

THE JUDGE GROUP

Preparing for e-discovery

The litigator and the information professional responsibilities



Fred V. Diers CRM FAI

Vice President

Governance, Risk, & Compliance Practice

Judge Consulting Group

Contents

An e-discovery problem: Lack of collaboration between Legal and IT.....	3
E-discovery triggers.....	3
Repository disclosure.....	3
The gap between data and documents	4
Managing the e-discovery process	5
Collaboration action steps for IT and Legal	6
Step 1: Litigation pro-active response planning	6
Step 2: Applying Legal Holds.....	7
Step 3: Collecting ESI.....	8
Step 4: Analyzing and Reviewing ESI.....	8
Step 5: Producing ESI	9
Circle the wagons – Be proactive.....	9
About The Judge Group	11
About the Author	11

An e-discovery problem: Lack of collaboration between Legal and IT

E-discovery, by its very nature, is easier to get wrong than it is to get right. Gone are the days when attorneys had to sift through mountains of paper files looking for relevant information pertaining to a case or government investigation. Today's digital data can be classified, stored and searched. However, due to the ease by which digital information can be created and retained by employees in a multitude of different ways, and the constant and monumental change in how individuals manage and use information, many companies avoid or fail to introduce and monitor information organizational techniques. Because of this dispersed, unmanaged data, attorneys are no longer looking at a collection of potentially responsive information, but rather spend time examining system defaults, duplicative, and irrelevant personal data. What has developed is a misnomer by company attorneys who believe their data repositories are controlled by IT, when in fact much of the organization's data is in multiple disparate locations, squirreled away in personal storage devices and many other unmanaged systems. Compounding this issue is the seemingly endless amount of data digitally stored within an organization.

The combination of people, process and technology, and e-discovery best practices will help an organization deal with the growing amount of information and legal and regulatory requests that draw on that information; however, critical to the success of the approach is ongoing collaboration between the Legal and IT teams. Working together to manage data collection, understand your Electronically Stored Information (ESI) universe, and remain confident that you know where your information is retained will save corporate embarrassment, fines, court sanctions, and ultimately jobs.

This paper reviews e-discovery scenarios where Legal and IT must be in collaboration including understanding both sets of requirements and responsibilities, and managing the e-discovery process. It also outlines collaboration action steps for Legal and IT to follow which ensure regulatory compliance and reduced costs and risk of e-discovery.

E-discovery triggers

While Electronic Discovery (E-Discovery) has a simple definition i.e. the process of identifying, segregating, preserving, and reviewing, data and documents that are retained in an electronic repository – the implementation of e-discovery is not simple. Data and documents to be preserved are dependent on the type of court approved production order. These production orders are for specific information related to a legal matter, tax audit, government agency investigation resulting from non-compliance with regulations, or due diligence relating to a company transaction. Whatever the trigger for document discovery or disclosure, courts that oversee these cases require attorneys follow guidelines and rules.

The Federal Rules of Civil Procedure (FRCP) has dramatically changed the face of discovery not only in America, but for all international businesses that deal with a US organization, foreign operations that have a US presence, or international operations of a US-based organization. The focus on ESI and the disclosure requirement by counsel to identify all data repositories to opposing counsel by the 'meet and confer' clause of 120 days after the case is filed opens up Pandora's Box as it allows attorneys to internally question whether responsive data is stored in a particular known repository. From the e-discovery trigger, there is a need for collaboration and established processes between Legal and IT to be able to respond efficiently and effectively.

Repository disclosure

The first 120 days from the date a subpoena is received are where the e-discovery process can get derailed and become both a publicity embarrassment and legal liability to the organization. Although in-house counsel and IT professionals must collaborate upon receipt of a subpoena to determine what ESI needs to be preserved, this is not to be confused with the issuance of a legal hold (or hold) order. Repository disclosure is the process of

identifying all media storage initially preserving information until plaintiff counsel provides detailed information on production requests whereby a hold order can be issued. If the organization cannot reasonably document the disposition of content in question, the court could impose fines. This initial repository identification and preservation requires suspension of auto-deletes for data from servers, notices sent out to impacted employees, contractors, third party vendors, and anyone else holding information on behalf of the company. These notices instruct the recipient to suspend deletion of data and electronic documents stored on hard drives or external storage devices not controlled by IT, as well as preserving all metadata associated with the electronic document until a defined hold order is issued.

Once the data is preserved, the next step is to receive and review the plaintiff's production request. The production request requires company attorneys to evaluate the request and internally answer:

- What are the grounds for the case?
- What is the organization risk?
- What are the options – settle or take it to court?

These are critical issues to understand as early as possible in order to control the level of document production, IT and internal counsel resources, and outside legal costs that are based on the volume of data to be reviewed.

The gap between data and documents

When determining what information is to be put on hold and reviewed the definition of data versus document can be a wide communication gap between in-house litigation counsel and the IT teams. Attorneys tend to think of documents in a holistic sense – if a production order requests personnel information, for example, in-house counsel will request the Personnel File, referencing a familiar paper organization of documents that is comfortable and finite. On the other hand, an IT professional thinks of data as components or objects that make up a document or a workflow process. Referring to the Personnel File request, the data or objects that equal the content making up that 'paper' personnel file may be stored in multiple repositories and databases from personnel core data reflecting name, social security number, age, ethnicity etc. to images of resumes, letters of recommendation, etc. To compile and extract information to meet the attorney's *document* request may require multiple programs and searches within *data* repositories. Hampering the entire e-discovery process may be the ambiguity of the production search instructions or the sheer volume of data that is growing exponentially.

Consider the growth of e-mail content. IT is forced to add additional servers, force mail box limits, and auto-delete in-box and sent-item folders in shorter periods of time. These actions force users to retain e-mail messages on hard-drives, in print form, or external drives. Suddenly, the access to complete information on a subject is not centralized or known at the enterprise level - a 'document(s)' no longer represents all the relevant information. A communication gap occurs between Legal and IT when it comes to accessing and producing 'complete and disclosed' respondent information on a perceived simple request. Counsel cannot understand why IT cannot produce all of the desired data in a timely and assured complete manner. Linkages between data or objects stored are not clearly understood by attorneys while identifying complete content or response to a request does not register with IT since they traditionally rely on users who created the data to be knowledgeable as to the document's content and location.

It is imperative that in the establishment of an e-discovery strategy, communication and an understanding of common terms are clearly defined.

Managing the e-discovery process

Internal counsel and IT must understand their organization's ESI universe and apply standards and policies to ensure compliance and consistency in identifying and storing data, documents, and records. Once fundamental retention policies are established across the enterprise and all forms of information, using the following best practices – a combination of people, processes and technology – will enable both in-house counsel and IT personnel to be compliant and reduce the associated risk and costs of e-discovery:

- **Capture** – catalog the location, type, and volume of data being created, disseminated and retained on network servers, hard drives, back-up tapes or other storage devices.
- **Manage** – set high level indexing standards for users to consistently identify data and documents. Associated with these classification standards are preservation periods based on government guidelines and operating requirements.
- **Dispose** – apply retention periods to cataloged ESI as well as duplicates or copies and delete the data from all sources as a common practice during the normal course of business. Set up compliance audit reviews to ensure disposition practice is consistent.
- **Lawsuit** – receive notice of a lawsuit, in-house counsel evaluates the claim at 'meet and confer', determine if a preservation order is required, set up meetings with IT to stop automated deletions programs and send out notices to impacted parties (both internal and outside vendors) to suspend disposition.
- **Hold** – evaluate scope of production order and place a formal hold to suspend physical and electronic document destruction on impacted servers, PC and laptop hard-drives, PDA servers, back-up tapes from identified servers, and physical storage. This is a formal legal hold notice to those impacted employees retaining potentially responsive information.
- **Analyze** – assess the case and determine relevant information such as key custodians, search keywords, data ranges, events, and email discussions. Organizations also use this phase to cull-down collected data sets to much smaller relevant data sets.
- **Review** – work with IT to review, code, redact, and produce all documents relating to the case, to provide plaintiff counsel in response to the discovery order. A notice is sent to impacted employees and IT releasing documents stored on hard drives and servers determined to be non-responsive.
- **Production** – segregating responsive documents enables the organization to limit the scope of discovery orders by finding the content related to the lawsuit through the proactive use of enterprise classification and retention standards. Similar discovery orders can easily target existing responsive document holdings limiting the cost and IT resource requirements.

The above practices will only be successfully enabled when an organization's Legal and IT departments are proactive and prepared for e-discovery. Being proactive by setting enterprise standards and practices requires extensive change management.

- *Change management involves IT* and the selection of appropriate tools by applying retention policies to both structured and unstructured data, to change IT-user service composition regarding restore requests of old data, and rework back-up regimes to reduce tape volumes. Appropriate tools include Enterprise Content Management software including Document and Records Management software, E-mail vaulting software, and ERP (e.g. SAP, JD Edwards systems) object retention software, just to name a few.

- *Change management involves Legal* to endorse and enforce classification and retention standards, effectively manage legal holds with written procedures, and establish a technology subject matter expert or '30b6' witness with IT collaboration that is knowledgeable of the organization's ESI universe.
- *Change management impacts all employees* that create information by driving classification and responsibility of information standards adherence to the desktop. No longer can this work be relegated to another function or person, it is the responsibility of the employee to index their created and received documents, e-mails, etc. according to enterprise rules.

Without these changes, preparing for e-discovery challenges will be costly and disruptive to business operations. E-discovery is constant and will be unavoidable in the future; adequate preparation and management support is paramount.

Executive management, working with in-house counsel, must evaluate risk of litigation to the organization. If the number of lawsuits is manageable and the claims minor, then the scope of e-discovery preparedness can be modified i.e. best practices may be augmented to reflect the level of risk associated with issuing legal holds or locating responsive information. Regardless of the risk assessment, understanding, cataloging, and disclosing ESI and associated repositories at the 'meet and confer' remains a high priority.

Collaboration action steps for IT and Legal

E-discovery best practices can only be achieved when Legal counsel and IT professionals work together to understand their respective responsibilities. This requires on-going communication, written policies and procedures, and education on the issues. Other teams including Records Management should also be involved in areas such as classification and retention policy setting. Education and training must extend to all personnel with ongoing audits to monitor compliance. The following outlines key steps Legal and IT must collaborate on and control for effectively managing the e-discovery process.

Step 1: Litigation pro-active response planning

IT is responsible for information technology infrastructure mapping. Mapping is cataloging various systems, software, databases, servers, legacy systems, back-up processes, share-drive structures, common databases, PDA services, PC's, laptop inventory, and e-mail structures/storage limitations.

This information is to be shared with Legal as the foundation for understanding how data or objects are created, disseminated, and retained in the IT environment.

From this mapping, IT and Legal should be able to map the required ESI to the appropriate databases, servers, drives, and external storage devices. This effort can be done, in part, using 'crawler software' that scans storage and databases listing their contents. Some crawler software will provide categories based on collected common themes. Usually, crawler software will create a detailed inventory of content that needs to be reviewed and analyzed.

For electronic documents or e-mail retained on personal hard drives or e-mail .psts, the user should be engaged to provide a list or inventory of directory structures and items retained.

Without Document and Records Management software, inventorying the various storage devices can be a laborious process. Human nature, without guidance on how to index and store information will develop a myriad of diverse systems that identifies or classifies their documents. Technology options for an organization are Electronic Document and Records Management (EDRM) software. With EDRM software, standard terminology and classifications can be applied to the software tables for users to select when they save a document. Additional benefits from these enterprise implemented software packages are a centralized storage repository and extensive

research capabilities. To minimize information duplication no electronic documents can be stored on local drives. This must be driven by corporate policy and compliance auditing.

For the purpose of executive management information, litigation attorneys usually track a list of the current open litigations with which the organization is engaged. In addition to the list of open litigations, the production orders associated with each litigation should be tracked to avoid repetitive searching of the same data. These reports must be shared with IT to not only preserve responsive data, but to avoid discarding responsive documents from a resolved claim or litigation while a similar litigation is in process. A technology solution that can apply multiple holds on a single document is a valuable tool for e-discovery.

Ongoing communication and training for all staff and external vendors holding records on the organizations behalf should be performed on a regular basis. This ensures a consistency in collecting and producing responsive records when requested and demonstrates to the court that the organization has made an effort to comply with rules and regulations.

Step 2: Applying Legal Holds

Once litigation is filed and the organization accepts notice, the first step by in-house counsel is to evaluate the grounds for the claim, determine the organization's exposure, and conduct a risk assessment that includes potential costs. As a precaution in this early case assessment, counsel should issue preservation instruction to suspend destruction of data from auto-deletes and scheduled retention disposition. This initial preservation order is a short term measure and should be lifted and replaced by a hold order once the scope of the production order is received and analyzed.

Too often these blanket preservation orders become the litigation hold order and freeze any destruction of records in the normal course of business. Universal hold orders impacting all of the organization's information assets are rare. Generally, requests for documents relating to the claim are older records and not current information. Why have holds on destruction of all information when specific documents related to the litigation production request can be preserved allowing routine disposition of unrelated information?

Once counsel reviews the production order and determines that a legal hold is required, the next step is to work with IT and Records Management to identify the data repositories and personnel that the legal hold will impact. Communication must be immediate and contain the following information, at a minimum:

- List of databases, servers, and back-up tapes (if applicable) that will be searched and produced by IT.
- List of employees who may have documents pertaining to the subject matter.
- List of executives who may have responsive information (originals and copies).
- Detail of claim, type of information and date ranges, to be collected and forwarded to designated database or person.
- List of personnel storage devices that may be searched including home computers containing company data that meets the hold order.
- Penalties for not adhering to the hold order and association policies.

Since major litigations could take years to resolve, regular communications (monthly or quarterly) must occur to remind affected parties of the legal hold and the necessity to preserve information even if collection has not yet taken place. This is referred to as 'phasing' the hold order process to ensure relevant information is being preserved, as well as notify changes in document production scope during the course of the litigation.

Releasing hold orders is critical once a case is resolved. Unfortunately, due to the duration of the case, attorneys often forget that hold orders are in place, resulting in information being retained long after the case is settled. Releasing a hold order not only allows the routine disposition of data retained for collection, but of all the copies

of information and the responsive document collection repository. It is the responsibility of Legal to notify IT and users of the release, as well as listing claims and litigation requiring similar information for ongoing production orders that are still in force.

Legal hold policies and procedures must be documented and available to all personnel to avoid spoliation of evidence.

Step 3: Collecting ESI

The most common requested information by plaintiff counsel is e-mail messages. Traditionally servers retaining e-mails have a limited retention based on user mail box size. E-mails exceeding mail-box size limits are held on local hard-drives either in personal e-mail folders (.pst) or document folders. To collect e-mail, IT must search from multiple sources – servers, back-up tapes, imaged hard drives, or external storage devices. If no document, records management software, or compliance archiving and storage solutions are used to capture and catalog e-mail for easy access and retrieval, then responsive e-mail from all sources, even if it duplicated multiple times must be collected and copied to a single repository for review.

Journaling (capturing) e-mail coming into or sent from an organization is gaining popularity as it allows one instance of an e-mail message to be stored in a single repository for key-word search and review. This can cause problems however as e-mail is still being retained in multiple repositories that create a volume management problem based on the hold orders for duplicates.

Back-up tapes pose another liability problem for organizations. IT has traditionally maintained back-up tapes as a data repository for users to request restores if the user inadvertently deletes a document or cannot locate a document that is several months or years old. The defensible position to avoid producing tapes is having a strict policy that back-up media for disaster recovery of internal systems reduces the retention of these tapes to days instead of years. If the documented policy is applied, it is a defensible position for the organization from having to produce the tapes and a list of contents of each tape.

Counsel and IT must collaborate on a production approach, one that identifies accessible information and one that argues the safe harbor provision of the FRCP. This provision states that if data is inaccessible due to the cost of extracting information from old or legacy systems or that the software/hardware no longer exists, the contents should not be produced. Generally the defense of a safe harbor is cost of accessing meaningful data. There has been limited success in applying the safe harbor provision as plaintiff counsel may wish to share the cost of getting the inaccessible data whereby the court may grant this approach.

Step 4: Analyzing and Reviewing ESI

Once all the data potentially relevant to the case has been collected and preserved, the traditional approach to e-discovery has forced companies to launch a massive “review effort” that entails hiring several contract attorneys who are allocated portions of the data for manual review. These reviewers spend many days sifting through false positives, irrelevant messages, and redundant data. As a result, it is often weeks before the true context of the case and case strategy are known. Instead, companies can use tools that allow them to rapidly process the data and identify relevant information, well before manual review. This allows them to perform early case analysis and receive fast answers to critical questions such as:

- Can we quickly find a smoking gun and locate all of its instances?
- Can we determine who knew what and when?
- How do I know what to look for?
- How do we find all the email address and domain permutations for certain individuals?

- Can we quickly determine how many documents are responsive and, thus, if we can meet the deadline?
- Are we sure that we have identified all the custodians and all the data relevant to the case?

Answers to these questions help companies determine the critically important early case assessment. By knowing early in the process whether they should settle a case or prepare for court, companies realize significant cost savings.

The review phase of e-discovery is seldom done by one individual, but rather depends on the efforts of a team of legal reviewers. An e-discovery management platform that allows for a collaborative review creates efficiencies in the review process, and easily allows a case manager to track the progress of the matter. Often times, legal teams in remote locations are involved in the review phase, and a web based interface that allows for collaborative review offers substantial cost and time savings.

Step 5: Producing ESI

Electronic production is providing all collected data together with the associated metadata (information about the document or e-mail) using an external drive or DVD to provide to outside counsel for their review. This step must be controlled by both Legal and IT. In some cases the organizations outside counsel will provide software to download the organization data. A copy of the collected data is preserved in-house under the auspices of attorney-client privilege. The responsibility to preserve this produced information resides with IT who manages the access to the information.

Prior to releasing collected data to outside counsel, IT, with internal counsel oversight, will strip the collected data of program related files or executables. This provides the reviewing counsel only those data files that may be responsive to the production request.

Now that the collected electronic documents have been reviewed and segregated by:

- Non-responsive to the specific production request
- Non-producible due to attorney-client privilege
 - Inadvertent production of protected documents usually is the result of ignoring information tagged as attorney-client privilege. Once this information is produced to plaintiff's counsel, the court may rule to release all documents so tagged or require plaintiff's counsel to ignore the documents. It is the decision of the court as to the disposition of the documents in question.
- Extracted duplicate information

The remaining set of documents is coded, redacted, filtered and delivered to plaintiff counsel. A copy of the delivered documents is held by the organization as litigation evidence until the case has been resolved. This copy will be destroyed once all appeals are concluded and any court preservation instructions are lifted.

Circle the wagons – Be proactive

Without continued collaboration between the in-house Counsel and IT professional, an organization cannot be proactive in preparing for and managing the e-discovery process. Understanding each team member's mission within the organization, defining roles and responsibilities, and mutually developing information standards and practices enables effective and defensible compliance with e-discovery rules. Without these internally recognized, enforced standards and practices, ongoing deletion of data cannot be justified as it will expose the organization to obstruction of justice charges. Ignorance is also not an excuse, nor is an oversimplified policy that lacks teeth to ensure compliance. E-discovery policies must become a repeatable and consistent business process. Knowledge of

data repositories and establishment of processes for the content contained in those repositories is a core capability of today's enterprise.

Staff training and selection of the appropriate technology tools ensure that policies are compliant and enforceable. An organization cannot have one without the other.

The extent of being proactive by establishing standards and practices will depend on the business environment and risk tolerance. But an organization cannot afford to forgo information standards completely. Policies, procedures and process documentation are the first line of defense in the new e-discovery world.

This first line of defense cannot prevail without close coordination between Legal and IT. Each must understand the service culture of IT and the defense culture of Legal. Working together as a team with willingness to compromise is essential for both groups to meet e-discovery challenges, realistic volume reductions, and the ESI discovery requirements and limitations of the organization's current system infrastructure and documented rules. Implementing best practices and bringing IT and Legal counsel together as a united front to manage e-discovery is a requirement of any organization seeking to reduce the risk and cost of e-discovery.

About The Judge Group

The Judge Group's Governance Risk and Compliance (GRC) Practice specializes in developing enterprise-wide sustainable and compliant Information Lifecycle Programs for managing both unstructured and structured electronic information assets, physical documents, e-mail content and data archives.

Our mission is to leverage our best practices, utilize our international resources and continue to offer our clients innovative approaches to develop business solutions for tomorrow's needs.

Unbiased Subject-Matter Expertise:

Our deep industry knowledge combined with unbiased subject matter expertise enables Judge to provide our clients with the right GRC program to compliment their corporate culture, budget and needs.

International Capabilities and Experience:

Judge's GRC Practice utilizes in-country consultants throughout a global network. Our international reach extends across boundaries, bridges cultural and language gaps and enhances the quality of service we provide to our clients.

Sustainable and Compliant Information Lifecycle Programs:

In today's compliance and risk landscape, organizations must be proactive in developing enterprise data, document, and records policies and procedures that are both sustainable and compliant. This is why Judge provides experienced consultants to assist multinational organizations in implementing information business rules that conform to today's regulatory and compliance requirements.

For more information visit http://www.judge.com/techconsulting_governance.asp

About the Author

Fred V. Diers, CRM FAI Vice President – Governance, Risk, and Compliance Practice, The Judge Group

Fred Diers has over 35 years of Records and Information Management experience for multinational organizations as a practitioner and consultant. He has successfully implemented realistic and sustainable records management programs on a global scale for companies operating in over 80 countries addressing both electronic and paper documents and records. More recently he has worked with information technology and law functions to develop e-discovery process solutions based on the Department of Justice revised rules of evidence.

A significant component of Fred's expertise involves developing business rules pertaining to information life cycle including indexing, metadata, and retention standards. His methodology focuses on developing a balance between compliance and the organization use of its information resources.