the defendant and a recording of a secret interview with the former was used as part of the grounds for her dismissal from the company. However, the defendant failed to preserve the recording after the litigation hold went into effect, resulting in the Court's decision to set a hearing to determine sanctions to be levied against the defendant.

- **Collection**
  All relevant ESI must be collected from the various sources that contain it, such as email archives, desktops, laptops, backup tapes, file servers, employees' home computers, smartphones and other sources.

- **Processing**
  Collected data is then indexed and, thus, made searchable. The data should also be de-duplicated so that the amount of data can be reduced to make review during subsequent phases of the discovery process more efficient and less expensive. 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 format that will permit the most efficient and thorough review of its contents.

- **Review**
  This phase includes evaluating the content for its relevance, determining if specific items are subject to attorney-client privilege, and redacting ESI as appropriate, among other activities.

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

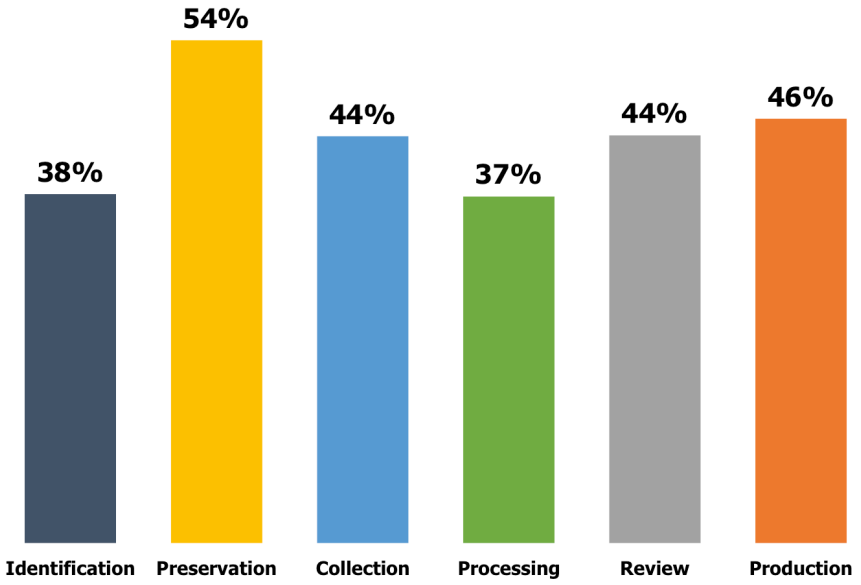
- **Production**
  The phase involves delivering the relevant ESI to any parties or systems that will need it. It also includes the activities focused on delivering ESI in the appropriate formats (e.g., in native or image format) and form(s), including DVDs, CD-ROMs, paper, etc.

- **Presentation**
  The presentation of ESI is an important consideration at various points of the e-discovery 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 research conducted for this white paper asked about six key elements of the EDRM model in the context of how well prepared organizations are to satisfy them. We found that most organizations simply are not adequately prepared to deal with these issues, as shown in Figure 5.

Preservation is an essential step that ensures that ESI is protected from spoliation and modification.

Figure 5
Ability to Satisfy Key Elements of the E-Discovery Process
Percentage of Organizations That Nearly Have or Have Everything in Place



Source: Osterman Research, Inc.

FEDERAL RULES OF EVIDENCE

Put into place in 1975, the Federal Rules of Evidence (FRE) are a set of requirements that focus on evidence presentation during trial in the US federal courts. Individual US states may employ these rules as the basis for their own rules of evidence, or they can implement a different set of requirements for presenting evidence during trial. 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 component of the e-discovery process because it is focused on demonstrating that a document is what its presenter claims it to be – an actual and verifiable representation of an electronic document. However, authentication for electronic content is more critical than for paper documents because ESI is more easily altered. For example, the process of copying data from one location to another can alter metadata and can call into question its authenticity. When the authenticity of evidence is challenged, this can create a number of problems and can add to the expense of a legal action. For reference, Atkinson-Baker has developed a good overview of the authentication requirements for electronic records[xv].

STATE REQUIREMENTS

There are a number of changes occurring at the state level that are placing more focus on e-discovery, proper management of ESI, and improved education around technology-related issues in the context of discovery. As just a couple of examples:

- Florida is the first state that requires technology-focused Continuing Legal Education (CLE) credit hours for attorneys. The Supreme Court of Florida and the Florida Bar Association in late 2016 amended their CLE requirements "to change the required number of continuing legal education credit hours over a three-year period from 30 to 33, with three hours in an approved technology program."

- In June 2015, the US District Court for the District of Colorado published *Checklist for Rule 26(f) Meet-and-Confer Regarding Electronically Stored Information (ESI)* and Guidelines Addressing the Discovery of Electronically

Stored Information to update attorneys' understanding of ESI and related matters.

LAWS OUTSIDE OF NORTH AMERICA

E-discovery practices in the United States are arguably more advanced and requirements more specific than in other nations because of the more litigious nature of US society relative to other countries. This is evidenced by the relatively large number of attorneys per capita in the United States: for example, the United States has 265 residents per attorney compared to the United Kingdom with 401[xvi].

E-discovery (often referred to as "e-disclosure" outside of the United States) in US legal proceedings can be onerous and expensive, but requirements in other parts of the world can present their own challenges. For example:

- English and Welsh courts can require standard disclosure – namely, the disclosure that a document "exists or has existed". The recipient of the disclosure has a right to inspection of the content, but subject to a variety of restrictions[xvii]. However, in April 2013 the UK Civil Procedure Rule 31.5 went into effect, permitting courts more latitude when ordering disclosure. Some of the rules in England and Wales 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[xviii].

- Litigants in most European nations are not required to produce content that runs counter to the claims they make in a legal action. Obligations in the UK, however, can compel organizations to produce damaging content, but only after a court order[xix].

- In 2010, Ontario amended its rules of civil procedure so that it could accommodate the growth of electronic information 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."

- In Practice Note No. 1 of 2007 (February 2007), Australia's Supreme Court of Victoria strongly suggested that the parties to a legal action should consider using technology to improve the efficiency of legal proceedings, including e-discovery tools. The Federal Court of Australia has developed e-discovery rules similar to those contained in the 2006 amendments to the FRCP. Further, in 2009 the Australian Federal Court ruled that all cases meeting minimum requirements must be managed only with digital content and not via paper documents.

- Various statutes designed to block discovery proceedings have been in place for many years in a number of countries. These statutes exist in Federal Canada (Business Records Protection Act), Ontario, the United Kingdom (The Shipping and Commercial Documents Act) and the Netherlands (Economic Competition Act). The key issue with regard to blocking statutes is that even though data has been found, it may not necessarily be usable.

E-discovery in US legal proceedings can be onerous and expensive, but require-ments in other parts of the world can present their own challenges.

OTHER ISSUES TO CONSIDER

In order to minimize the cost and improve the efficiency of e-discovery, there are three basic principles that decision makers should follow:

- **Retain only what is necessary and only for as long as necessary**
  Organizations should capture information at the right point, classify it for retention, and store each form of data in a tamper-proof archive, in a search-ready state, for as long as necessary. When records can be safely deleted, the deletion process should occur quickly with a carefully prescribed plan for "defensible deletion". Employees should be trained to know what they should

and should not do to remain in compliance, and should follow the policies, procedures, and system requirements correctly.

- **Rapidly identify suspect or non-compliant content**
  The organization should be able to demonstrate appropriate actions that have been to address this type of content. This should be performed in a proactive sense to minimize downstream harm, or in response to a request for information from an external body.

- **Manage content with the goal of minimizing risk**
  Organizations should employ systems, policies, and training to minimize the legal compliance risks they face, such as inaccurate identification of content for retention, systematic failures to delete appropriate content, and insufficient care by employees in following corporate policies. Increasingly, analytics capabilities are being applied to archived content in order to identify information that could pose security, compliance or legal risks. These capabilities can proactively surface content that might put the organization at risk, and to enable the organization to address any problems before they become significant.

BEST PRACTICES AND RECOMMENDATIONS

Osterman Research recommends a number of best practices, and offers some useful recommendations, for organizations that are either planning their e-discovery strategy or that wish to fine-tune their current processes:

ESTABLISH A MEET-AND-GREET

It is essential to start with a "meet-and-greet" among the relevant internal parties, among them senior IT management, key legal decision makers, executives and all other relevant individuals and teams inside and outside of an organization. In many organizations, internal legal teams do not have in place the processes and visibility to track e-discovery tasks, so these teams need to reassess their relationships and protocols with other teams.

Key questions to ask include:

- Do your organization's CIO and IT managers know the name of your organization's chief legal counsel and/or external legal counsel?

- Does legal counsel know who the IT decision makers are in the context of archiving or e-discovery technologies?

- Are the IT and legal stakeholders aware of who else would potentially be involved in e-discovery planning?

The establishment of this "legal-IT handshake" is a key step in developing an effective e-discovery strategy. If each group understands the key requirements of the other groups, it will go a long way toward developing an effective e-discovery plan.

FOCUS ON EMPLOYEE INVOLVEMENT

Policies, practices, procedures and technologies are essential components of a robust e-discovery strategy. However, it is important to provide adequate education for all employees, consultants and others about the critical importance of retaining important content, using corporate communication and collaboration resources in accordance with corporate policies, taking care not to delete important documents, and the like. Using employees as the initial line of defense can significantly improve e-discovery significantly and reduce the likelihood of evidence spoliation and violation of litigation holds.

IMPLEMENT ARCHIVING, NOT BACKUP FOR E-DISCOVERY

Litigation is clearly more efficient if the right solutions are in place for e-discovery and litigation hold. This begins with good archiving technology that will capture, index and retain business records for the appropriate length of time, ensure that these records cannot be deleted or modified after the fact, and that will enable the archives to be searched quickly, efficiently and at scale. E-discovery tools will help define content that is and is not available, and make the entire process much more efficient. Archive search capabilities are often the front line for e-discovery requests – these solutions enable IT and legal teams to initiate searches directly from the archive and ingest this content directly into e-discovery tools. Surprisingly, many organizations still rely on backup tapes as their litigation "archive", a role that backups were never intended to fulfill and one at which they fail miserably.

It is essential to acknowledge that backups and archives are not interchangeable. While both are important best practices for any organization to follow, backups are designed for tactical, short-term preservation of content in order to restore servers after a crash or system fault; while archives are strategic tools designed to preserve information for long periods.

There are a number of problems associated with using backups as an archive, including the fact that backups constitute unprocessed content and lack any sort of indexing. Moreover, the integrity of backup tapes is not guaranteed, and because backups capture a snapshot of data, information generated and deleted between backups will not be captured. Moreover, searching through backup tapes for e-discovery purposes can be extremely expensive. For example, in the case of *Radian Asset Assurance, Inc. v. College of the Christian Brothers of New Mexico*[xx], the defendant estimated that the cost to search through 50.5 backup tapes would be $420,315, or an average of $8,323 per tape.

DEPLOY THE RIGHT E-DISCOVERY TOOLS

While archiving is essential to deal with much of the left side of the EDRM model, other tools are necessary to deal with the right side of the model for purposes of reducing the cost of these processes and to make them more efficient. According to the RAND Institute for Civil Justice in their report[xxi] entitled *Where the Money Goes*, the document review process constitutes more than 70 percent of e-discovery costs. This is important when discussing e-discovery in the context of overall information governance (or the lack of it), since organizations create, receive and stockpile so much digital data that the amount of reviewable content for even a single lawsuit can easily reach into the millions or billions of pages of reviewable content.) A respected US Magistrate, Judge Andrew J. Peck, stated in a video interview on February 4, 2013:

"Part of the reason e-discovery is so expensive is because companies have so much data that serves no business need. Companies are going to realize that it's important to get their information governance under control to get rid of all the data that has no business need…in ways that will improve the company's bottom line…."

Decision makers should evaluate and implement new technologies that can enable legal teams to learn more about the cases presented to them and to do so sooner in the litigation process. For example, in-place preservation/search tools can empower legal teams to search for data without actually collecting it, enabling them to make decisions earlier in the litigation process. Legal project management tools are important to better manage the multiple technologies and teams involved so as to create a uniform, consistent and repeatable process that will ensure defensibility and greater efficiency in the e-discovery process. Predictive coding, which employs machine-learning technologies, can analyze data sources and help to cull data during e-discovery. Advanced sampling capabilities can significantly reduce the amount of content presented for review, thereby making e-discovery more efficient and less expensive.

…the document review process constitutes more than 70 percent of e-discovery costs.

Moreover, legal and other teams can implement various processes that will drive down the cost of e-discovery, such as targeted collections, non-forensic collections, and early case assessments that will enable legal teams to identify potentially responsive data before it is collected.

In short, appropriate e-discovery tools that help organizations deal with the complete EDRM model are essential.

BECOME PROACTIVE, NOT REACTIVE

It is essential for decision makers to acknowledge the importance of e-discovery in the context of all of the information it manages and to give it the appropriate priority for budgeting, staffing and planning purposes. E-discovery for email is a relatively high priority for the majority of decision makers, but e-discovery for other content is not viewed as importantly. E-discovery must be a high priority for all managers within an organization and should be a key consideration for employees who are charged with creating, storing and managing information. As a growing proportion of business records become discoverable, decision makers will need to implement capabilities to capture this information for long-term retention and retrieval. For example:

- As part of good e-discovery practices, early case assessments and the tools to support them will help decision makers understand an organization's legal position early in the litigation process, potentially saving it the cost of going to trial or pursuing a case for too long a period.

- Doing more work in the preservation, identification and processing stages can reduce the amount of data sent to review, which can substantially reduce the amount spent on e-discovery activities. Moreover, this can enable legal teams to ascertain the facts of a case more quickly, a very important benefit.

- Good e-discovery helps decision makers to understand if compliance with corporate policies is taking place and helps them adjust these policies over time.

- Good e-discovery minimizes the amount of time required for information to be recovered in order to make the process more efficient.

- Finally, good e-discovery helps decision makers to make better-informed decisions and so can minimize the risk of legal actions, legal costs and disruption to normal business processes.

REDUCE THE COSTS OF EMAIL AND BUSINESS MANAGEMENT

Good e-discovery tools and processes can reduce the cost of content and business management by streamlining the litigation support processes involved in e-discovery. This will result in hard cost savings by reducing the amount of internal staff time that must be devoted to e-discovery, reducing external legal counsel expenses, and reducing the risk of damaging consequences like adverse inference instructions or sanctions.

IMPLEMENT LITIGATION HOLDS PROPERLY

Litigation that is "reasonably anticipated" [FRCP Rule 37(e)] requires identification and retention of all data that might be considered relevant for the duration of the litigation. For example, a claim for a breached contract with a contractor might require retention 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 e-discovery and data archiving capability will enable organizations to immediately place a hold on data when requested by a court or regulator or on the advice of legal counsel, suspend deletion policies and practices, and retain it for as long as necessary. One element of the litigation hold process that is commonly missed, and that creates spoliation concerns, is not tracking employee movements and protecting data on litigation hold from being

accidentally deleted when an employee departs, changes roles, or when computers are automatically wiped by IT.

Parties to litigation that do not preserve or hold ESI adequately are subject to a variety of consequences. These might include harm to the organization's reputation, added costs for third parties to review or search for data, court fines or other sanctions, directed verdicts or adverse inference instructions.

ESTABLISH KEY BEST PRACTICES

Establishing data retention and deletion schedules is essential for all content types, a practice that many organizations do not pursue with sufficient urgency if they address this issue at all. It is important for any organization to retain all of the ESI that it will need for current and anticipated e-discovery and other retention requirements, including data types like social media, text messages, voicemails, files and other data that it might never have considered capturing. Specifically, key best practices should include establishing data retention schedules for various types of content and continually monitoring and updating these schedules based on changes in the law and recent court decisions.

DEPLOY THE APPROPRIATE SOLUTIONS

It is essential to deploy the appropriate capabilities – archiving, storage, predictive coding, etc. – that will enable an organization to fully satisfy its e-discovery obligations. These capabilities will ensure that all necessary data is accessible and reviewable early in a legal case. An adequate technology platform will help an organization to classify data as it is created and then discover content wherever it exists, regardless of location or platform. The e-discovery technologies implemented should ensure that all required data is accessible, that data can be properly classified as it is created, that it can be discovered on every platform on which it exists, and that the data can be deduplicated to streamline the e-discovery process.

UNDERSTAND CHANGES THE CLOUD AFFORDS e-discovery

Finally, it is important to understand how the cloud affords changes in current e-discovery processes. Many organizations are replacing legacy, on-premises storage solutions with lower cost cloud storage, such as Amazon Web Services, Microsoft Azure or Google Cloud. A growing number of cloud-based archiving solutions offer performance that rivals or is better than on-premises solutions in terms of search performance and content extraction. There is a growing number of other e-discovery capabilities offered either with a cloud component or as cloud-only capabilities. In short, the cloud will figure prominently into future e-discovery and should be seriously considered by any decision maker focused on improving e-discovery practices.

…it is important to understand how the cloud affords changes in current e-discovery processes.

SUMMARY

E-discovery is an essential set of best practices and technology choices that will enable organizations to retain business information, search this information quickly and efficiently, produce the required content, and prevent the spoliation of information that should be retained. While good e-discovery capabilities have always been important, they are becoming more so because of the increasing volume of ESI that organizations possess, changing legal requirements to preserve information, and the increasing level of risk that can result from a failure to retain and produce information adequately.

SPONSOR OF THIS PAPER

Archive360 is the market leader in email archive migration software, successfully migrating more than 12 petabytes of data for more than 500 organizations worldwide since 2012. The company's flagship product, Archive2Anywhere™, is the only solution in the market purpose-built to deliver consistently fast, trouble-free, predictable archive migrations, with verifiable data fidelity and defensible chain of custody reporting. Archive360's newly released Archive2Azure solution is the industry's first regulatory compliance and grey data storage solution based on the Microsoft Azure platform. Archive360 is a global organization that delivers its solutions both directly and through a worldwide network of partners. Archive360 is a Microsoft Cloud Solution Provider and the Archive2Azure solution is Microsoft Azure Certified.

ARCHIVE360
POINT. CLICK. MIGRATE. STORE.

www.archive360.com

@Archive360

+1 212 731-2438

info@archive360.com

REFERENCES

[i] *Skepnek v. Roper & Twardowsky, LLC,* 2014 U.S. Dist. LEXIS 11894, at *3-4 (D. Kan. Jan. 27, 2014)
[ii] *Stinson v. City of New York* (S.D.N.Y. Jan. 2, 2016) 2016 U.S. Dist. LEXIS 868, at *1
[iii] *Tompkins v. Detroit Metro. Airport,* 278 F.R.D. 387 (E.D. Mich. 2012)
[iv] *Wilkinson v. Greater Dayton Reg'l Transit Auth.,* 2014 U.S. Dist. LEXIS 64522, 9 (S.D. Ohio May 9, 2014)
[v] 2010 U.S. Dist. LEXIS 110496 (E.D. Mo. Oct. 18, 2010)
[vi] Source: Kroll Ontrack
[vii] http://archivesocial.com/blog/social-media-recruitment/
[viii] http://www.businesswire.com/news/home/20160104005438/en/IDC-Forecast-Shows-Worldwide-e-discovery-Market-Surpasses
[ix] https://globenewswire.com/news-release/2016/11/23/892343/0/en/Global-e-discovery-Market-Size-will-reach-USD-18-49-Billion-by-2021-Zion-Market-Research.html
[x] http://blog.kcura.com/relativity/blog/murder-data-privacy-and-the-internet-of-things
[xi] http://www.mcall.com/mc-car-black-box-data-can-be-used-as-evidence-story.html
[xii] http://blog.kcura.com/relativity/blog/e-discovery-in-2017-back-to-the-future
[xiii] Source: EDRM (edrm.net)
[xiv] *Hart v. Dillon Cos.,* 2013 U.S. Dist. LEXIS 95441, 1-5 (D. Colo. 2013)
[xv] http://www.depo.com/resources/aa_the-discoveryupdate/authenticating_email.html
[xvi] http://wiki.answers.com/Q/What_country_in_the_world_has_most_lawyers_per_capita
[xvii] http://www.justice.gov.uk/courts/procedure-rules/civil/rules/part31#IDAALICC
[xviii] http://www.clearwellsystems.com/e-discovery-blog/tag/practice-direction/
[xix] http://www.legaltechnology.com/the-orange-rag-blog/guest-article-the-e-discovery-passport/
[xx] 2010 WL 4928866 (D.N.M.)
[xxi] RAND Institute for Civil Justice Report "Where the Money Goes"