WHITE PAPER

Why eDiscovery Should be a Top Priority for Your Organization

An Osterman Research White Paper

Published October 2013

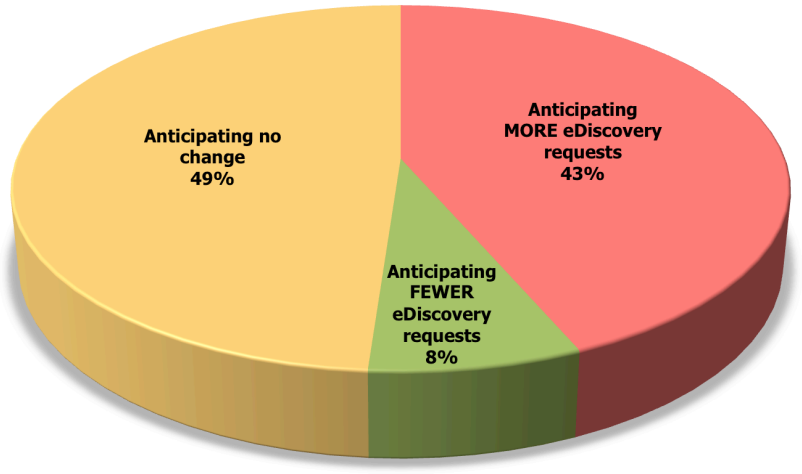
Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 253 630 5839 • Fax: +1 253 458 0934 • info@ostermanresearch.com
www.ostermanresearch.com • twitter.com/mosterman

EXECUTIVE SUMMARY

eDiscovery is a critical process that occurs early in civil litigation matters and involves the exchange of information between parties involved in a lawsuit or some other legal action. eDiscovery has implications for a variety of activities, including the archival of electronic information, the ability to search for relevant content, the ability to modify content deletion policies, how storage systems are managed, how corporate policies are developed and risk management.

The importance of eDiscovery should not be underestimated: it is among the primary drivers for the deployment of archiving systems and has significant implications for how organizations retain, store and manage their electronic content. A failure to manage eDiscovery properly can carry with it serious ramifications. Moreover, the problem of eDiscovery is expected to become more serious as evidenced by the growing number of eDiscovery requests that are anticipated over the next 12 months.

Figure 1
Anticipated Change in the Number of eDiscovery Requests
September 2013 to September 2014



KEY TAKEAWAYS

There are three important issues that decision makers should consider:

- eDiscovery is an important issue and is becoming more serious over time, but most corporate decision makers believe they are not as well prepared for it as they should be.
- Most organizations have at least partially addressed eDiscovery issues focused on email, but a growing number of data types and venues are complicating the problems of eDiscovery and content management in general.
- eDiscovery rules and requirements continue to evolve and are placing additional demands on decision makers to manage eDiscovery properly.

ABOUT THIS WHITE PAPER

This white paper includes data from a survey conducted by Osterman Research specifically for this white paper during September 2013, as well as other Osterman Research survey data generated during 2013. This white paper was sponsored by HP Autonomy - relevant information about the company and its offerings are provided at the end of this document.

The importance of eDiscovery should not be underestimated: it is among the primary drivers for the deployment of archiving systems and has significant implications for how organizations retain, store and manage their electronic content.

WHAT IS CHANGING IN eDISCOVERY?

DISCOVERY AND eDISCOVERY DEFINED

Discovery can be viewed in a couple of ways: first, as a relatively strict set of requirements focused on searching for content that may be relevant for use as evidence in a trial or in pre-litigation activities. Viewed in this way, it can include any sort of document or other information that might be useful to prove a plaintiff's or defendant's case in a civil action. Viewed more broadly, however, discovery can be considered the ability to search for content not only within the relatively strict confines of court-ordered discovery activities, but also all of the efforts focused on finding content that might somehow be relevant in the context of any litigation-related activity, such as senior managers performing informal early case assessments or departmental managers searching for potentially damaging content in their employee's communication or collaboration streams.

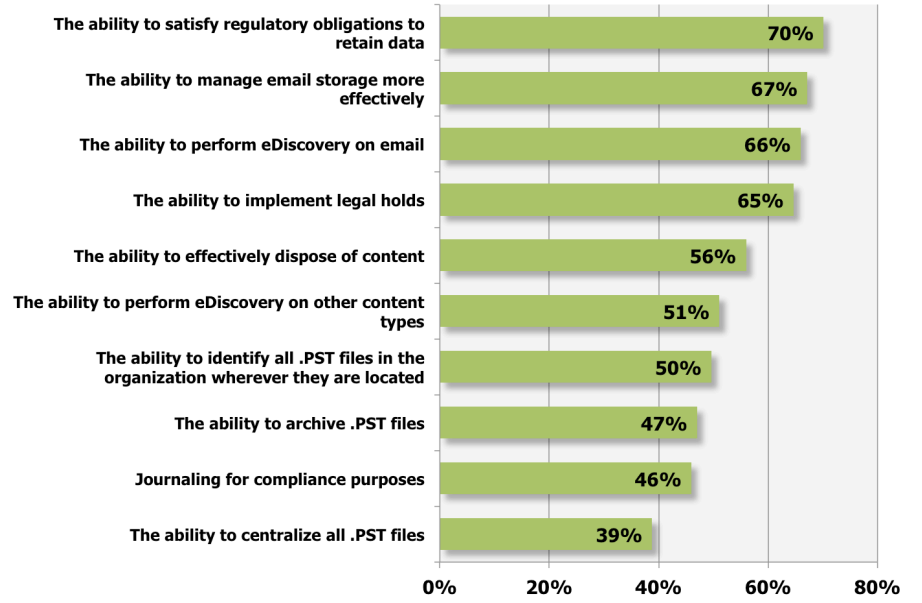
"eDiscovery" is merely the extension of the well-established discovery process to any Electronically Stored Information (ESI) that an organization might possess – email messages, voicemails, presentations, word processing files, spreadsheets, tweets, Facebook posts and all other relevant communication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

AN ESSENTIAL ACTIVITY

eDiscovery is an essential element of any organization's information management strategy because of the significant implications that can result from poor eDiscovery. This is a reality that has not been lost on organizational decision makers – as shown in the following figure, the ability to perform eDiscovery on email is nearly as important as the ability to satisfy regulatory data retention obligations and the ability to manage email storage more effectively. Moreover, the ability to perform eDiscovery on other content types, such as social media (whether public tools like Facebook or Twitter, or enterprise focused) and files, is also viewed as highly important by a significant proportion of organizational decision makers.

eDiscovery is an essential element of any organization's information management strategy.

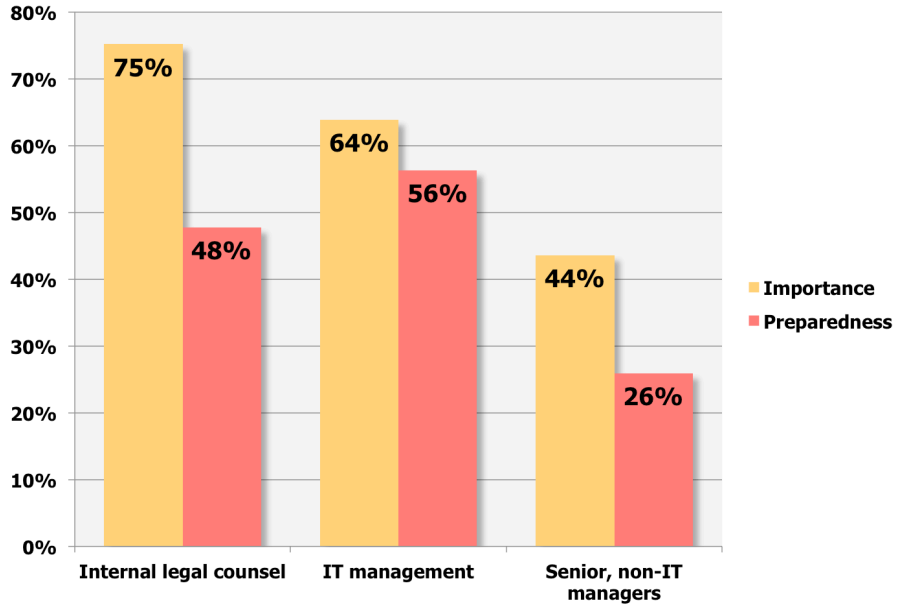
Figure 2
Importance of Key Information Management Capabilities
% Responding Important or Extremely Important



IMPORTANCE AND READINESS ARE AT ODDS

In contrast to the perceived *importance* of eDiscovery is the relative lack of *preparedness* for it that our research found among various groups. For example, as shown in the following figure, internal legal counsel perceives eDiscovery to be of significant importance – 75% of legal counsel believes that it is important or extremely important – but a much smaller proportion of internal legal counsel considers themselves to be well prepared or very well prepared to manage eDiscovery. While we find a similar disparity between senior, non-IT managers, IT management has the smallest disparity between the importance it places on eDiscovery and its preparedness for it.

Figure 3
Importance of and Preparedness for eDiscovery by Various Groups
% Responding Important or Extremely Important
% Responding Well Prepared or Very Well Prepared

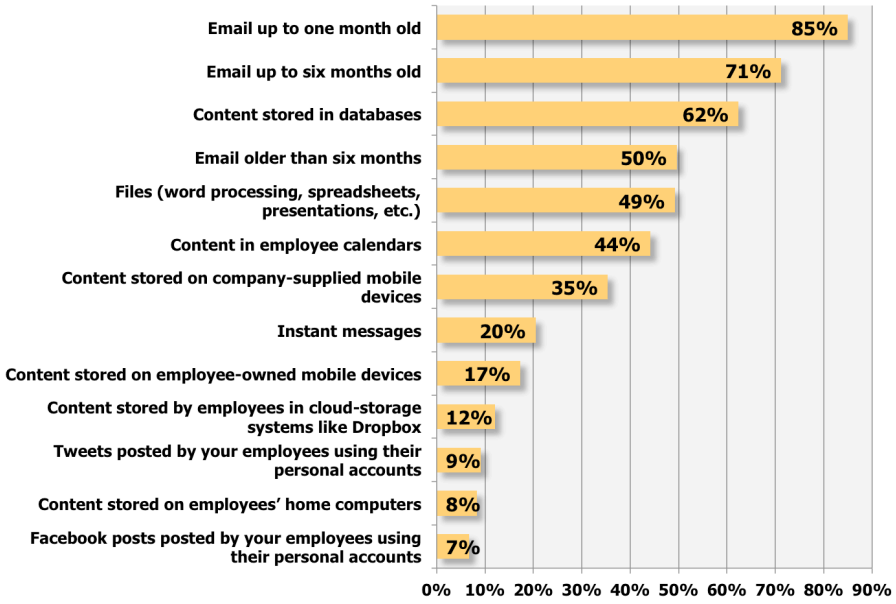


In the context of how ready organizations are for eDiscovery, our research also found a significant disparity of organizational preparedness based on the types of data that might be required for eDiscovery. As shown in the following figure, 85% of organizations consider themselves to be well prepared or very well prepared to conduct eDiscovery on email that is up to a month old, although preparedness to discover email falls significantly as email ages.

For conventional, non-email data like files, preparedness for eDiscovery is relatively poor, with only about one-half of organizations indicating they are prepared to conduct eDiscovery on files, despite the fact that other Osterman Research surveys have found that the largest single type of discoverable data is contained in files. With regard to other data types, preparedness for eDiscovery is quite poor, with only a fraction of organizations reporting that they are ready to conduct eDiscovery on these data types.

For conventional, non-email data like files, preparedness for eDiscovery is relatively poor.

Figure 4
Preparedness for Various eDiscovery-Related Activities
% Responding Well Prepared or Very Well Prepared



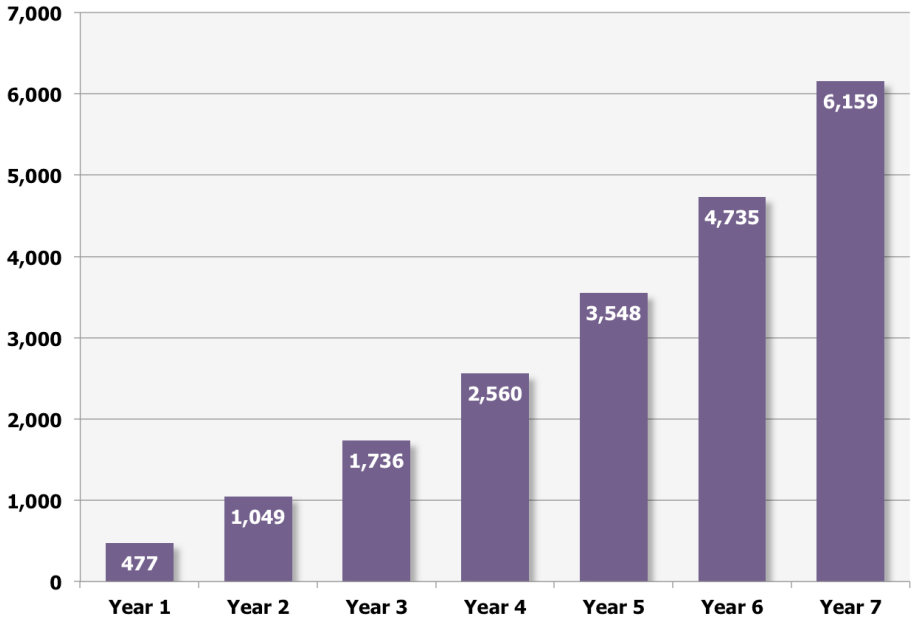
ELECTRONIC DATA VOLUMES ARE GROWING RAPIDLY

Organizations of all sizes generate an enormous amount of digital information. For example, the IDC Digital Universe study published in December 2012 estimated that 2.8 zettabytes (2.8 trillion gigabytes) of information were created and replicated during 2012, a dramatic increase from 2006 and a 56% increase from just 2011[i]. Add to this the fact that IBM estimates that every day 2.5 quintillion bytes of data are created[ii].

While a significant proportion of this data is normally not the focus of eDiscovery, the enormous scale and growth of ESI clearly illustrates the problem that organizations have, and will have, in finding and producing ESI. As a simple illustration of data growth, the figure on the following page demonstrates the growth of content storage in an organization with just 1,000 email users.

The enormous scale and growth of ESI clearly illustrates the problem that organizations have, and will have, in finding and producing ESI.

Figure 5
Archiving Requirements for a 1,000-Person Company Over Seven Years
Gigabytes of Content Storage



PRIMARY DRIVERS FOR eDISCOVERY

THE FEDERAL RULES OF CIVIL PROCEDURE

The Federal Rules of Civil Procedure (FRCP), established in 1934, are a set of rules that are focused on governing procedures for managing civil lawsuits in the United States district courts. The United States Supreme Court is responsible for overseeing the FRCP, but the United States Congress must approve these rules and any changes made to them.

A variety of important changes to the FRCP went into effect in December 2006. These included 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)]; the requirement that 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)]; the rule that 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)]; and the rule that 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)].

UPCOMING CHANGES TO THE FRCP

The Civil Rules Advisory Committee has offered a number of amendments to the FRCP that, if accepted, will go into effect on December 1, 2015 unless Congress intervenes. Key elements of these amendments will include:

- Greater emphasis on cooperation between litigants focused on controlling the burden and expense of eDiscovery with particular emphasis on court-initiated efforts to improve the level of cooperation between the parties. As part of this change, Rule 16(b)(1) would be amended to provide for improved communication for scheduling conferences, requiring that synchronous communication (face-to-face meetings, telephone calls, etc.) be used instead of written correspondence or email.

The Civil Rules Advisory Committee has offered a number of amendments to the FRCP that, if accepted, will go into effect on December 1, 2015.

- An increased emphasis on the proportionality of discovery efforts with the goal of limiting the scope of discovery. This includes limiting sanctions for failing to preserve content only if the lack of retention was "willful or in bad faith" and "caused substantial prejudice in the litigation" (with some exceptions). Part of this would include encouraging litigants to include preservation agreements as part of the 26(f) conference.

- Increased specificity would be required when objecting to document requests, including the requirement that any objection must "state whether any responsive materials are being withheld on the basis of that objection". This would affect parts of Rule 34.

- Earlier production of content would be required, including halving the length of time to serve defendants with a summons from 120 to 60 days.

A good overview of the proposed amendments is available from a number of sources[iii].

FEDERAL RULES OF EVIDENCE

The Federal Rules of Evidence (FRE), which have been in effect since 1975, are a set of requirements that focus on evidence presentation during trial in the US federal courts. Individual US states may use these rules as the basis for their own rules of evidence, or they can adopt 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 an essential component of the eDiscovery 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.

Authentication for electronic content is more critical than for paper-based documents because electronic documents are more easily altered. The process of copying data from one location to another can alter metadata, for example, and call into question its authenticity. When the authenticity of evidence is challenged, this can create a variety of problems and can add to the expense of a legal actions. Atkinson-Baker has developed a good overview of the authentication requirements for electronic records[iv].

A key ruling involving authenticity of electronic content is *Lorraine v. Merkel*, for which 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."*

RULES OUTSIDE OF THE UNITED STATES

US eDiscovery practices are perhaps more advanced and requirements more specific than in most other nations owing largely to the more litigious nature of US society relative to other nations. 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[v].

Authentication for electronic content is more critical than for paper-based documents because electronic documents are more easily altered.

While eDiscovery (often referred to as "e-disclosure" outside of the United States) in US legal proceedings can be difficult and expensive, laws in other parts of the world can present their own unique challenges. For example:

- Ontario amended its rules of civil procedure in 2010 so that it could 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."

- In most European nations litigants 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[vi].

- Courts in England and Wales can 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[vii]. However, in April 2013 the UK Civil Procedure Rule 31.5 went into effect, permitting courts more discretion 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[viii].

- Mexico does not have pre-trial discovery or disclosure requirements, but the courts can compel litigants and third parties to produce information if they determine it is necessary and if the documents are specifically identified.

- Australia's Supreme Court of Victoria, in Practice Note No. 1 of 2007 (February 2007), strongly suggested that the 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 developed eDiscovery rules similar to those contained in the 2006 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 and not via paper-based means.

- Various statutes designed to block discovery proceedings have been in place for many years in a number of countries. These statutes exist in Ontario, federal Canada (Business Records Protection Act), 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.

In most European nations litigants are not required to produce content that runs counter to the claims they make in a legal action.

LOCATION OF DISCOVERED DATA CAN ALSO BE AN ISSUE

Adopted in October 1995, European Commission Directive 95/46/EC was designed to standardize the protections for data privacy among EU member states and to protect individuals' rights to privacy. The Directive focuses on the processing of individuals' data held within the EU, but also applies to any entity outside of the EU to which data might be provided, such as data shared during the eDiscovery process. A key element of the Directive is that it does not permit data to be provided to any entity whose national laws do not adequately protect privacy rights.

Other noteworthy examples:

- France, with its somewhat unique legal system, imposes 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.

- The *Convention on the Taking of Evidence Abroad in Civil Matters* (the Hague Evidence Convention), ratified by 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."

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

OBLIGATIONS FOR ALL ORGANIZATIONS

A robust eDiscovery strategy should include several elements to ensure that it can satisfy an organization's litigation requirements and 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:

- **Litigation holds are key**
  A litigation hold requires the suspension of any content deletion processes or practices before during a legal action. Because organizations must preserve all relevant data when a legal action is reasonably anticipated, continuing to delete content after this point can result in serious consequences. Courts have the discretion to impose a variety of sanctions, including fines, adverse inference instructions to a jury, 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 harm to its corporate reputation.

- **Respond to requests rapidly**
  FRCP Rule 26(a)(1) requires that litigants have a good understanding of their data assets and that they are able to discuss these issues ahead of the initial pre-trial discovery meeting. Moreover, FRCP Rule 16(b) requires that this meeting take place within 99 days from the commencement of a legal action, and so all parties must have solid eDiscovery capabilities in place prior to litigation. In some cases, a court will require even more rapid production of content.

- **Identify content that can and cannot be accessed**
  All parties to civil litigation must determine the content that it can and cannot reasonably produce. If the evaluation determines that specific electronic content cannot be provided 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 content must be made available. As just one example, information describing content on backup tapes that is in a format that can no longer be read might need to be made available.

- **Manage a growing number of data types and venues**
  The eDiscovery process is further complicated by the need to produce a large and growing number of data types and platforms on which relevant data may be stored. For example, social media content from official, corporate accounts and personal accounts – if it contains business records that might be relevant during litigation – must be produced. Information on personally owned devices – which are rapidly becoming the mobile platform of choice in many organizations – must also be produced even though it is on devices that often are not under direct corporate control.

A litigation hold requires the suspension of any content deletion processes or practices before during a legal action.

eDISCOVERY REQUIREMENTS AND COMMON MISTAKES

There are a number of lessons that decision makers can learn from court decisions about what to do – and what not to do – with regard to eDiscovery. Here are some notable cases that can shed light on best practices when considering how to plan for eDiscovery:

- **eDiscovery must not be overly broad**
  In the 2010 case of *Moulin Global Eyecare Holdings Ltd. v. KPMG*, the court rejected the plaintiffs' arguments for a discovery request that it considered too expansive. The court determined that allowing such broad access to the defendant's electronic content would be "tantamount to requiring the defendants to turn over the contents of their filing cabinets for the plaintiffs to rummage through.[x]"

- **A failure to retain ESI can lead to sanctions**
  In *Pension Committee of University of Montreal Pension Plan v. Banc of America Securities, LLC*[xi], the Court issued sanctions against parties for not adequately preserving ESI, citing the "gross negligence" of their actions. This ruling occurred even though the judge found no evidence of bad faith on the part of those who did not retain the required ESI.

  In *Frank Gatto v. United Air Lines*, the plaintiff deleted his Facebook information, access to which had been requested by the plaintiffs. The court agreed with the defendant's motion and issued an adverse instruction[xii].

- **Backup tapes can create problems in eDiscovery**
  As we have discussed many times in other reports, backups tapes are a poor method for preserving discoverable content because extraction of this content is potentially time-consuming, expensive and may not produce all of the required information. The case of *Johnson v. Neiman*[xiii] is a good example: 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. Moreover, the defendant argued that this data was not reasonably accessible, a position with which the Court agreed and did not require production of the data – fortunately for the defendant.

- **Agreement about discoverable content is essential**
  In the case of *Digicel v. Cable & Wireless PLC*, the defendant made a decision not to search through their backup tapes for content without consulting the plaintiff. Moreover, the defendant determined the search terms it would use even though the plaintiffs did not agree with them. The UK 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 additional search terms.[xiv]

- **Demonstration that appropriate material was used**
  Many organizations use social media content in the recruiting and candidate evaluation process. However, employers are limited in the types of content that they can evaluate in the hiring process and 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 hiring process, it should archive the specific content it used about employment candidates to demonstrate that it did not evaluate material that could not be considered. A failure to do so – and an employer's inability to demonstrate its good faith evaluation of this information during eDiscovery – could result in serious consequences. Relevant regulations include the Americans with Disabilities Act, the Age Discrimination in Employment Act, the Civil Rights Act of 1964 and Executive Order. No. 11,246[xv].

- **eDiscovery must be managed properly**
  In the case of *Green v. Blitz U.S.A.*[xvi], the Court sanctioned the defendant for a variety of failures, including not putting a legal hold on relevant data, not coordinating the work of their representative with the defendant's IT department, and not performing keyword searches. The result was that relevant documents were not produced. Key documents were not discovered in this case, but were discovered in another case a year later. The result was a $250,000 civil

In Frank Gatto v. United Air Lines, the plaintiff deleted his Facebook information, access to which had been requested by the plaintiffs. The court agreed with the defendant's motion and issued an adverse instruction.

contempt sanction against Blitz, an order to inform plaintiffs from the past two years about the sanction, and an order to include a copy of the sanction memorandum in every case in which it would be involved during the next five years.

SOCIAL MEDIA RAISES OTHER ISSUES

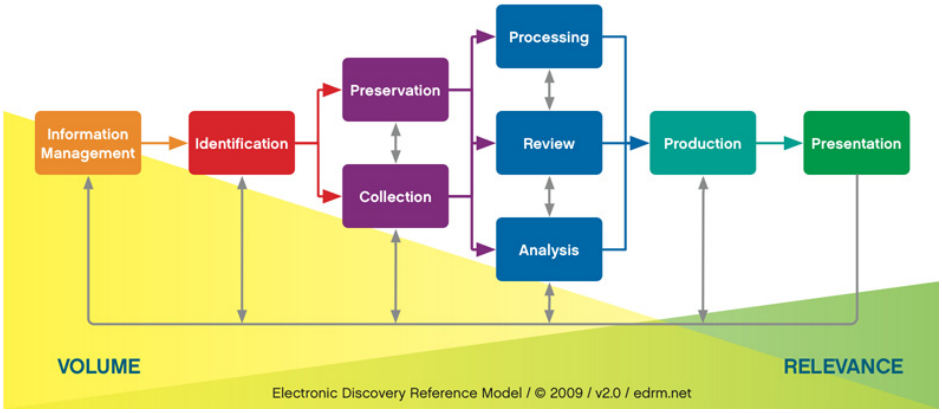
Social media has raised a number of issues in the context of litigation. One interesting development has been the increasing acceptance of courts to allow process serving to occur via social networks. The first such case was permitted by an Australian court in 2008 when legal documents in a foreclosure case were delivered via Facebook when conventional means of content delivery had proven to be fruitless. Courts in New Zealand, Singapore, Canada, the United Kingdom and in a few US states followed suit and now many courts allow process serving to occur when more conventional means of document delivery cannot be used[xvii].

Another interesting use of social media is its use in the jury selection process. For example, in the case of *Johnson v. McCullough* that was adjudicated before the Missouri Supreme Court in 2010, the Court ruled that attorneys have an affirmative duty to use online resources as a key component of the jury selection process[xviii].

THE ELECTRONIC DISCOVERY REFERENCE MODEL (EDRM)

The Electronic Discovery Reference Model (EDRM), which was placed into the public domain in May 2006, was developed in 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.

Figure 6
Electronic Discovery Reference Model[xix]



Social media has raised a number of issues in the context of litigation.

The EDRM is important because it represents a useful tool in the standardization of the eDiscovery process. Standardization is essential for eDiscovery 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 during the normal course of eDiscovery.

The EDRM XML project followed in the 2006-2007 timeframe. The goal of the 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.

ADDRESSING COSTS EARLY IN THE PROCESS

A RAND Corporation study[xx] found that 73% of the costs associated with producing electronic documents were consumed by review-related activities, while 19% was for processing and only 8% was for collection. Consequently, one of the fundamental goals of a good eDiscovery program should be the culling of non-relevant documents during the collection and processing phases because of the lower costs associated with the these two phases compared to the costs incurred during review. For example, one source estimates the cost of collection at $910 per gigabyte, the cost of processing at $2,931 per gigabyte, and the cost of review at $13,636 per gigabyte[xxi] (although other sources estimate the cost of review at between $18,000 and $25,000 per gigabyte). Based on these estimates, every 100 megabytes of content (~1,600 documents)[xxii] eliminated during the collection phase will save $1,364 in review costs.

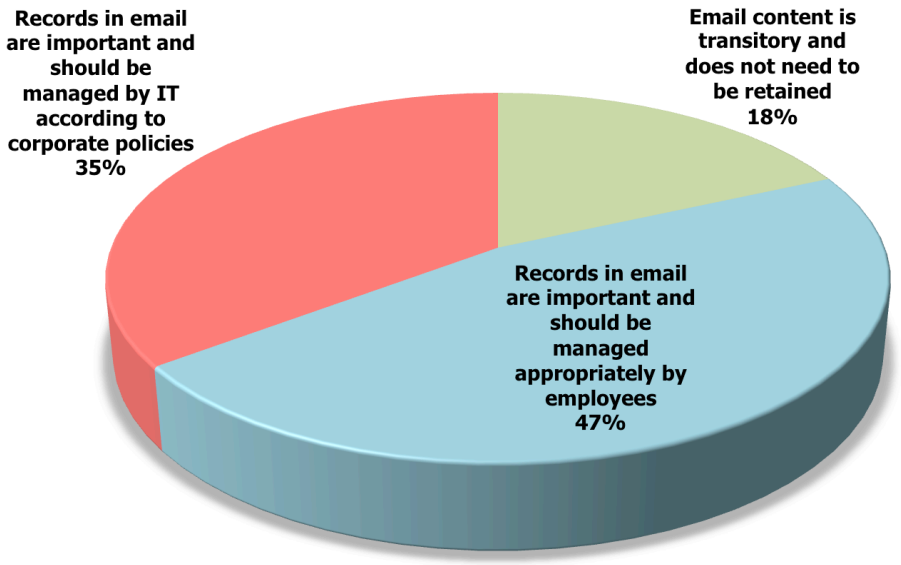
BEST PRACTICE RECOMMENDATIONS

THE CRITICAL IMPORTANCE OF GOOD CAPTURE

Our first recommendation is the need for management to understand the critical need to retain electronic records. While this may seem obvious to decision makers with a focus on good archiving practices, this view is not universally held. For example, as shown in the following figure from a major survey that Osterman Research conducted among mid-sized and large organizations in North America, nearly one-fifth of decision makers believe that corporate email is a transitory communications medium and consequently does not need to be retained. The survey also found that nearly one-half of decision makers believe that while email records are important, their retention should be managed by employees and not by IT according to a set of corporate policies.

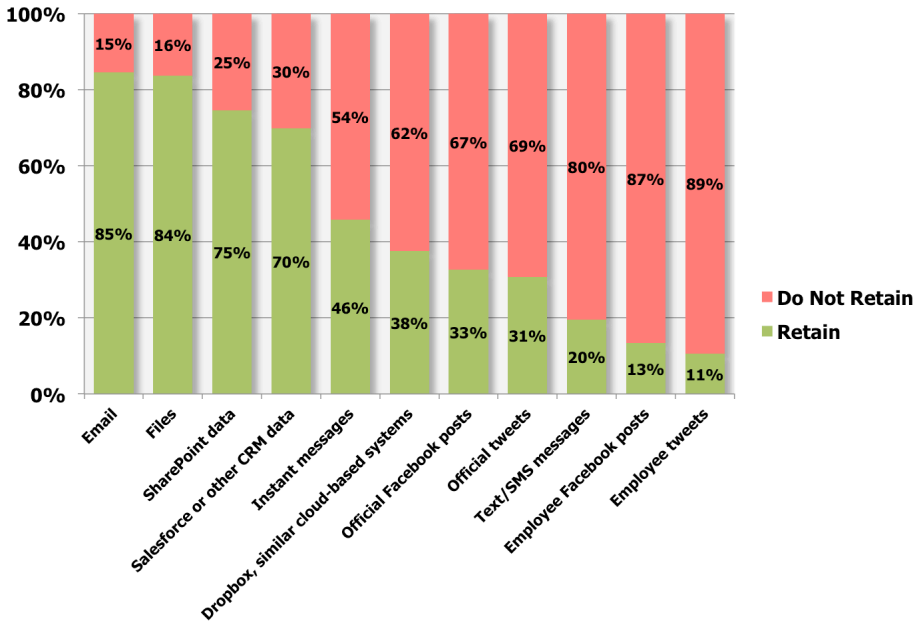
Nearly one-fifth of decision makers believe that corporate email is a transitory communications medium and consequently does not need to be retained.

Figure 7
Views on the Importance of Retaining Corporate Email



However, as shown in the following figure, the problem of not retaining important business records is not limited to email: most organizations do not retain content like social media posts, text messages and other information that might, at some point, be required for eDiscovery purposes.

Figure 8
Types of Information That Organizations Retain and Do Not Retain



GIVING eDISCOVERY THE IMPORTANCE IT DESERVES

Another important best practice is for decision makers to acknowledge the critical importance of eDiscovery in the context of all of the information it manages. As noted earlier, eDiscovery for email is a relatively high priority for the majority of decision makers, but eDiscovery for other content is not viewed as importantly. eDiscovery 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 an increasing proportion of business records become discoverable, decision makers will need to implement capabilities to capture this information for long-term retention and retrieval.

ESTABLISH KEY BEST PRACTICES

There are a variety of best practices that organizations should consider as they develop an eDiscovery strategy:

- **Focus on employee involvement**
  Policies, practices, procedures and technologies are essential components of a robust eDiscovery strategy, as discussed below. However, it is essential to educate all employees, consultants and others in the organization 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 eDiscovery significantly.

- **Ensure that IT and legal understand each other**
  So that a robust eDiscovery capability can be established, it is essential to start with a "meet-and-greet" among the relevant internal parties, most notably senior IT management and key legal decision makers. For example, 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 technology or eDiscovery technologies? Are the IT and legal stakeholders aware of who else would potentially be involved in eDiscovery planning? The establishment of this "legal-IT handshake" is a key first step in developing an effective eDiscovery strategy.

eDiscovery 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.

Having each group understand all of the requirements of the other groups will be helpful in developing an effective eDiscovery plan.

- **Develop good eDiscovery policies**
  It is essential to establish data retention and deletion schedules 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 electronic data that it will need for current and anticipated eDiscovery and other retention requirements, including data types like social media that it might never have considered capturing.

- **Implementing deletion policies**
  Many organizations, either by overspecifying the amount of data they must retain and/or by not establishing good data deletion policies, retain more information than is necessary, creating more and unnecessary liability. This can also result in higher eDiscovery costs because more data is retrieved and must be reviewed, as well as higher than necessary 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 is an important step here because decision makers must define what needs to be retained, what can safely be deleted, and the disposition method to be used.

- **The importance of litigation holds**
  If litigation is "reasonably anticipated", it is essential that an organization immediately begin to identify and preserve all of the data that might be considered relevant for the duration of the legal action. 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 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, suspend deletion policies and practices, and retain it for as long as necessary.

  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.

- **Implement the right technologies**
  Finally, it is essential to deploy the appropriate capabilities – archiving, storage, predictive coding, etc. – that will enable an organization to be proactive in the context of eDiscovery. As discussed above, 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.

It is essential to deploy the appropriate capabilities – archiving, storage, predictive coding, etc. – that will enable an organization to be proactive in the context of eDiscovery.

SPONSOR OF THIS WHITE PAPER

HP Autonomy, is a global leader in software that processes human information, or unstructured data, including social media, email, video, audio, text, web pages, and more. HP Autonomy's powerful management and analytic tools for structured information together with its ability to extract meaning in real time from all forms of information, regardless of format, offer a unique capability for organizations seeking to derive the most value from their data.

HP eDiscovery is the industry's most complete application for responding to legal matters and investigations. With a wide range of features built into a single application – including data processing, ECA, clustering, visual analytics, and Technology Assisted Review – customers can perform from identification through production, without the added risk and cost of switching applications at various stages. Autonomy eDiscovery, powered by HP's IDOL technology, uniquely expedites the eDiscovery process by forming a conceptual understanding of enterprise content, independent of language or format. With our eDiscovery product, you can deploy in house, or leverage the security and scalability of the HP cloud infrastructure, as well as the expertise of our trained professional services staff.

protect.autonomy.com

twitter.com/ HPAutnInfoGov

autonomyinfo@hp.com

+1 415 243 9955

+44 1223 4480000

---

[i] http://www.storagenewsletter.com/news/marketreport/idc-digital-universe-study-2012
[ii] http://www-01.ibm.com/software/data/bigdata/
[iii] http://www.martindale.com/litigation-law/article_Drinker-Biddle-Reath-LLP_1932044.htm
[iv] http://www.depo.com/resources/aa_thediscoveryupdate/authenticating_email.html
[v] http://wiki.answers.com/Q/What_country_in_the_world_has_most_lawyers_per_capita
[vi] http://www.legaltechnology.com/the-orange-rag-blog/guest-article-the-ediscovery-passport/
[vii] http://www.justice.gov.uk/courts/procedure-rules/civil/rules/part31#IDAALICC
[viii] http://www.clearwellsystems.com/e-discovery-blog/tag/practice-direction/
[ix] http://www.mcmillan.ca/Files/ARTICLE_E-Discovery_Around_the_World_0110.pdf
[x] http://www.clearwellsystems.com/e-discovery-blog/tag/case-law/
[xi] 2010 WL 184312 (S.D.N.Y. Jan. 15, 2010)
[xii] http://aplcs.com/caselaw/social-media-legal-discover/
[xiii] 2010 U.S. Dist. LEXIS 110496 (E.D. Mo. Oct. 18, 2010)
[xiv] Source: Kroll Ontrack
[xv] http://archivesocial.com/blog/social-media-recruitment/
[xvi] http://civilprocedure.dbllaw.com/2011/08/past-eDiscovery-errors-result-in-sanctions/
[xvii] http://www.rmmagazine.com/2012/10/08/like-it-or-not-how-social-media-can-lead-to-litigation/
[xviii] Ibid
[xix] Source: EDRM (edrm.net)
[xx] *Where the Money Goes: Understanding Litigant Expenditures for Producing Electronic Discovery*, RAND Institute for Civil Justice
[xxi] http://www.slideshare.net/jmancini77/arma-michigan
[xxii] http://www.providusgroup.com/doc_review/doc_review_calc.php