MAYER·BROWN

Electronic Discovery & Records Management

2012 TIPS OF THE MONTH – A Compilation

Table of Contents

Tip of the Month

Introduction

2012 Trends in E-Discovery

The year 2012, while lacking the blockbuster e-discovery cases of some recent years, still demonstrated the ongoing growth of e-discovery's role in state and federal litigation. Moreover, e-discovery's footprint continues to expand beyond active discovery practice in litigation to encompass a fundamental aspect of information governance, an issue of growing importance in many organizations. Early investment in policies, procedures technology and personnel regarding information governance, which allow for routine or project-based defensible deletion, continues to pay dividends when put in place *before* litigation is threatened or commenced. Indeed, the key trends of 2012 illustrate e-discovery's impact on business both before and after the start of a lawsuit. Key issues included the ongoing clarification of e-discovery rules by state and federal courts, the increased availability of enterprise technology to aid in the enforcement of information governance policies (including preservation for legal holds), the rise of technology assisted review, and the ongoing expansion of the role of social media as an important communication tool (and data source for litigation/investigations).

E-Discovery Court Rules and Decisions

By the end of 2012, over thirty states had adopted e-discovery rules based upon the 2006 Amendments to the Federal Rules of Civil Procedure. In 2012, Florida (In re: Amendments To The Florida Rules of Civil Procedure – Electronic Discovery, July 5, 2012 (Supreme Court of Florida)) and Connecticut (Minutes of the Annual Meeting, Judges of the Superior Court, June 20, 2011, approving amendments to the Practice Book and to the Code of Evidence effective January 1, 2012) promulgated their e-discovery rules, while Massachusetts and the District of Columbia have proposals pending approval. Courts have also continued the trend toward more uniform e-discovery standards. In February 2012, largely resolving a long-standing uncertainty in New York state practice, the First Department, Appellate Division of the New York State Supreme Court adopted the *Zubulake* standard that the producing party bears the initial cost for searching for, retrieving and producing discovery, subject to cost-shifting based upon a seven-factor guideline. *U.S. Bank National Association v. GreenPoint Mortgage Funding, Inc.*, 2012 NY Slip. Op. 01515 (1st Dep't Feb. 28, 2012). Finally, a 2012 ruling by U.S. District Judge Shira Scheindlin in the Southern District of New York significantly elevated the standard the federal government must meet in showing the adequacy of data search efforts in the context of the Freedom of Information Act. *National Day Laborer Organizing Network, et al. v. United States Immigration and Customs Enforcement Agency, et al.*, 2012 U.S. Dist. Lexis 97863 (S.D.N.Y. July 13, 2012). The federal government's new exposure to the harsh standards of e-discovery practice may gradually

have an effect upon the discovery demands made by government bodies to civil litigants. While state and federal courts are still working to provide more certainty in e-discovery practice, and many states still lack practice rules concerning e-discovery, the trend toward greater predictability and uniformity continued through 2012.

Defensible Deletion

The volume of data processed by organizations of all sizes continued to increase unabated in 2012, and there is a trend to start developing and implementing information governance policies and procedures around ESI to allow for defensible deletion *(i.e.*, deletion of ESI that is not subject to legal or regulatory requirements, and is not needed for business reasons). Effective information governance is vital to any business and the tools used by organizations to store, manage, monitor, track and protect their data simply must involve a consideration of e-discovery issues. In particular, organizations, especially highly regulated serial litigants, have endeavored to more efficiently manage ESI subject to legal and regulatory requirements by, *inter alia*, segregating ESI subject to regulatory requirements, streamlining the process of implementing legal holds in response to pending or threatened litigation, and routinely (or a project basis) deleting other ESI (a marked shift from the "save-everything" approach of the last decade). Interestingly, the driving factors in considering defensible deletion are not exclusively cost-related, but developing concepts of data privacy (e.g., imposing time limits on how long certain personal data should be retained by an organization) and the idea that certain information is valuable to an organization and potentially revenue-generating if the less-valuable data was removed.

The Cloud

Increasing numbers of organizations are considering placing their data in a "cloud" environment. Cloud computing is the use of computing resources, including both hardware and software, that are made available over the Internet by a subscription-based service provider. Because cloud computing is Internet-based, it offers several advantages over more traditional access to an organization's data and software, including the ability to scale the environment to meet an organization's needs. However, there are a number of challenges in implementing a cloud-based information environment, and the legal and regulatory landscape is not fully developed. At this stage, organizations are focused on the language of the cloud-computing contracts to best protect them from the legal and regulatory uncertainties. We will see if such protections are adequate in the coming years.

Technology Assisted Review

While technology assisted review, particularly predictive coding, remains a new and largely untested technology, two influential courts endorsed its application under certain circumstances in 2012. In very basic terms, predictive coding is a process by which attorneys code an initial sample set of data for responsiveness. That coding is then used to "train" a software program to review the broader set of documents automatically. In *Da Silva Moore v. Publicis Groupe*, the U.S. District Court for the Southern District of New York endorsed the use of predictive coding in certain cases, especially those with large amounts of ESI at issue. Case No. 1:11-cv-01279 (S.D.N.Y. April 26, 2012). Additionally, in October 2012 the Delaware Chancery Court *sua sponte* ordered the parties to use predictive coding for their review of documents. *EOHB, Inc. et al. v. HOL Holdings, LLC*, CA No. 7409-VCL (Del. Ch.

Oct. 15, 2012). In his ruling Vice Chancellor J. Travis Laster also acknowledged that the case at issue would potentially involve the review of a huge amount of documents. Although the benefits of predictive coding remain widely debated, the search for improved cost-effectiveness and efficiency in the review and production of ESI may continue to lead courts to encourage the use of technology assisted review.

Social Media

Social media platforms have attracted record numbers of users year after year, and 2012 was no exception. In order to tap into this expanding market of potential customers and consumers, businesses continue to expand their engagement with social media. Such engagement into previously uncharted waters may present significant risk to organizations and individuals. For example, a July 5, 2012 Facebook post by Netflix CEO Reed Hastings prompted a SEC investigation into whether the post, which concerned record levels of monthly viewership, violated securities rules concerning the dissemination of material corporate information. The voluminous amount of data associated with social media are ongoing targets for discovery by both plaintiffs and defendants, and recent court decisions have clearly demonstrated that relevant information will be discoverable regardless of how that information is generated or where that information is stored. Social media also raises questions of preservation obligations in a world of constantly updated profiles and "statuses." Organizations must be cognizant of social media use by their employees and, as importantly, must develop clear protocols for social media use on behalf of the organization or via its network and equipment.

For inquiries related to this summary of the 2012 Trends in E-Discovery, please contact any of the following lawyers.

Anthony J. Diana
adiana@mayerbrown.com

Michael E. Lackey
mlackey@mayerbrown.com

Therese Craparo
tcraparo@mayerbrown.com

Kim A. Leffert
kleffert@mayerbrown.com

Jarman Russell
jrussell@mayerbrown.com

Learn more about Mayer Brown's Electronic Discovery & Records Management practice, please contact any of the following lawyers.

Anthony J. Diana
adiana@mayerbrown.com

Michael E. Lackey
mlackey@mayerbrown.com

Ed Sautter
esautter@mayerbrown.com

Please visit us at www.mayerbrown.com.

Electronic Discovery & Records Management

Tip of the Month

Court-Initiated Pilot Programs and Model Rules in E-Discovery

Scenario

An organization is named as a defendant in a putative class action in the Southern District of New York. In-house counsel notices the long order that follows the complaint, including a twelve-page form that the parties are to complete regarding electronic discovery. In-house counsel is concerned about gathering all of that information so early in the litigation, and wonders if other courts are requiring similar early due diligence with respect to electronic discovery.

From Recommendations to Requirements

It is no secret that discovery costs, including the review and production of electronically stored information (ESI), frequently make up a substantial portion of the overall cost of a lawsuit. The Federal Rules of Civil Procedure, various corresponding state rules, and guidance from individual judges each try to reduce these costs by encouraging the parties to agree on plans for electronic discovery early in a dispute.

More recently, several courts at both the state and federal levels have promulgated standing orders, model orders or pilot programs to force litigants to organize and manage e-discovery early in the litigation and to cooperate with opposing counsel in developing an e-discovery plan. Counsel who are accustomed to postponing discussions of ESI may find their cases automatically subjected to orders that require rapid agreements on e-discovery issues.

Southern District of New York Standing Order

The US District Court for the Southern District of New York (SDNY) is one such court, having implemented Standing Order M10-468, *In re: Pilot Project Regarding Case Management Techniques for Complex Civil Cases in the Southern District of New York*, in November 2011 (the "Standing Order"). The Standing Order applies by default to class actions, multi-district litigation, and other specified types of claims. It sets forth the court's expectations in relation to electronic discovery during the initial pretrial conference and the parties' Rule 26(f) conference.

Topics for Initial Pretrial Conference

The Standing Order provides that at the pretrial conference, "[t]he parties shall provide the Court with a concise overview of the essential issues in the case and the importance of discovery in resolving those issues so that the Court can make a proportionality assessment and limit the scope of discovery as it

deems appropriate." To assist with this proportionality assessment, the parties must submit an Initial Report seven days before the conference. The Initial Report must include the following points relating to ESI:

- Possible limitations on ESI preservation, restoration, and production;
- Planned preservation depositions;
- A proposed protocol and schedule for electronic discovery; and
- Anticipated disputes over e-discovery and a proposal for how to resolve them.

Topics for Rule 26(f) Conference

The Standing Order calls for a more detailed filing based on the Rule 26(f) conference. Federal Rule of Civil Procedure 26(f) already requires the parties to discuss various issues regarding ESI; the Standing Order fleshes out those requirements with more specific expectations. The Standing Order includes a "Joint Electronic Discovery Submission" form, described as "a checklist of electronic discovery issues to be addressed at the Rule 26(f) conference." Parties would be well-advised to be prepared to cover all of those issues at the conference itself, including:

- **Preservation:** The agreed scope and methods of preservation, including "retention of electronic data and implementation of a data preservation plan; identification of potentially relevant data; disclosure of the programs and manner in which the data is maintained; identification of computer system(s) utilized; and identification of the individual(s) responsible for data preservation."
- **Search and Review:** The parties' positions on a variety of questions regarding how search will proceed, including: (i) the exchange of keyword lists, hit reports, and responsiveness rates; (ii) the potential use of concept searches, "machine learning" algorithms, and "other advanced analytical tools"; (iii) limitations on the fields and file types to be searched; (iv) plans for backup, archival, legacy, and deleted ESI; and (v) testing and sampling.
- **Sources of ESI:** The parties' positions on such contentious topics as "databases, instant messages, web sites, blogs, social media, ephemeral data, [and] electronically stored information in the custody or control of non-parties."
- **Forms of Production:** The agreed-upon production format, including plans for document types that will be produced in native format, such as spreadsheets.
- **Inadvertent Disclosure:** The parties' agreement, if any, regarding their ability to "claw back" inadvertently produced documents over which they claim a privilege.
- **Cost:** The parties are expected to "have analyzed their client's data repositories and have estimated the costs associated with the production of electronically stored information." The Standing Order also asks for the parties' positions on cost allocation and the reduction of discovery costs through shared discovery vendors and document repositories.

Best Practices

While the Standing Order only applies to SDNY cases, in many ways it embodies best practices for e-discovery generally. In fact, the SDNY Standing Order provides useful checklists for early ESI discussions regardless of the venue of the litigation. And parties should keep in mind that other jurisdictions, such as the Seventh Circuit and the Delaware District Courts, have implemented similar programs.

In general, the SDNY Standing Order embodies the judiciary's view that parties cannot simply say "I don't know" with respect to issues such as data retention, restoration of backup media, and other electronic discovery topics. More and more courts are implementing programs designed to force parties to educate themselves on e-discovery issues so as to engage in meaningful discussions regarding ESI with opposing counsel and the court early in a case. The SDNY Standing Order even requires counsel to "certify that they are sufficiently knowledgeable in matters relating to their clients' technological systems to discuss competently issues relating to electronic discovery or have involved someone competent to address these issues on their behalf."

A few simple practices can help companies prepare for obligations like those in the SDNY Standing Order:

- Document (and follow) e-discovery practices and policies.
- Maintain written document retention policies and a map of the company's data.
- Recommend that outside counsel become well-versed in e-discovery issues.
- Consider hiring dedicated discovery counsel to assist with e-discovery matters.

For inquiries related to this Tip of the Month, please contact Anthony J. Diana at adiana@mayerbrown.com, Therese Craparo at tcraparo@mayerbrown.com, or Zachary Ziliak at zziliak@mayerbrown.com.

Learn more about Mayer Brown's Electronic Discovery & Records Management practice or contact Anthony J. Diana at adiana@mayerbrown.com, Michael E. Lackey at mlackey@mayerbrown.com, or Ed Sautter at esautter@mayerbrown.com.

Please visit us at www.mayerbrown.com.

Electronic Discovery & Records Management

Tip of the Month

Data Mapping: Helping to Manage the Risks and Costs of Organizational Data

Scenario

During a litigation, a large company received discovery requests that were particularly focused on the company's electronically stored information (ESI)—e.g., email, document drafts, spreadsheets, and other material stored on the company's computer systems. However, the company's ESI was stored on multiple computer systems by various business units. The process of generating litigation holds and responding to the discovery requests was complicated by the company's need to access data from numerous, disparate sources. After the ESI was produced, plaintiffs complained that the production appeared incomplete in some parts and was duplicative in others. As a result, the company's general counsel wants to streamline the collection, review, and production of electronically stored information.

Organizing Information by Data Mapping

A data map is an index of a company's records and information systems. A data map can provide an easily accessible reference to determine where and how data is stored—particularly data that a company considers most valuable or most risky. For instance, when a company wishes to quickly locate information related to a customer, a data map offers a simple and comprehensive method to identify the multiple business units and information systems where such data may reside.

Benefits of Data Mapping

In addition to helping it better manage its records and information, data mapping can benefit a company in a variety of ways:

- More efficient document collection and review in litigation (and reduced risk of inadvertent noncompliance or underproduction);
- Faster and more accurate litigation holds;
- Stronger evidence that certain discovery requests are unduly burdensome or duplicative;
- Greater accuracy and consistency in discovery disclosures and responses;
- Enhanced management of data security, backup, and record retention policies;
- Improved compliance with legal and regulatory obligations;
- Improved communication and data-sharing between business units and with external service

providers; and

- Greater efficiency in business operations.

Data Mapping and Litigation

Data maps can simplify a company's compliance with discovery obligations imposed by the Federal Rules of Civil Procedure and similar state procedural rules.

- *Initial Disclosures.* A company with sound data mapping policies will have an easier time describing, by category and location, potentially responsive documents, electronically stored information, and tangible materials.
- *Meet-and-confer.* A company with a data map will be better prepared to meet and confer about discovery issues. A data map can also help to limit discovery to relevant sources and counter an opponent's demands for information that is not reasonably accessible.
- *Avoiding sanctions for information loss.* A data map showing data retention policies will aid a company with preserving and maintaining potentially responsive data.

Nuts and Bolts of Data Mapping

Designing, implementing, and maintaining a data map involves a company's legal, IT, and records management staff. Some companies engage an outside consultant to assist in the data mapping process. At a high level, the process of building a data map should include the following steps:

- *Reviewing existing data maps.* Various employees or business units may have already generated partial, *ad hoc* data maps for various purposes. These partial maps may be useful for obtaining an overview of a description of the data and where it is located.
- *Defining scope and level of detail.* Depending on the objectives of the data map, it may not be necessary or practical to map all of a company's data at the same level of detail. For instance, to decrease implementation and maintenance costs, a company may choose to map its most significant data systems in detail, but other systems with less granularity.
- *Identifying key sources.* A data mapping team should interview legal, IT, records management and business staff in order to determine which sources of data are most frequently responsive to litigation and other requests. These identified sources can constitute the focus of the data map.
- *Gathering information about the data.* A data map should reflect basic information about data sources, such as who created it, the custodian or owner of the data or system, what policies govern retention and maintenance, and how it can be preserved, collected and reviewed, if needed.
- *Understanding how data is used.* It is important to understand where a company's data is actually used and stored on a day-to-day basis. For instance, if employees regularly copy email or other documents to their local hard drives, that can be reflected on the data map. Similarly, employees may create *ad hoc* backups or secondary data systems that should be mapped as well. This information can be gathered through questionnaires, surveys, and face-to-face

interviews with a cross-section of employees.

- *Centralizing the data map.* Information should be imported into a central data map that can be easily accessed, searched, and updated. A data map can be created manually or can be created through a semi-automated process by using commercially available data management software.
- *Maintaining the data map.* The company should have a plan for updating the data map to reflect changes in the underlying information. Updates should be automated to the extent possible—a data map can become ineffective if updating it relies too heavily on manual effort.

A comprehensive data map can be a valuable asset, particularly with regard to high-value or high-risk data sources. Generating a data map may require substantial time and resources in the long term, but by focusing initially on high-priority data sources, progress can be made in the short term to help reduce legal risks, decrease discovery costs, and enhance records management and data security policies.

For inquiries related to this Tip of the Month, please contact Michael E. Lackey at mlackey@mayerbrown.com, Kim A. Leffert at kleffert@mayerbrown.com, or David Fang-Yen at dfang-yen@mayerbrown.com.

Learn more about Mayer Brown's Electronic Discovery & Records Management practice or contact Anthony J. Diana at adiana@mayerbrown.com, Michael E. Lackey at mlackey@mayerbrown.com, or Ed Sautter at esautter@mayerbrown.com.

Please visit us at www.mayerbrown.com.

March 2012

MAYER·BROWN

Electronic Discovery & Records Management

Tip of the Month

Automating the Legal Hold Process

Scenario

For the past few years, a manufacturing company has seen its volume of litigation increase significantly. While the company's legal department has a manual process in place for issuing and monitoring legal holds, the increase in litigation is making this manual process more difficult to manage. In particular, there have been issues with the Information Technology, Human Resources and Records Management departments regarding their routine practices and communications with the Legal Department about custodians on legal hold. The company is considering ways to improve the process through some type of automation.

Is Implementing New Technology the Right Answer?

The concept of an "easy button" for legal holds is very appealing, especially for overburdened in-house counsel and senior executives looking to simplify the process and manage costs. As with other too-good-to-be-true solutions, there is no such button. Technological solutions bring with them a new layer of complexity, in particular because such solutions may impact so many aspects of the organization's business. That said, technology can help to automate, streamline and consolidate the legal hold process under the right circumstances. But before investing in any type of technology, it is important for the organization to develop a systematic approach to evaluating the pros and cons of the proposed solution.

Developing a Systematic Approach

The first step is identifying the right people to include in the conversation. At many organizations, those people include far more than the Legal Department. Other groups to consider include: Information Technology, Information Security, Human Resources, Procurement, and Records Management/Information Governance. The legal hold process and the implementation of an automated tool impacts each of these groups in different ways.

The next step is understanding the organization's real needs when it comes to legal holds: exactly what problem is the organization trying to solve? The answer to that question may very well dictate the appropriate solution.

Finally, the organization needs to develop a clear plan for evaluating the available technology and whether it is truly suited to meet the organization's needs. When it comes to developing that plan,

there are a number of factors that are critical to consider in order to ensure success.

Factors to Consider

- **Litigation Risk Profile**. The investment and the return on investment (ROI) of an automated legal hold tool is directly tied to the number of legal holds and the number of people on the typical legal hold. For highly regulated serial litigants, the ROI of implementing an enterprise solution behind the firewall may be quite high. For the organization facing run-of-the-mill employment and contract actions, with only the occasional more-complex litigation, a web-based, case-by-case legal hold tool may be entirely sufficient and certainly an upgrade from the "spreadsheet and email" approach to managing legal holds.
- **Budgeting and Procurement**. When considering a significant investment in the more advanced technology solutions, budgeting is a major consideration. Legal can often obtain the necessary budget through Information Technology if Legal can convince the Information Technology leaders that the automated legal hold tool will improve the routine operations of the organization's systems and save money. A similar approach may work with Information Governance if you know that there is an ongoing or upcoming information governance project. Keep in mind that if Information Technology or Information Governance are involved, the organization's Procurement Group is likely to be involved as well.
- **Compatibility with Existing Systems**. Possibly the most important factor to consider when selecting a legal hold technology is whether that technology will be compatible with the organization's existing system. The systems to consider include:
    - Human Resources Databases
    - Document Management Systems (including archives)
    - Asset Management Systems
    - Research/Financial Databases
    - Email Systems
    - Compatibility/Interface with Outsourced IT Providers
- **Information Security**. If an organization considers a web-based "software as a service" (SaaS) option, it is particularly important to take data security into consideration. An SaaS option opens a portal into the organization's infrastructure, creating at least some risk of a data breach or a cyber attack. Evaluating the security and integrity of the provider's networks, backup procedures and redundant layers of data protection, as well as the provider's security protections and audit procedures, is critical to determining whether the service provider can offer the level of data protection the organization requires.
- **Integration**. A major benefit of an automated tool is enhancing the integration of the legal hold process throughout the organization.
    - *Business Personnel*. An automated tool can streamline and simplify communications between Legal and the business personnel subject to the legal hold. Such tools can assist with distribution of legal hold memoranda and reminder memoranda, specific instructions for preservation and collection, questionnaires, and the tracking/auditing process.
    - *Information Technology.* When selecting an automated legal hold tool, it may be helpful to consider access to that system, including whether Information Technology can be provided with visibility into key information stored within that tool. The organization may also want to consider whether the tool can be configured to accommodate the unique

identifiers used by Information Technology when referring to individual custodians. Having visibility into such information helps Information Technology to ensure that its routine business operations do not conflict with legal hold obligations, including with respect to departing employees, upgrades to software/technology, and break/fix.
    - *Human Resources.* With Human Resources, integration of the legal hold tool and the Human Resources database can significantly minimize the risk associated with departing or transferring employees on legal hold. Such tools can automate the notification process among Human Resources, Legal and Information Technology.
    - *Information Governance.* Information Governance is often responsible for enforcing an organization's data retention policies, including purge or janitorial functions (especially in archives and document management systems). Automatic integration between the legal hold tool and those systems can protect against the inadvertent loss of data.
- **Functionality**. Not every organization needs the Cadillac of legal hold tools. These tools range in functionality from simple notification and tracking to preserve-in-place to preserve-by-collection. An organization needs to determine how the tool fits into the existing legal hold process and whether the added costs often associated with the advanced functionality makes sense.
- **Unintended Consequences**. Even the best tools may have unintended, or unexpected, consequences and considering those possibilities in advance can assist with long-term planning. For example, the more advanced the functionality of the tool, the more likely it is that significant internal resources may be needed to maintain and manage it. Similarly, an organization may want to consider the burden of integrating historical holds into the new legal hold tool and plan accordingly. In addition, while the ability to more easily identify and capture data for preservation may seem like a strong upside, it can also lead to the retention of greater volumes of duplicative data depending on how the tool implements preservation rules.

For inquiries related to this Tip of the Month, please contact Anthony J. Diana at adiana@mayerbrown.com, Therese Craparo at tcraparo@mayerbrown.com, or Patrick Garbe at pgarbe@mayerbrown.com.

Learn more about Mayer Brown's Electronic Discovery & Records Management practice or contact Anthony J. Diana at adiana@mayerbrown.com, Michael E. Lackey at mlackey@mayerbrown.com, or Ed Sautter at esautter@mayerbrown.com.

Please visit us at www.mayerbrown.com.

April 2012

MAYER·BROWN

Electronic Discovery & Records Management

Tip of the Month

Best Practices in Collecting Data: Who To Do It, When To Do It, How To Do It

Scenario

A putative class action complaint has just been filed against a large company. After distributing a legal hold, the general counsel considers who should be in charge of the eventual collection of documents, including electronically stored information (ESI), when the collection process should begin, and how the collection process should operate in order to be efficient and effective.

Why Worry About Collecting Data?

Collecting data, including ESI, can be a daunting task. Counsel's collection and production obligations often can go far beyond e-mail servers and archives. Depending on the claims and defenses in a dispute, a company may have to produce ESI from a wide variety of additional computer systems and media, including: hard drives of laptop and desktop computers; PDAs and smartphones; various removable media such as flash drives; personal network storage locations assigned to individuals; shared network storage locations assigned to departments or business units; various software applications and associated databases; and sometimes even telephonic and voice mail systems or instant messages.

Ensuring that ESI is properly collected requires a plan designed to meet basic discovery objectives, overcome claims of under-collection, allow for the processing of data for review and production, and ensure the admissibility of the evidence if necessary.

Who Should Collect Data?

The first choice that a collecting party faces is whether to do the collection internally or to outsource the process to a specialized vendor. The appropriate decision will vary based on the frequency with which the party finds itself in litigation, the financial stakes of the current litigation, and the breadth of the issues in play.

A frequent litigant may want to bring ESI collection in house, where an investment in software tools that enable document collection and personnel to manage the process can ultimately save money over the course of repeated litigations. An infrequent litigant may be better served by bringing in an outside vendor retained to collect data in an efficient and defensible manner, rather than diverting IT staff, who may be unfamiliar with the objectives of collecting data, from their regular functions.

Outsourcing the collection process is not an all-or-nothing decision, however. As a middle ground, companies may invest in ESI collection software and contract with the software vendor or another entity to provide the personnel and technology for certain tasks, such as collections from relational databases or other large scale collections. In this way, the litigant can outsource some portions of the collection process while retaining direct control over others.

When Should Data Be Collected?

Unlike in the days of exclusively paper discovery, where it was common practice to await discovery requests before collecting evidence, the current Federal Rules (and the nature of ESI) require a much earlier commitment to collection of data. Indeed, given the difficulty and risk involved in enforcing a legal hold that relies on preserving ESI 'in place', litigants increasingly are "collecting to preserve" at the outset of litigation.

This approach combines the identification of potentially relevant information with the storage of that information in an appropriate and defensible manner. In addition, given that a more detailed review of individual sources of ESI typically accompanies the collection effort, early collection can reveal unforeseen sources of data.

Front-loading collection can come with a cost, including the expense of organizing and maintaining data long before, if ever, it is produced. Thought can be given to collecting some data, including data responsive to Rule 26(a) initial disclosures, early in the litigation and collecting other data, such as data responsive to a putative class that has yet to be certified, later in the case.

How Should Data Be Collected?

A litigant need not collect every e-mail, electronic document, backup tape or shred of paper it possesses. Understanding the kinds of data to be collected helps a litigant to prepare a collection plan. For example, data collection should be conducted in a manner that considers how the particular data is kept in the ordinary course of business for several reasons. First, the processing for review and production of different types of ESI—e-mails vs. spreadsheets, for example—can differ. Second, the default form of production for ESI under the Federal Rules is the form in which the data is ordinarily maintained. The collection process can also consider whether steps should be taken to collect any metadata associated with collected files. In some instances, the collection of metadata is essential; for other kinds of ESI, the collection of metadata is either unnecessary or unduly burdensome.

Further, especially when collection is done early in the case, it is not always possible to limit the collection with a defensible set of search terms. Therefore, litigants often opt to collect *all* ESI from key custodians, and to cull unneeded files later. However, one can limit the ESI collected by using "exclusionary" restrictions; that is, collecting all files *except* those that satisfy particular filtering criteria. For instance, it is generally appropriate to exclude the collection of system files and executables, as these rarely contain responsive information. Likewise, it is often appropriate to exclude data that has been "deleted" but still resides in fragmented form or in slack space on a hard drive.

Once collected, the data is best placed in a "write once, read many" format, such as a recordable CD or DVD, to ensure that the files and associated metadata, if any, are not inadvertently modified. Collected

data is then typically processed, either internally or by an outside vendor, for review and production.

What's the Takeaway?

Planning for collection of ESI ideally starts before litigation. Planning early allows a company to choose an optimal combination of in-house resources and outside vendors to efficiently handle collection of ESI. Once litigation has started, it is often best to collect ESI early and to use a collection methodology intended to maintain the integrity of the data but is also relatively easy and inexpensive to process for review and production. Employing exclusionary restrictions to limit collection can be effective when used at an early stage of litigation.

For inquiries related to this Tip of the Month, please contact Anthony J. Diana at adiana@mayerbrown.com, Kim Leffert at kleffert@mayerbrown.com, or Frank Dickerson at fdickerson@mayerbrown.com.

Learn more about Mayer Brown's Electronic Discovery & Records Management practice or contact Anthony J. Diana at adiana@mayerbrown.com, Michael E. Lackey at mlackey@mayerbrown.com, or Ed Sautter at esautter@mayerbrown.com.

Please visit us at www.mayerbrown.com.

May 2012

MAYER·BROWN

Electronic Discovery & Records Management

Tip of the Month

Managing the Risks and Costs of Email Archives: *Part I - Initial Considerations & Functionality*

Scenario

Several years ago, a large multinational corporation implemented an email archive system in order to better manage its volume of email and the potential complications associated with backup media in its frequent litigations. Now, the corporation's General Counsel is concerned about the volume of email that must be searched, processed, reviewed and produced in every litigation, and the Chief Information Officer has realized that the exponential growth of the email archive system is not sustainable. The corporation is exploring ways to manage the risks and costs associated with its existing email archive.

Benefits and Risks of Email Archives

There are a number of benefits associated with email archives and, when managed properly, such archives can be an important asset to any organization. However, they can become a liability if not properly implemented and managed.

First, email archives often make business and IT operations more efficient and cost-effective. *Second*, email archives can be useful—and are often necessary—for enforcing regulatory or other legal requirements relating to the retention of records. *Third*, email archives can help consolidate email in a central location. This can make managing, searching and collecting relevant email more efficient and cost effective. *Fourth*, email archives can facilitate the implementation and management of legal holds. These systems minimize the risk of loss of data necessary for legal purposes by placing control of such data in the hands of the organization, rather than the individual.

With that said, no technology offers a perfect solution to data management. It is, therefore, important to be mindful of the risks posed by the use of email archives. *First*, the functionality promoted by many providers has often been tested only on a small volume of data. Organizations frequently find that when such systems are subjected to data volumes typically found in large organizations, functionality is lost or its effectiveness is decreased. *Second,* the idea of retaining all email and reducing the risk of loss may be appealing, until you consider the implications. The volume of email can quickly become unmanageable. And the mantra that "storage is cheap" is simply not accurate. Storage is not cheap when an organization is retaining all email, nor is it cheap to manage that data and the resulting risks of keeping the data longer than is needed for business or legal reasons. *Third*, much of the data flowing through an organization's systems is not needed for either business or legal reasons. But an email

archive does not make substantive judgments about whether a particular message is critical to business operations, or is just junk. *Fourth*, limitations in email archive technology often do not allow for easy deletion or extraction of data. Being able to retain data easily where necessary is helpful, but only if you can manage the data after it has been ingested into the email archive just as easily.

Understanding the Purpose of an Email Archive

The most important step in properly implementing and managing an email archive system is understanding why the organization is acquiring (or has acquired) the email archive in the first place. Does the organization have regulatory or other legal obligations that it needs to meet? Is the organization primarily looking to be able to better manage its email? Or is the organization concerned about the risk of loss of critical email? The answers to these questions will inform the appropriate use of the email archive. And when it comes to minimizing risk and maximizing effectiveness, there are a number of factors to consider.

Factors to Consider

- Reality Check. As with any technology, email archives cannot necessarily do all of the things that they purport to do. Understand from the outset that email archives require thoughtful planning and management to be effective. Know your organization's priorities and goals, and choose your email archive, or any upgrades to such systems, accordingly.
- Data Volume. In addition to understanding the volume of email flowing through your organization, it is important to understand how the applicable email archive system retains email. Does the system retain a single instance of each email by archive, by server or by retention folder? Understanding how much redundancy is built into the email archive under normal conditions may provide insight into how much email will ultimately be retained by the email archive—and whether it is truly necessary for business or legal purposes.
- Legal Holds. Many email archive systems offer some functionality to place data on legal hold. Your organization should also understand how the email archive system handles data placed on legal hold. Is data placed on legal hold on an employee-basis or document-basis? How much time and effort is required to identify data for legal hold, and does that time and effort increase as the data volume increases? Is a copy of the data created for each legal hold, or does the system mark an item for hold and associate that item with separate legal holds, as needed? Must data put on hold be "evergreen," e.g., does the system automatically begin to retain all incoming and outgoing email for an individual put on legal hold on a going-forward basis? How easy is it to lift a legal hold once a matter is ultimately concluded? For serial litigants, the legal hold function of an email archive can result in exploding data volumes that the system may not be equipped to handle.
- Retention Requirements. Remember that email archives do not have to be an all-or-nothing proposition. It is wise to consider a "risk-based" approach when implementing an email archive. That is, an organization can utilize an email archive without saving every email sent or received by its employees. And with most email archives, the organization can enforce different retention periods for individual employees in particular departments or groups. Consider whether enforcing different retention periods for different employees within the email archive would be

useful for your organization, and whether email for certain low-risk employees should be excluded from the email archive.

- Search. One of the key benefits of an email archive is the ability to consolidate and search an organization's email in a central location. The impact of that benefit, however, may depend on the system's search functionality. Consider what type of basic searches the system allows, e.g., by employee name, key words, dates, etc., whether the system facilitates filtering to identify and remove "junk" emails, and whether the system allows more complex Boolean searches. In addition, make sure to ask whether the system searches email attachments.
- Extraction. Be sure to evaluate the process involved with extracting data from the email archive, including the time and effort required and the parameters of such extraction. If extracting the data will be a significant burden on the organization, then the value of retaining that data will be diminished.
- System Requirements. Remember that the use of an email archive system does not, on its own, alleviate all prior risks associated with email. For example, even with an email archive, critical email may end up decentralized if individuals are able to save email to PSTs stored on hard drives or other locations. Evaluate all document retention and records management policies and how those policies are impacted (or not impacted) by the email archive, to make sure the organization has controls in place to manage the risks associated with email where the email archive does not.

This is Part One of Two in a set of Tips of the Month addressing email archives. The Tip of the Month for June will address preserving, searching, collecting and producing data from email archives.

For inquiries related to this Tip of the Month, please contact Anthony J. Diana at adiana@mayerbrown.com or Therese Craparo at tcraparo@mayerbrown.com.

Learn more about Mayer Brown's Electronic Discovery & Records Management practice or contact Anthony J. Diana at adiana@mayerbrown.com, Michael E. Lackey at mlackey@mayerbrown.com, or Ed Sautter at esautter@mayerbrown.com.

Please visit us at www.mayerbrown.com.

Electronic Discovery & Records Management

Tip of the Month

Managing the Risks and Costs of Email Archives: *Part II: Preservation, Collection & Production*

This is Part Two of Two in a set of Tips of the Month addressing email archives. The tip of the Month for May addressed initial considerations and functionality relating to email archives.

Scenario

A large multinational corporation journals all incoming and outgoing employee emails in an email archive system in order to better manage email volume and the potential complications associated with backup media in its frequent litigations. For each legal matter requiring the production of documents, the corporation must preserve, search, retrieve and produce large volumes of email from the archive. The corporation is beginning to realize just how time consuming, cumbersome and subject to error this process can be, and is evaluating ways to better manage the process in future litigation.

Understanding the Challenges of Email Archives in Legal Matters

Email archives can be useful to an organization in many ways. For example, they can assist with regulatory compliance and with email consolidation to streamline preservation and collection in connection with legal matters. However, many email archives were primarily designed to enable consolidation and retention of email, not to preserve an individual employee's email, search and retrieve emails for litigations or to provide a defensible email deletion program that is consistent with an organization's policies and legal obligations. This deficiency can cause several challenges to managing the preservation, collection and production of email from email archives in a cost-effective way.

First, discovery, whether in federal or state court, remains largely focused on the concept of data associated with a "custodian." A custodian is traditionally understood to be an individual employee of the organization who has access to, and stores, information related to the operations of the organization. Parties to a litigation often spend significant time and effort identifying relevant custodians and discussing how to associate responsive data with that custodian. Email is a classic example of data considered to be associated with a particular custodian.

This use of the term custodian, however, is a misnomer when it comes to email archives. Email archives do not generally store email by custodian. Email archives generally store email based on the concept of applicable retention periods and limited duplication. Thus, in the case of an email archive,

the "custodian" is the archive itself, not the individual employee. Thus, when an organization searches for an employee's email in an email archive, what the organization is really doing is running searches on certain metadata fields in the email archive using that employee's name or email addresses as keywords.

Second, the search capabilities of email archives are often limited—allowing for only the most basic of searches, such as searches by date or simple keywords. In addition, some archives are limited in the type of documents they can search. For example, some email archives search the text of an email, but not the content of any email attachments, while other email archives may be able to search some email attachments, but may not be able to search certain types of email attachments (e.g., older PDFs or facsimiles that are not readable).

Third, searches in email archives must often be conducted sequentially, i.e., the email archives cannot conduct more than one search at a time. Nor can an email archive "tag" or otherwise identify a document that has already been collected for a particular legal matter. This means that when an organization conducts more than one data collection for the same legal matter using employee names/email addresses or keywords, the organization invariably is collecting duplicate data. This result can translate into significant additional costs to the organization in the processing of that data for review.

Fourth, in many cases, organizations use email archives that are maintained and serviced by a third-party vendor. While the organization may technically "control" the email in a legal sense, the organization is nonetheless limited in its ability to expedite or control the search and retrieval. Given the large volumes of data that are often maintained in an email archive, the search limitations imposed by the architecture of such email archives and the effort required to extract that data, the collection and retrieval process can take weeks or months for just one search and collection request.

Finally, email archives are, in essence, large databases of information. Those databases are fallible. Most email archives experience the corruption of a certain percentage of the data they retain in the ordinary course of business. Email archives do not, therefore, contain 100 percent of all emails flowing through the organization's systems. Moreover, when searching through massive amounts of information, and retrieving vast quantities of data, technical failures may arise. This often means that the search and retrieval of emails from an archive is a manual process, requiring significant hours by employees to ensure that the archive is functioning correctly.

Best Practices for Managing Search and Retrieval from Email Archives

Understanding the operation and limitations of email archives is an important step in managing those archives when it comes to search and retrieval of data for legal purposes. It is also critical in properly communicating with opposing counsel or the court when it comes to collection and production in connection with a particular legal matter.

- Plan Your Collections. Once you understand the operation of the organization's email archive, plan your collections accordingly. Consider how to minimize duplication in collections and how to most efficiently and effectively search for responsive emails. And be prepared to discuss your collection methodology—including any limitations to the email archive's search capabilities and

how your methodology addresses those limitations—with opposing counsel.

- Custodians. In many document productions, the parties negotiate the deduplication of the collected data and how custodian information may be preserved, collected and produced in conjunction with such deduplication. Be prepared to discuss the concept of "custodian" when it comes to email archives with the court or opposing counsel. It may be less burdensome—and more accurate—to identify the archive itself as the custodian of any email retrieved (in the custodian metadata field of the load file), and to rely on the names listed in the "to," "from," "cc" and "bcc" fields to identify who sent or received the email. Collecting the email data from the archive for a group of employees at once (which may eliminate the need for deduplication) may also confuse your outside e-discovery vendor and opposing counsel, and impair your processing and review workflow. Planning is critical to avoid an ad hoc approach during the pendency of a litigation or investigation.
- Timing. Be aware of the time it is likely to take to retrieve email from the organization's email archive, and be sure to communicate that potential time frame to legal counsel. It is critical to make sure that any representations to the court or opposing counsel take into consideration the time it will take to actually obtain the necessary data.
- Investing in Technology. Most archive vendors are developing new technology to help manage the legal hold and collection process. There may be a significant return on investment for such technology, but be sure to understand how the new technology functions and whether it actually makes the way your organization presently manages legal holds and collections more cost effective.

This is Part Two of Two in a set of Tips of the Month addressing email archives. The Tip of the Month for May addressed initial considerations and functionality relating to email archives.

For inquiries related to this Tip of the Month, please contact Anthony J. Diana at adiana@mayerbrown.com or Therese Craparo at tcraparo@mayerbrown.com.

Learn more about Mayer Brown's Electronic Discovery & Records Management practice or contact Anthony J. Diana at adiana@mayerbrown.com, Michael E. Lackey at mlackey@mayerbrown.com, or Ed Sautter at esautter@mayerbrown.com.

Please visit us at www.mayerbrown.com.

July 2012

MAYER·BROWN

Electronic Discovery & Records Management

Tip of the Month

Selecting And Working With An E-Discovery Vendor

Scenario

A multinational construction company receives a wide ranging subpoena from the US Department of Justice demanding the production of a variety of documents maintained at various locations inside and outside the United States. That same day, the company's US affiliate receives a complaint filed in state court seeking damages for a relatively minor injury that occurred on one of the company's construction sites in Texas. The company intends to select an electronic discovery vendor to assist with the discovery process in both matters.

Considerations When Choosing an Electronic Discovery Vendor

The range of choices of electronic discovery vendors keeps increasing: with both a proliferation of small niche vendors on one hand and a significant expansion of services by a handful of soup-to-nuts vendors on the other. Many smaller vendors focus on one part of the process, such as converting paper records using optical character recognition (OCR) and coding, while other large vendors have invested heavily in infrastructure to provide capacity, reliability, fault tolerance and geographic availability. Some vendors now offer "cutting edge" technologies intended to streamline the process, such as predictive coding for document reviews. Choosing the right vendor can be essential to a successful discovery outcome.

For smaller, localized cases, a specialized vendor may be appropriate. For complex matters, where discovery may help determine criminal penalties or fines, a larger, integrated provider may be more appropriate.

The following issues should be considered when deciding what type (or types) of electronic discovery vendor to retain:

- **Existing state of the company's information management system.** If a company already has an effective document management system, and the scope of the discovery is small and well-defined, the need for expert help from a large, integrated vendor may not be required. Conversely, if organizing, collecting, reviewing and producing responsive files may be complicated by a less-than-fully integrated document management system, wide geographic distribution of salient records, or potentially broad scope, a small, localized vendor may not provide sufficient coverage or services to meet all of the company's discovery needs.

- **Time.** If the company must quickly produce all relevant files, then a larger, more sophisticated vendor may be the prudent choice.
- **Chain of custody.** As with physical evidence in a civil or criminal case, it often can be critical to establish and maintain a clear, unbroken chain of custody for each file from every custodian. Such chains of custody can be easier to maintain and prove with a single integrated vendor than with several vendors each retained to perform discrete tasks. In any case, no matter what type of vendor is selected, counsel should supervise the process to help ensure the appropriate chain of custody is maintained.
- **Proportionality** The importance of the matter is a critical factor. The potential for criminal penalties or sanctions may prove a determining factor in deciding in favor of a particular type of vendor and the costs expended on discovery.
- **Cost.** An electronic discovery vendor's fees and fee structure varies based on the size of the task, the complexity of the processing and the speed in which completion is needed, among other factors. A major customer of a large electronic discovery vendor may be able to negotiate a mutually agreeable fee structure that reflects economies of scale. However, not all litigation needs a full-service electronic discovery vendor, and, in some cases, it may be more cost effective to choose a local, niche vendor.

Irrespective of which vendor is selected, when working with an electronic discovery vendor, counsel should keep the following issues in mind:

- **Preservation and Collection.** If the decision is made to copy data as a means of preservation, counsel and the vendor should work together with the goal of ensuring that the data cannot be altered, deleted or destroyed, and that a copy is created and maintained in a forensically sound manner. Counsel also should work with the vendor to identify and collect potentially responsive sources of data in a forensically sound manner. Counsel should be aware of and work with the vendor to ensure data privacy laws, to the extent implicated, are appropriately addressed.
- **Data Culling.** Effective data culling can dramatically reduce the volume of data that needs to be processed, thus potentially reducing production and review costs. Counsel and the vendor should work together to ensure data is culled and de-duplicated, but that all nonduplicative potentially responsive sources collected are reviewed.
- **Processing.** Once files are collected and culled, they should be processed, searched for privilege, and sorted by type or topic, and, in some cases, separated into smaller units for review. It has been estimated that approximately 80 percent of the time, and 80 percent of the cost, devoted to electronic discovery is spent in processing, review and analysis; therefore, having powerful workflow tools to manage this part can be critical to managing scarce resources.
- **Review.** A number of vendors provide software designed to simplify the review and analysis of data. Careful consideration should be given to finding the tools best suited to counsel's needs, which may differ from case to case.
- **Production.** Generally, the goal at the production phase is to be able to deliver data in a useable format to other parties, to a court or to a regulatory agency. Vendors often work with various litigation support applications, and counsel and the vendor should work together to ensure that appropriate production formats are used (e.g., load files or "native" production formats). Counsel and the vendor also should discuss potentially unforeseen consequences

associated with the chosen production format(s), such as the potential effects on metadata or any changes to document integrity.

Conclusion

There is no one 'right' answer when choosing an electronic discovery vendor. Consider working with vendors of different sizes and service offerings to provide the right solution for the specific litigation or investigation.

For inquiries related to this Tip of the Month, please contact Anthony J. Diana at adiana@mayerbrown.com, Kim A. Leffert at kleffert@mayerbrown.com or Robert E. Entwisle at rentwisle@mayerbrown.com.

Learn more about Mayer Brown's Electronic Discovery & Records Management practice or contact Anthony J. Diana at adiana@mayerbrown.com, Michael E. Lackey at mlackey@mayerbrown.com, or Ed Sautter at esautter@mayerbrown.com.

Please visit us at www.mayerbrown.com.

August 2012

MAYER·BROWN

Electronic Discovery & Records Management

Tip of the Month

Effectively Managing a Large-Scale Document Review

Scenario
A multinational company is in litigation with multiple parties regarding a patent dispute. Due to the breadth of the claims and the complexity of the issues involved, the parties expect to produce millions of documents in discovery. With merits depositions scheduled to take place in the upcoming months, the multinational company must engage in a comprehensive document review to produce documents, prepare its witnesses and refine its litigation strategy.

Goals of the Document Review
Every document review has unique components that reflect the issues involved in the case. However, the document review team typically strives to achieve accuracy, efficiency and diligence.

First, the review team strives for an accurate review by locating and itemizing documents responsive to the discovery requests and the parties' theories of the case.

Second, using the appropriate tools together with an organizational review structure, the review team seeks to winnow the production in an intelligent, efficient and cost-effective manner.

Finally, the review team works diligently to attempt to minimize the risk of errors in the review process that could result in a waiver of privilege, the dissemination of proprietary information without the proper confidentiality designation or missing important documents.

Preliminary Assessment
Although a document review is often time-sensitive, it is important to have the ultimate review goals in mind before beginning the review process. This can be achieved by conducting a preliminary assessment that considers the following items:

- The nature of the case and the objectives of the review;
- The volume of documents, including electronically stored information, to be reviewed;
- The form the review will take (electronic or hard copy);
- The form in which documents will be or have been produced;

- The establishment and implementation of quality-control procedures; and
- The anticipated production and/or discovery schedule.

Keeping these components in mind, as well as other case-specific issues, will help the review team to achieve an accurate, efficient and diligent review.

The preliminary assessment stage is a good time to consider the review platform and which vendor to use for the review. It is also an appropriate time to consider whether contract lawyers, a party's internal or external lawyers, or some combination, will be doing the actual review. This is also a good time to learn about any technological issues or quirks of how a party keeps or collects its documents that may affect the review or the choice of review tool.

The final step in the preliminary assessment is to consider the available review options, taking into account the prevalence of electronically stored information. For example, the document review may consist of: (i) native files, (ii) hard copy documents, (iii) a litigation support database such as Concordance, (iv) an online repository that is either vendor-provided or client-proprietary or (v) a combination of the foregoing. In deciding which option(s) to choose, it is helpful to keep in mind the goals discussed above and take into account the size and experience of the review team. Additionally, consideration of the internal resources available, including network storage space, bandwidth and case room availability, can be made.

Review Phase

Before the review team can begin its review, it is recommended that each team member be informed of the review plan. Elements of the review plan can include:

- A statement of the issues and anticipated review deadline;
- A description of the rules for the review and how the review should be administered (i.e., subsets of documents, tagging procedures, document families, privilege and confidentiality issues);
- A description as to how progress will be tracked for each attorney and for the review as a whole (i.e., "reviewed" tag, subsets of documents);
- A list of criteria for the reviewers to use in categorizing a document into files (i.e., "relevant" tag, specific issue tags, "privilege" tag, "hot" or "key" documents); and
- A specific statement of the estimated time and staffing requirements for completing the review in an efficient manner. If possible, additional time can be built into the time estimate to allow for unforeseen problems and more complicated documents.

Quality Control Procedures

Even with an experienced review team, it is important to ensure that quality-control processes are also implemented. The use of quality-control processes can provide information to help determine early on how best to organize the review to maximize quality and efficiency. Additionally, quality-control processes also assist in the identification of potential ambiguities and/or gaps in the review plan which

might result in errors or other issues. Some quality control processing includes:

- A second-tier review on some, or all, of the documents reviewed;
- A statistical analysis on the documents reviewed to check consistency and a second-tier review on the categories of documents that show unexplained statistical variations; and/or
- A targeted second-tier review on specific documents addressing issues most central to the case.

Conclusion

Although every document review involves its own set of challenges, it is a crucial aspect in the discovery process and in developing a litigation strategy. As such, the document review team should strive for an accurate, efficient and diligent review. By performing a preliminary assessment, and implementing quality-control processes, the review team can minimize unexpected problems and provide a high-quality, efficient, cost-effective document review.

For inquiries related to this Tip of the Month, please contact Anthony J. Diana at adiana@mayerbrown.com, Kim Leffert at kleffert@mayerbrown.com or Richard Nowak at rnowak@mayerbrown.com.

Learn more about Mayer Brown's Electronic Discovery & Records Management practice or contact Anthony J. Diana at adiana@mayerbrown.com, Michael E. Lackey at mlackey@mayerbrown.com, or Ed Sautter at esautter@mayerbrown.com.

Please visit us at www.mayerbrown.com.

Electronic Discovery & Records Management

Tip of the Month

Managing the Risks and Costs of E-Discovery in Class Actions

Scenario

A large manufacturing company is a defendant in a putative nationwide class action lawsuit. The putative class will most likely number in the thousands, or tens of thousands, of consumers, resulting in potentially significant damages and expensive electronic discovery costs for the company. The few named plaintiffs, on the other hand, are likely to have a relatively small number of documents. The company is confident in the merits of the case, but is concerned that it will not have sufficient leverage to negotiate reasonable limits to discovery and is considering settlement in order to avoid the costs and burdens of an extensive electronic discovery effort.

Understanding the Challenges of E-Discovery in Class Action Lawsuits

In class action lawsuits, discovery is typically one-sided. The defendants are frequently large organizations with significant volumes of electronic data, while the plaintiffs are frequently a large group of unnamed individuals represented by a few named plaintiffs with a small amount of electronic data. As a result, the potentially exorbitant costs associated with discovery in a class action lawsuit fall almost exclusively on the defendant. This situation can create disincentives for the parties to work together to resolve discovery disputes, and it poses the risk that class action defendants will face unfair pressure to settle even meritless claims to avoid those discovery costs. Electronic discovery magnifies the extent of the disproportionate impact on class action defendants.

In evaluating how best to manage discovery in class action lawsuits, it is useful to keep in mind the unique characteristics associated with those actions that impact discovery issues. First, with the exception of the few named plaintiffs, the putative class members are largely unknown and may be difficult to identify, especially prior to class certification. This is particularly true when the putative class is poorly defined and may encompass thousands of unknown employees or customers. Determining the scope of preservation in such circumstances can be challenging. For example, it may be difficult to identify and preserve communications with a putative class member if the identity of that putative class member is unknown. Second, pre-certification discovery may be necessary when facts relevant to the certification requirements are in dispute. Courts are often willing to bifurcate discovery related to class certification and discovery related to the merits of the case. Third, merits-related discovery may be unnecessary depending upon the outcome of the certification dispute. In fact, courts generally discourage merits discovery prior to class certification in order to avoid superfluous costs (unless, of

course, the discovery also relates to the certification of the class).

Strategies for Managing E-Discovery in Class Action Lawsuits

Despite the inherent imbalance associated with e-discovery in class action lawsuits, there are strategies that can help manage the scope and control the costs of such discovery.

- **Preservation**: The challenges associated with determining the scope of preservation for a class action lawsuit often lead counsel to submit to costly and burdensome over-preservation to avoid even the appearance of a failure to preserve. But the costs and risks (both legal and business-related) of over-preservation grow exponentially the longer the litigation persists, and there will always be some risk that, despite diligent efforts, an organization will inadvertently fail to preserve relevant information. The organization and its counsel should carefully weigh the costs and risks of extended over-preservation, and its impact on the organization's business, against the costs and risks of defending a process in which reasonable steps are taken to determine the scope of preservation based on the available information. In some cases, it may be prudent to consider raising preservation issues with opposing counsel or the court early in the litigation in an effort to narrow, or at least define, the scope of preservation.

- **Bifurcating Discovery**: The difficulties associated with attempting to preserve data for an unknown group of putative class members demonstrate the benefits of bifurcating class certification discovery and merits discovery. By conducting targeted discovery directed at enabling the court to define (or deny) class certification, the parties may be able to reduce or avoid costly and extraneous merits discovery. Even where merits-related discovery is permitted prior to class certification, the organization should consider advocating for restrictions that narrow the scope of early merits discovery to issues that are closely related to class certification or to groups, subjects or time periods that are the most likely to survive class certification.

- **Be Creative**: When the burdens of e-discovery fall almost exclusively on one party, it is easy to assume that negotiation and cooperation are not feasible. But by cooperating with opposing counsel to facilitate discovery and offering creative solutions to burdensome discovery problems, an organization can position itself to seek relief from the court should class plaintiffs prove to be unreasonable. Moreover, offering strategies that streamline and expedite discovery, while still providing the class plaintiffs with the information requested (if not every document containing that information), may even appeal to opposing counsel. For example, when it comes to class certification discovery, it may be more efficient and cost-effective to produce reports from an organization's structured databases summarizing the information requested than to attempt to find every individual electronic document relating to an undefined class of individuals.

- **Consider Cost-Shifting**: Typically, in federal litigation, the producing party bears its own costs of discovery. However, in some circumstances, courts have been willing to shift the costs of overly burdensome discovery requests to the requesting party. Cost-shifting may be particularly appropriate where the costs and burdens of discovery fall almost exclusively on one party. In fact, one federal court recently did apply cost-shifting to pre-class certification discovery where the court determined that the class plaintiffs' were seeking extensive and expensive additional discovery from defendant. If class plaintiffs seek to enforce extensive, burdensome and costly

pre-certification discovery demands, it may be prudent to seek cost-shifting for at least a portion of those costs.

For inquiries related to this Tip of the Month, please contact Anthony J. Diana at adiana@mayerbrown.com or Therese Craparo at tcraparo@mayerbrown.com.

Learn more about Mayer Brown's Electronic Discovery & Records Management practice or contact Anthony J. Diana at adiana@mayerbrown.com, Michael E. Lackey at mlackey@mayerbrown.com, or Ed Sautter at esautter@mayerbrown.com.

Please visit us at www.mayerbrown.com.

Electronic Discovery & Records Management

Tip of the Month

Best Practices for Preparing a Clawback Agreement

Scenario

A large corporation is sued over the alleged breach of a substantial contract. Due to the complex nature of the contract, the corporation's business executives frequently sought advice from in-house counsel when entering into, and performing under, the agreement. The corporation's in-house counsel has concerns that sensitive documents reflecting attorney-client communications—or even in-house counsel's own work product—may be produced by mistake, given the volume of email and electronic documents that must be reviewed quickly.

Clawback Provisions Provide Protections and Cost Savings

Even when a party to a litigation employs precautions to prevent the inadvertent disclosure of privileged documents, some privileged materials are likely to slip through. Recognizing this likelihood, litigants commonly enter into "clawback agreements" at the start of discovery. Typically, a clawback agreement permits either party to demand the return of (that is, to "claw back") mistakenly produced attorney-client privileged documents or protected attorney work product without waiving any privilege or protection over those materials.

Clawback agreements allow parties to specifically tailor their obligations (if any) to review and separate privileged or protected materials in a manner that suits their needs. For example, before discovery begins, the parties can agree on how they will search for and separate privileged or protected materials from their document productions. So long as the parties abide by the agreement, they will be permitted to take back any privileged or protected material inadvertently produced. Thus, parties can reduce their exposure to costly and time-consuming discovery disputes over whether the protection of privileged material was waived by its production.

Clawback agreements can work in conjunction with the protections of Federal Rule of Evidence 502, which provides that the inadvertent disclosure of privileged or protected information does not operate as a waiver of the privilege or protection if the inadvertently disclosing party took reasonable steps to prevent the disclosure and rectify the error. Indeed, Rule 502 expressly provides for the enforcement of clawback agreements. Further, clawback agreements can be useful in those situations, such as state court litigation, arbitrations or investigations, where the protections similar to those under Rule 502 may not be available.

Clawback agreements often include "no fault" or "irrespective of care" provisions. These clauses allow privileged or protected materials to be returned, without a waiver of privilege for the document and the subject of its contents, regardless of the steps the producing party did (or did not) take to prevent the disclosure. These provisions can provide benefits, but should not be relied upon in lieu of a privilege review altogether. Not only are there often important strategic benefits to withholding privileged material, but the savings realized from avoiding an initial privilege review may be negated if the parties must continuously sift privileged material out of their opponents' production. Moreover, some courts, as a matter of public policy, may not enforce such provisions if they believe one party exploited the provision to engage in a "document dump" that, essentially, shifted the costs and responsibility of a privilege review entirely upon its opponent.

Best Practices When Preparing a Clawback Agreement

- *Establish that inadvertent production is not a waiver*. The goal of any clawback agreement is to ensure that mistakenly producing attorney-client communications or attorney work product will not result in a waiver of any protections over the material or subject matter. This concept should be clearly stated in the agreement.

- *Incorporate the clawback agreement into a protective order*. Clawback agreements are binding only on the parties to the agreement, they typically cannot be enforced against third-parties who may seek to obtain protected materials inadvertently produced during the litigation. To protect against this, ask the court to enter a protective order that incorporates the terms of your clawback agreement. Once entered, the order is binding against non-parties as well.

- *Head off any dispute about "reasonable steps."* Clawback agreements allow the parties to define the steps they will take to prevent the mistaken disclosure of privileged or protected materials. Defining these steps in the agreement can reduce your exposure to discovery-related litigation, and it allows you to tailor the steps to best suit your needs. Sometimes, it may make sense to eliminate any required steps altogether—i.e., "no fault" or "irrespective of care" provisions. Other times, the parties agree to use targeted keyword searches of electronically stored information (or other advanced methods of screening privileged materials) as the preferred method of conducting a privilege review.

- *Establish procedures for invoking the clawback*. A clawback agreement can define the steps required to invoke its protections including: whether a party must request the clawback within a certain period of time after learning of its inadvertent production; whether the clawback request must be in writing; and whether the requesting party must explain the grounds on which the document is privileged or protected.

- *Agree to disagree*. The parties may disagree whether an inadvertently produced document is privileged or protected. The clawback agreement can establish a framework for resolving such disputes in a cost-effective manner.

- *Do not limit yourself to documents*. Concerns over the attorney-client privilege are not limited to your document production. Witnesses may reveal privileged or protected information during the

course of their deposition testimony. To address this, consider adding provisions in your clawback agreement that provide a method of striking such testimony from the record.

- *Keep it confidential*. Attorney-client communications and attorney work product are not the only types of materials a clawback agreement should seek to protect. Complex commercial litigation can involve producing materials with "confidential," "highly confidential," and "attorneys' eyes only" designations. If this is an issue in a litigation, a clawback agreement can provide a method of reassigning document designations in the event that a highly sensitive document (such as a trade secret) is mistakenly produced without the proper designation.

A well designed clawback agreement can save time and expense, especially in a complex business litigation where internal counsel were involved in matters relevant to the litigation.

For inquiries related to this Tip of the Month, please contact Michael Lackey at mlackey@mayerbrown.com, Kim Leffert at kleffert@mayerbrown.com, or Michael Bornhorst at mbornhorst@mayerbrown.com.

Learn more about Mayer Brown's Electronic Discovery & Records Management practice or contact Anthony J. Diana at adiana@mayerbrown.com, Michael E. Lackey at mlackey@mayerbrown.com, or Ed Sautter at esautter@mayerbrown.com.

Please visit us at www.mayerbrown.com.

November 2012

MAYER·BROWN

Electronic Discovery & Records Management

Tip of the Month

Managing the Risks and Costs of E-Discovery in Multiple Related Investigations and Litigations

Scenario

The Securities and Exchange Commission (SEC) and several state attorneys general are investigating aspects of a financial institution's specific service offering. Moreover, the financial institution has been named in a number of class actions related to that same service offering. The financial institution has received subpoenas and Civil Investigative Demands (CID's) from the SEC and the state attorneys general, and is in the process of expediting a response to such requests. However, the company's general counsel has serious concerns about some of the information being produced in these investigations ending up in the civil class action litigations. Indeed, the first document request from one class action plaintiff seeks all documents produced to the SEC and other government entities related to the service offering.

The Complications with E-Discovery in Multiple Related Investigations and Litigations

Managing the competing document requests and strategic goals stemming from multiple related investigations and litigations can be overwhelming. Often, what results is a seemingly never-ending fire drill of frantic attempts to preserve and collect data in an attempt to meet unrealistic production deadlines. Key decisions about what should be produced, to whom and by when often go unaddressed until it is too late.

The general challenges related to the preservation, collection and production of electronically stored information (ESI) are compounded by several factors, including:

- The risks related to regulatory and government investigations;
- The frequency of competing and subsequent requests, which may not be consistent in what information is requested, or how it is to be produced;
- The possibility that different regulators and government agencies will share information about an organization's compliance with subpoenas or requests for production;
- The possibility that plaintiffs will request whatever has been produced in the investigations to government agencies; and
- The reality that the requesting party in such situations often does not have similar challenges on

its side that can provide incentives for negotiated solutions.

In practice, the Federal Rules of Civil Procedure and their state rule counterparts fail to provide relief from unduly burdensome requests because organizations do not seek to limit these requests for fear of appearing uncooperative during an investigation. Plaintiffs in litigation, who are limited by these rules, seek to benefit from this fear and leverage the investigatory work of the government agencies and regulators. It is with these challenges in mind that an organization must prepare for and comply with requests for production in connection with multiple related investigations and litigations.

Best Practices for Managing ESI in Multiple Related Investigations and Litigations

Effective planning, strategic negotiations and appropriate disclosure are the keys to satisfying investigators and plaintiffs that an organization has complied with its preservation and production obligations while controlling costs. The key is maintaining control—an organization should be proactive and try to dictate the terms of the preservation, collection and production of data. While obtaining and maintaining control can be very difficult to accomplish, particularly with regulators and government agencies, it is possible to do so if an organization, and its outside counsel, has a comprehensive understanding of the issues, the data addressing those issues and the location of key data within your organization.

An organization will be given more leeway to conduct all aspects of e-discovery without much interference if:

- Investigators and plaintiffs sense that the organization, or its outside counsel, knows more than they do;
- The organization and outside counsel have empirical evidence to support the assertions; and
- The organization and counsel are willing to be transparent about what steps are being taken to identify, preserve, collect and produce such information.

Formulate a Preservation, Collection and Production Plan. Prior to receiving a specific request for production, identify key data sources for ESI and develop a preservation and collection plan. Use early case assessment (ECA) tools to help identify key issues, documents and personnel. This lays the groundwork for more defensible decisions regarding preservation, collection and production of ESI from various data sources. In the end, an organization cannot preserve, collect and produce all ESI related to a matter—important decisions need to be made early in the investigation or case about what ESI is truly material to the key issues in the matter and the steps that the organization plans to take to preserve, collect and produce that data. In other words, do not be distracted by attempting to get everything—focus on the smaller set of key documents.

Consider Use of a Master Repository for Data. The use of a master repository for all data being collected may help keep track of what documents have been produced to which parties at what time. Depending upon the vendor you use and your data management planning, this can result in a major costs savings, particularly if the vendor can avoid creating multiple databases and TIFF image production sets. This may also allow for documents to be "produced" by providing adversaries with limited access to a production database, giving an organization greater control over the production sets. Having a master

repository helps an organization manage the data and should lead to better documentation of defensible practices.

Consider What Documents Should Be Shared Among Investigators and Plaintiffs. It is unlikely that state and federal agencies will agree to not share key documents with other investigating agencies. Determine early on what information will be shared with which regulators and government agencies, and when the best time to share such information may be. These are key strategic decisions that should be tied into the strategic goals of the organization, not the result of *ad hoc* collection and review processes dictated by the circumstances. Also, while protective orders may limit the use of documents by plaintiffs, you should be prepared for a request by plaintiffs for you to produce what has been produced in the investigation to regulators and government agencies. An organization or counsel may have a very different view of privilege or data privacy with a regulator or government agency than it does with plaintiffs in a litigation. Consider these issues before any documents are produced, and have the plan to defend the organization's decisions.

Document Preservation, Collection and Production Decisions and Activities. The best way to convince investigative agencies and plaintiffs that appropriate steps have been taken to preserve and collect relevant data, is to be able to explain exactly what steps were taken. Carefully documenting the organization's efforts to implement its preservation and collection plan will put the organization in a position to provide immediate and accurate answers in response to questions.

Anticipate and Plan for Future Requests. It is common to receive overlapping requests from different parties. It is good practice to anticipate the possibility of such requests and to consider, during the initial review and production, which data, if any, may be useful for later productions in response to future requests. As noted earlier, to obtain and maintain control of the process while managing the costs, consider conducting a broad culling and review protocol (e.g., broad subject-matter related search terms and a review protocol tied to the subject matter, like a service offering, product or activity). Once that subject matter set is determined, develop a plan to defend the position that this set will be the master set from which all requests will be sourced (including the use of a statistical sampling of the complete set to develop a baseline of responsiveness, sampling of the null set to establish precision and recall of any term used, or other techniques that objectively support the determination). With this targeted set of data to manage, additional data analytics can be applied to identify and review documents responsive to specific requests without reviewing the whole set again. Consider whether some type of coding will be helpful during the initial review to help with this process.

Carefully Plan for Meet and Confers with Investigators. Even though there is no rule or regulation that imposes an obligation to "meet and confer" with a regulator, regulators are often open to such discussions. Upon receiving a preservation letter or more formal subpoena, an organization (or its counsel) should immediately engage in a dialog with the regulator about the steps that the organization is taking to preserve and produce ESI. Any burdens or impediments to effective compliance should be raised as soon as possible, if for no other reason than to demonstrate that the organization intends to cooperate with the investigation.

Carefully Plan for Meet and Confers with Plaintiffs. Meet and confers with plaintiffs while there are on-going investigations are particularly critical. Key decisions need to be made about the scope of the

productions, and in particular if they are going to track the scope of the productions to the investigators. Proportionality and court supervision may help limit costs and burdens, which is additional leverage. Likewise, there may be important reasons why certain documents produced in an investigation should not be produced to plaintiffs, including potentially privileged documents, documents with data subject to privacy laws, or documents outside some parameters of a case (e.g., different subsidiaries outside the jurisdiction of a court, time periods due to statute of limitations, etc.)

Be Aware of Production Guidelines. Many regulators have specific guidelines for productions. Compliance with such guidelines is presumed, and organizations and their counsel must be cognizant of them. Any burdens or challenges of meeting the production guidelines should be raised during the meet and confer, and attempts should be made to make them consistent from one investigating entity to the next. An organization also should leverage those production guidelines with plaintiffs so that productions can be consistent across litigations as well.

Negotiate to Meet Strategic Goals and Manage Costs. It is possible, and advisable in most cases, to negotiate the scope of production with any requesting party, including government agencies and regulators. Keep in mind that regulators often have staffing or budgetary limitations, as well as time constraints, that impact their ability to review large volumes of data. Counsel for an organization should be prepared to discuss the scope and limitations on the production to the most relevant ESI, which may avoid excessive costs. Generate empirical evidence to support any assertions as to the burdens and costs related to the preservation and production of documents, and why the data being produced is the most relevant during the negotiations. This information provides more control to an organization during the negotiations around the scope, timing and format of the productions.

For inquiries related to this Tip of the Month, please contact Anthony J. Diana at adiana@mayerbrown.com, Therese Craparo at tcraparo@mayerbrown.com or Patrick Garbe at pgarbe@mayerbrown.com.

Learn more about Mayer Brown's Electronic Discovery & Records Management practice or contact Anthony J. Diana at adiana@mayerbrown.com, Michael E. Lackey at mlackey@mayerbrown.com, or Ed Sautter at esautter@mayerbrown.com.

Please visit us at www.mayerbrown.com.

December 2012

MAYER·BROWN

Electronic Discovery & Records Management

Tip of the Month

Cloud Computing and Data Privacy

Scenario
A multinational company is negotiating an agreement with a cloud computing provider to maintain and hold all of the company's electronically stored information and data. The general counsel of the multinational company is concerned about data privacy and data protection both in the United States and worldwide.

What is Cloud Computing?
Cloud computing is the use of computing resources, including both hardware and software, that are made available over the Internet by a subscription-based service provider. Because cloud computing is Internet-based, it offers several advantages over more traditional access to a company's data and software. Cloud-based software and files can be accessed "on demand" from virtually any computer with an Internet connection. For example, when email is stored "in the cloud," the contents of a user's email folders may actually be stored in one or more easily accessed Internet-connected servers located around the world. Moreover, because a company that receives cloud computing services does not rely on its own servers, the amount of data that can be stored is unlimited. Finally, because cloud computing services typically are managed by a third-party provider, they have the potential to reduce a company's IT costs by eliminating the need to acquire and maintain expensive hardware and software. For all of the above reasons, many businesses are seeking to take advantage of this still-evolving technology.

Potential Risks: Data Privacy, Data Storage, and E-Discovery
Data privacy is an issue of concern for companies, their IT professionals and legal departments, whether files stay on-site or are stored electronically with a cloud computing provider. For companies considering cloud computing options, it is particularly important to carefully evaluate the provider's policies and procedures to ensure that they provide sufficient safeguards to protect confidential data. The company's lawyers and IT professionals should develop an understanding of the technology so that they can make informed decisions about whether cloud computing provides the level of protection they require.

One specific risk is that electronically stored information (ESI) may be co-mingled with the ESI of another company or of a separate but related corporate entity. Such situations can make it difficult to determine what entity has "possession, custody, or control" of the data and is under an obligation to

preserve or produce the data. Moreover, if a cloud computing provider stores data in multiple servers around the world, ESI may be split up among jurisdictions with different data protection and transfer laws, making it difficult to keep track of how to access and retrieve data, and how to keep data private and secure.

ESI stored with a cloud computing provider can also present challenges to the discovery process in litigation. For example, the U.S. Federal Rules of Civil Procedure allow a party to request discovery of ESI in the responding party's "possession, custody, or control." If a company has contracted with a cloud computing provider to maintain and hold its ESI, the company does not have direct control over, or possession of, the ESI. For purposes of discovery, however, the company still has a duty to preserve and produce that data, as long as it has the practical ability to do so.

Tips for Managing Risks

The use of cloud computing should not fundamentally change the way a company handles ESI. No matter where the ESI resides, a company is responsible for being aware of the information that it creates and for governing that information in accordance with applicable business and legal requirements. It is important that the company be familiar with and closely monitor how its information is stored, retrieved, retained and disposed of by its cloud provider. A company should also develop effective procedures for auditing such activities by its cloud provider. At a minimum, the company should make sure it is capturing sufficient data when information is created (including what the information is, who created it, and for what purpose) to properly govern it.

Before signing a service contract with a cloud computing provider, a company should be sure that the contract contains provisions protecting the company's interests and its need to comply with data privacy requirements. Consider the following items when negotiating a service contract:

- Access: The company should have the right to access all ESI "on demand" and in a specified format that is easy to use.
- Control: The company should have the ability to reasonably direct actions of the provider to preserve and produce ESI.
- Cooperation: The provider should be willing to comply with the company's directions regarding its ESI and to comply with any and all legal holds.
- Speed: The provider should agree to cease any data destruction in a timely manner and to produce data with sufficient speed to meet the company's obligations.
- Metadata: The company should inquire as to the form or format in which data will be stored and returned for production during litigation, including whether metadata will be intact.
- Costs: Beyond the subscription price for the service, the contract should address the costs of potential production, as well as potential indemnification policies and attorneys' fees should the cloud provider's failure to comply with the contract terms result in liability for the company.
- Transparency: The contract should address confidentiality, data integrity and availability issues, including whether data will be commingled with the data of other cloud customers.

- Jurisdiction: The company should discuss with the provider where the data will be maintained and should consider whether production of the data might require compliance with data transfer laws or international privacy laws.
- Ownership: The contract should clearly state that the company owns the data.
- Security: The company should inquire about the security measures that the provider has in place to protect data privacy and attorney-client privilege and whether the company will be informed in the event of a security breach.
- Policies: The company should determine whether the provider's policies and procedures could impede the company's obligations to preserve, collect and produce ESI during litigation.
- Disaster Recovery: The company should have contingency plans in the event the provider was to suffer a server crash or other data loss or go bankrupt or out of business. The contract should stipulate that its provisions will remain in force if the provider is acquired by another company.

The best way to manage the data privacy and security risks associated with cloud computing is to gain a comprehensive understanding of how the company plans to use cloud computing and to establish procedures and contract terms with the cloud computing provider that meet the company's data security and privacy needs.

For inquiries related to this Tip of the Month, please contact Michael E. Lackey at mlackey@mayerbrown.com, Kim A. Leffert at kleffert@mayerbrown.com or Patrick M. Tierney at ptierney@mayerbrown.com.

Learn more about Mayer Brown's Electronic Discovery & Records Management practice or contact Anthony J. Diana at adiana@mayerbrown.com, Michael E. Lackey at mlackey@mayerbrown.com, or Ed Sautter at esautter@mayerbrown.com.

Please visit us at www.mayerbrown.com.