MAYER·BROWN

Electronic Discovery & Records Management

2010 TIPS OF THE MONTH – A Compilation

TABLE OF CONTENTS

Page

Electronic Discovery & Records Management

Tip of the Month

January 2011

2010 Trends in E-Discovery

The year 2010 saw several key court decisions and several emerging trends in e-discovery that are likely to continue to be a focus in 2011. Hot button issues included social media, cloud computing, privacy concerns, the blurring of lines between business and personal communications, data located in foreign jurisdictions, and, of course, the courts' willingness to impose severe sanctions against companies that failed to properly manage ESI (Electronically Stored Information).

Spoliation & the Knowledge Expectation

Several decisions this year demonstrate the courts' continued willingness to sanction litigants who allegedly fail to properly manage ESI or make inaccurate representations (inadvertent or advertent) regarding their management and preservation of ESI, including decisions from Judge Shira A. Scheindlin in Pension Committee of University of Montreal Pension Plan v. Banc of America Securities LLC, 685 F. Supp. 2d 456, 470 (S.D.N.Y. 2010) and Magistrate Judge Paul W. Grimm in Victor Stanley, Inc. v. Creative Pipe, Inc., 2010 WL 3530097 (D. Md. 2010). While there is, as noted by Judge Grimm, significant confusion and little consensus surrounding the standards that govern preservation and spoliation, it is clear that courts – both state and federal – expect counsel and their clients to have a firm handle on the organization's information systems from the outset of a litigation.

Social Media, Cloud Computing & Other Emerging Technologies

The development of new technologies means new e-discovery challenges. In particular, both courts and regulators took steps to tackle social media as a potential source of discoverable information in 2010. Regulatory requirements like FINRA Regulatory Notice 10-06 (Jan. 2010) and court decisions like EEOC v. Simply Storage Management, LLC, No. 1:09-cv-1223 (S.D. Ind. May 11, 2010) and Crispin v. Christian Audigier, Inc., No. CV 09-09509, 2010 WL 3703242 (C.D. Cal. May 26, 2010) merely scratch the surface of the issues underlying the discoverability of information posted to social media sites, especially mounting privacy concerns. The movement toward cloud computing is likely the next big challenge on the horizon for e-discovery and invokes many of the same concerns as social media.

Personal Email, Phones & Other Personal Devices Used for Work-Related Communications

As the line between "personal" and "work-related" communications becomes blurred by the increasing use of personal email or personal devices for work-related communications, questions arise regarding whether the sources of potentially relevant

information that need to be preserved include handheld devices issued to an employee, home computers or personal email accounts. But the potential discoverability of personal email or data on personal devices used for work-related communications also gives rise to privacy concerns. Organizations must work to strike a balance between the realities of a mobile work force and the e-discovery or other legal risks associated with the cross between personal and work. For example, in Stengart v. Loving Care Agency, Inc., 990 A.2d 650 (N.J. 2010), the court concluded that an employee had a reasonable expectation of privacy in emails sent to her attorney using a password-protected Yahoo! account via an employer-issued computer. And in In the Matter of vFinance Investments, Inc., Exchange Act Rel. No. 62448 (July 2, 2010), the SEC censured, fined and issued cease and desist orders against a company and its former COO for violating the recordkeeping and production requirements of the securities laws by failing to preserve and promptly produce electronic communications in response to SEC requests, including the personal email and personal computer of an independent contractor.

Privacy & Confidentiality

Privacy issues were at the forefront of concerns surrounding e-discovery in 2010, cropping up in relation to the discoverability of data from online service providers (including social media websites), cloud computing, employment matters and criminal investigations. The court in Crispin v. Christian Audigier, Inc., No. CV 09-09509, 2010 WL 3703242 (C.D. Cal. May 26, 2010) addressed the discoverability of private messages on social media sites like Facebook and MySpace directly from the website operators and whether the Stored Communications Act prohibits such providers from responding to subpoenas. In U.S. v. Warshak, Nos. 08-3997, 08-4085, 08-4087, 08-4212, 08-4429, 09-3176, 2010 WL 5-71766 (6th Cir. Dec. 14, 2010), the Sixth Circuit held that a subscriber enjoys a reasonable expectation of privacy in the content of emails "that are stored with, or sent or received through, a commercial [Internet Service Provider]," and found that government agents may not compel an Internet Service Provider to turn over the content of emails that are stored with or sent or received using ISP systems unless the government first obtains a warrant based on probable cause. Privacy concerns have important operational implications as well; to avoid inadvertent data breaches in connection with e-discovery, an organization must consider the types of confidential information it maintains, its legal obligations relating to that information and how to minimize the risks of data breaches when producing such data in response to legal production obligations.

Data Preservation & Collection from Foreign Jurisdictions

Increasing economic globalization gives rise to heightened concerns about the preservation and collection of ESI located in foreign jurisdictions. But US courts in 2010 demonstrated a willingness to require the production of relevant ESI even in the face of blocking statutes or data privacy laws. In AccessData Corp. v. ALSTE Techs., No. 2:08cv569, 2010 WL 318477 (D. Utah Jan. 21. 2010) and Services Antitrust Litigation, Case No. 1:06-md-1775-JG (VVP) (E.D.N.Y. Mar. 29, 2010), courts rejected efforts to resist responding to document requests based on the claims that foreign blocking statutes barred the discovery. A similar argument was rejected in Gucci America, Inc. v. Curveal Fashion, 2010 WL 808639

(S.D.N.Y. Mar. 8. 2010) based on prohibitions against disclosure in Malaysian banking secrecy laws. Interestingly, the courts' opinions often rely on a purported failure to show a likelihood of prosecution once the objecting party actually produced the documents.

For inquiries related to this summary of the 2010 Trends in E-Discovery, please contact any of the following lawyers.

Michael E. Lackey
mlackey@mayerbrown.com

Anthony J. Diana
adiana@mayerbrown.com

Therese Craparo
tcraparo@mayerbrown.com

Rebecca Kahan
rkahan@mayerbrown.com

To 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

Please visit us at www.mayerbrown.com

Tip of the Month

What You Need To Know About Instant Messaging

Scenario

An organization learns that an employee has filed a complaint with the Equal Employment Opportunity Commission (EEOC) alleging that she was sexually harassed in the workplace. The organization is aware that many of its employees, including key employees named in the EEOC complaint, use publicly available Instant Messaging (IM) software to communicate with one another while at work. The organization does not have an existing policy governing the use of IM and is concerned that key employees may be engaging in discoverable communications via IM. The organization is now considering whether, and how, to take steps to retain potentially relevant IM communications.

What is Instant Messaging?

Originally popularized by teenagers and college students, IM has spread into the workplace. IM allows direct communications between two or more individuals via the Internet using a small message window to deliver a typed message from the sender's computer to the recipient's computer. It differs from email in that it is instant and is designed to be interactive and conversational. In addition, unless specific measures are taken to retain the text exchanged during an IM session, the messages generally cease to exist once the session is terminated.

Many business people use IM because of its immediacy and efficiency in exchanging real-time information. Initially, business people used public IM services such as AIM, Yahoo IM or Google Chat — products they downloaded free of charge on their employers' computers. In recent years, however, some organizations have installed internal IM systems.

Although a consensus has yet to be reached as to whether, for purposes of discovery, instant messages most resemble email, chat room "conversations," conference tools, or telephone conversations, it is clear that IM has borrowed features from both telephony and email. However, whether IM remains as ephemeral as telephone communications or endures like email depends on whether transcripts of the

messages are made, printed or otherwise recorded by the user prior to ending the IM session or, in the case of corporate IM, whether the conversation is captured on the organization's server.

What Issues Arise Regarding Instant Messaging in Discovery?

The significance of IM as a source of electronically stored information (ESI) has grown in recent years due, in part, to the increasing use of IM in the corporate world, the increasing ability to capture or log IM sessions and the fact that communications via IM are often even more casual than email communications. Under Fed. R. Civ. Proc. 34(a) "electronically stored information" is discoverable if it is "stored in any medium" from which it can be obtained and "translated, if necessary," into a "reasonably usable form." To the extent that IM is retained in the ordinary course of business, by either individual users or on an organization's servers, IM may, like email, constitute ESI and be subject to preservation and production to the extent it is reasonably calculated to lead to the discovery of admissible evidence.

An even more difficult question arises when an organization does not retain instant messages in the ordinary course of business and where a continuing obligation to preserve information arises in connection with a pending or anticipated litigation. In those situations, an organization that does not retain IM in the ordinary course of business must consider whether it is required to institute some form of retention as a result of the anticipated or pending litigation.

There has, to date, been very little explicit guidance from the bench on this subject. Given this lack of direction, whether an organization has a legal obligation to preserve instant messages is best determined by examining the practical issues involved, such as the specificity of any demand for preservation (whether by demand letter, subpoena or the like), its likely relevance to the issues in dispute, and any regulatory or other business needs involved.

Best Practices for Preserving Instant Messages

Organizations should consider taking affirmative steps to establish policies and procedures regarding the use of IM in the workplace. Further, the absence of clear guidance from the courts regarding the production and preservation of instant messages counsels in favor of taking affirmative action to address this issue at the onset of litigation.

- *Evaluate the Need for an IM System.* Before considering the question of instant message retention, organizations should carefully consider whether IM should be made available at all. While IM can provide substantial efficiencies in the conduct of business matters, it may trigger employee misuse and become a tool for sexual harassment, offensive or other non-professional communications, theft of corporate secrets, or simple abuse of corporate time and resources. Only if the benefits of IM outweigh the risks should an organization adopt the use of an IM system in the workplace.
- *Install a Corporate IM System and Prohibit Public Instant Messages from Being Used.* If an organization concludes that IM poses a net benefit, the next step is to decide what kind of IM system it should use. While this is a business decision, the issue of control of the server is likely

going to tip the balance in favor of purchasing an enterprise-wide system. An organization that has its own IM platform, and that implements and enforces a policy on the use and retention of instant messages, is in a much better position to ensure that instant messages are being treated correctly and consistently.

- *Establish a General Policy Governing the Use, Content and Retention of Instant Messages.* Organizations should consider implementing a written, clear and understandable IM policy. In evaluating the need for retention, organizations should consider regulatory or other industry requirements: for example, in recent years, both the Securities and Exchange Commission and the Financial Industry Regulatory Authority have promulgated rules that specifically require the retention of instant messages for three years. Retention, archiving and deletion procedures for instant messages should be described if a determination is made that retention is appropriate.
- *Raise the Issue of Instant Messages Early in Discovery.* Organizations should carefully evaluate their preservation obligations at the outset of any litigation, including whether a requirement may exist to preserve instant messages on a going-forward basis. Litigants should consider raising this issue with the opposing party early in the litigation, including whether and how potentially relevant instant messages should be preserved or produced. As with all issues related to ESI, if an agreement cannot be reached, it is preferable to approach the court with a sensible, reasoned solution early rather than face allegations of spoliation later.

For inquiries related to this Tip of the Month, please contact the authors, 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 or Michael E. Lackey at mlackey@mayerbrown.com.

Please visit us at www.mayerbrown.com

February 2010

MAYER·BROWN

Electronic Discovery & Records Management

Tip of the Month

Selecting an Electronic Discovery Vendor

Scenario

A large, international company has been served with a complaint alleging antitrust violations. Vast amounts of electronically stored information (ESI) will need to be preserved, collected, reviewed and possibly produced in defense of this litigation. Over the years the company's legal department has retained many different vendors to assist with document collection and review, usually at the recommendation of outside counsel. A recent audit of the legal department questioned whether this is a cost-effective approach. Based on the nature of the claims, this litigation may continue for years.

What are the Considerations of Vendor Selection?

With so many electronic discovery vendors in the industry how does a company begin to select the most effective and efficient provider? Several general considerations should be addressed at the outset of the litigation: **Data Security and Privacy, Costs, Product Quality and Performance**.

Clearly defining the specific parameters of the case along with an analysis of the company's litigation risk profile will assist in selecting the most appropriate electronic discovery vendors. These considerations are important whether the company intends to enter into preferred provider agreements — to reduce costs and speed up the selection process when future litigation hits — or to hire a vendor that can get started immediately for this case only.

Data Security and Privacy

- A growing body of rules and regulations in the United States and internationally address data protection and privacy; these can, and frequently do, impact a company's operations. Consider whether a vendor is familiar with these rules and regulations and can provide viable options for compliance.
- Companies are legitimately concerned about how their data are managed, whether by outside counsel or third-party providers. Consider whether the vendor's data management policies and procedures meet the company's requirements.

- Information security is critical to business operations. Determine if the vendor has comprehensive guidelines in its policies and procedures addressing this risk.
- It is crucial to confirm the financial viability of any proposed vendor. There is significant volatility in the electronic discovery industry and data and time can be lost if a vendor unexpectedly ceases operations.

Costs

- Accurately predicting the final cost of a project is often difficult. Initial cost estimates are usually based on limited information. In addition, new issues will likely arise during the project that can have a significant impact on costs. Thus, it is very important to consider possible changes to the anticipated scope of work and to negotiate pricing for those tasks that is understandable and acceptable.
- Complex cases can require unique data handling, which may lead to additional resources and higher costs.
- Unexpectedly large data volumes and short production timelines also can drive up project costs.
- Various pricing options are available from vendors. Custom pricing and flat fees may provide more certainty, but they may not be the most cost-effective option for all cases. It is important to understand the cost factors, whether for the immediate case or for a longer-term engagement, before deciding on a vendor.

Product Quality

- The experience and skill of the project managers and technologists at each vendor are often key discriminators among providers. Check the vendor's references, by consulting with colleagues and other counsel who have used them.
- Consider the capabilities of the vendor in the following areas:
    - Electronic Discovery Consulting Services
    - Data Collection
    - Data Processing
    - Data Hosting
    - Document Review Staffing
    - Production Formats
    - Hosting Inactive Case Data
    - Printing
    - Project Management
    - Training
    - Technical Support
    - Security
    - Use of Subcontractors
    - Conflicts checking

- A company may not need all of these services in each matter. Further, nearly every vendor has a "sweet spot" where its services excel; consider retaining more than one vendor, even for a single litigation, if there is a particular need.

Performance

- An E-discovery vendor must be able to handle large data volumes, meet tight deadlines, and produce information consistent with specific requirements. The failure to produce documents in a timely fashion, or in the appropriate format, can lead to disputes with opposing counsel, loss of credibility with the court, and, at worst, sanctions. Many factors can affect production, including problems during the data collection, processing and review. The best vendors can anticipate potential problems and resolve them in a timely fashion, allowing counsel to meet their discovery obligations
- It is important to inform the vendor of the services needed and time frames in the litigation and verify that the vendor can deliver the services that enable you to meet your discovery obligations.
- It is also important to confirm that the vendor understands and can meet your specific production protocols and deadlines.

How to Get Started

For companies with routine or predictable litigations and investigations, it may make sense to enter into preferred provider agreements with select vendors. This can be done by issuing requests for proposal or requests for information to a number of vendors, evaluating the responses, and choosing several that meet the company's various ESI collection, review and processing needs.

Companies that face few or unique litigations or investigations may be more comfortable selecting a specific vendor for a particular matter when it arises. If time is of the essence, it may be most efficient to limit the selection to two or three vendors. Consult with your colleagues and outside counsel on their experience with vendors. Identify for each vendor the specific parameters and scope of your case and request a service agreement and Statement of Work (SOW) that suits your discovery plans and needs.

Despite some consistency throughout the industry in terms of the core services, there are unique approaches among vendors to pricing, functionality and workflow. Thus, you should determine key discriminators among the possible vendors. Further, consider how case priorities align with a vendor's policies in the areas of data security, project costs, review complexity and schedule. In addition, it is a good practice to have a comprehensive agreement that addresses various risks, including service level agreements, and that contains specific provisions regarding limitation of liability, indemnification, termination and restrictions on the vendor holding the client's data hostage.

While many vendors will try to convince you otherwise, no one vendor is the right choice for **every** litigation. Learning the strengths and weaknesses of each vendor, and comparing their services, will provide much-needed insight and will assist in the selection process.

For inquiries related to this Tip of the Month, please contact Patrick Garbe at pgarbe@mayerbrown.com, Chris Hansen at chansen@mayerbrown.com or Allisa Vermillion at allisa.vermillion@mayerbrown.com from Mayer Brown's Electronic Discovery Services, or Kim Leffert at kleffert@mayerbrown.com.

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

Please visit us at www.mayerbrown.com

March 2010

MAYER·BROWN

Electronic Discovery & Records Management

Tip of the Month

Managing the Electronic Discovery Vendor Relationship

Scenario

A large international company has just entered into antitrust litigation. After carefully selecting the electronic discovery vendor that will handle the processing, hosting, review and production of the responsive documents, the company's counsel needs to manage the vendor relationship throughout the case to ensure success.

Does the Relationship with the Vendor Really Need to be Managed?

Even though you may have selected the best electronic discovery vendor for your case, it is critical to manage that relationship to ensure a positive outcome. At the outset of every case, expectations of costs, timelines and deliverables are set with your vendor. Unfortunately, litigants rarely know everything there is to know about the case at the beginning, and issues that arise throughout the matter must be addressed. Establishing a few key processes and procedures with an electronic discovery vendor will allow a company to manage the substantial costs and risks associated with the unpredictable issues that arise during discovery.

Create a Case Playbook – Documentation

Documentation of the steps taken in electronic discovery is an important component of managing the vendor relationship. Remember that several in-house departments may be involved, such as the IT team that was involved in collecting data and the human resources people who may play a role with managing a litigation hold notice. Counsel should document the processes performed by all employees, vendors, and outside counsel, as well as individuals within the corporation. Key aspects of case playbooks include:

- Documenting the decisions made about the case. Such documentation may be used to demonstrate to a court that the discovery conduct was reasonable, and should describe the decisions made from the onset of the case by the corporation, outside counsel and the electronic discovery vendor.
- Creating, following and documenting the steps taken to follow a discovery plan.

- Including a change control process in your plan to manage any unexpected issues that arise.
- Identifying whether data is "self-collected" or a vendor is hired to conduct a forensically-sound collection, creating documentation of process that maintains a defensible chain of custody.

Documentation will facilitate management of the process, thereby reducing the costs and risks associated with electronic discovery. It will also help support an argument that any spoliation that may occur was the result of routine, good-faith operation of an information management plan for electronic data, which can provide some protections under the safe harbor clause of Rule 37(e).

Managing Expectations, Roles and Responsibilities

Managing the expectations, roles and responsibilities of in-house personnel, outside counsel and the vendor can facilitate success in complying with electronic discovery obligations. It can also be invaluable in controlling costs. Steps to take include:

- Creating or updating a Services Agreement or Statement of Work with the vendors and outside counsel so that each can gain a broad understanding of the others' roles and responsibilities; in particular, these documents should identify deliverables and performance guarantees.
- Communicating realistic expectations for meeting discovery obligations.
- Establishing a master team list with contact details that allows you to reach all parties on the team on a 24-7 basis. The master team list should include a pre-defined escalation plan of who will be contacted when issues arise.
- Understanding who is on the team and what must be achieved in order to reach the goals of an evolving discovery plan.
- Establishing a plan to manage various risks by enforcing compliance with service-level agreements that contain specific provisions that address the limitation of liability, indemnification, termination and restrictions on access to the case data.
- An increasingly important area for managing vendor relationships concerns insurance coverage. Clients should discuss coverage for electronic discovery costs with their insurance carriers early in the process. Vendors should understand how possible coverage limitations may impact the delivery of services. Law firms, as partners collaborating with clients to control costs, may strategically decide to litigate certain discovery issues that may lead to a more targeted discovery plan when insurance providers understand and support the plan.

Managing the Workflow by Staging the Discovery Process

Managing the workflow by staging the discovery process can help contain discovery costs and ensure that the individuals responsible for handling discovery are not trying to accomplish too much at once. Steps to take include:

- Defining the stages for processing the data and setting up the attorney review workflow. Doing so can prevent the wholesale processing of all client data upfront as well as starting the review without the benefits derived by data analytics. By loading data in a designated order and applying early

case assessment (ECA) techniques, a party will be better able to control and manage discovery services.

- Holding a Kick-Off meeting with all parties to review the goals of the case, timelines, review strategy and establish an electronic discovery processing workflow. Be sure to consider the end-to-end process from litigation hold and collections all the way to productions and possible trial.
- Scheduling conference calls on discovery planning at the outset of the engagement and establishing clear lines of communication between the client, vendors and law firms.
- Establishing a daily meeting time that can be utilized as needed. Too much time is wasted trying to bring the team together for discussions on a hot issue. Take the question of "when can we meet" out of the equation.
- Circulating supporting documentation in advance and finalize "to do" items during the calls.
- Establishing a primary point of contact with the vendor.
- Interviewing the vendor's project managers and "hiring" the best candidates.
- Providing vendors with clear guidance. The instructions should include guidance on:
    - The order for processing and filtering custodian data;
    - If applicable, the allotment of sufficient time for performing ECA and data analytics;
    - The preparation of a training program for responsiveness review;
    - Documentation of the process; and
    - Timelines.

Managing Services Provides Necessary Protections for All

It is important that clients, outside counsel and vendors discuss confidentiality and privilege issues as part of the increasingly complex relationships that arise with the delivery of electronic discovery services. While it is the client who holds the reins on maintaining privilege, providers of legal and technical services must be careful to maintain these vital, legal protections.

Managing and securing these protections require lawyers to actively participate in the process because many of the decisions made throughout the electronic discovery process amount to legal advice that, by law, non-lawyers are prohibited from dispensing. Consider, too, whether service providers will be called upon for expert testimony or to prepare an affidavit on some aspect of discovery. Have these discussions with providers and determine who is capable of providing testimony in defense of process, or can be relied upon for support when challenging the other side's discovery. Confirm that these issues are adequately protected.

Importantly, while managing performance, take the opportunity to audit the data security and safeguards that were negotiated as part of the Services Agreement. Although a formal audit is sometimes needed, a thorough review of the evolving documentation surrounding the engagement generally can assure that procedures are being followed. Remember that it is far easier and cost-effective to maintain proper documentation from the start than to re-create it when the need arises.

For inquiries related to this Tip of the Month, please contact Patrick Garbe at pgarbe@mayerbrown.com, Chris Hansen at chansen@mayerbrown.com or Allisa Vermillion at allisa.vermillion@mayerbrown.com , all from Mayer Brown's Electronic Discovery Services Department, which supports the Firm's case teams and its clients in handling the demands of collecting and managing electronic discovery.

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

Please visit us at www.mayerbrown.com

Tip of the Month

Critical Early Steps Regarding ESI After Receiving Reasonable Notice of Litigation or an Investigation

Scenario

Class-action litigation is filed against an airplane manufacturer alleging that its engines are defective because they are unreasonably susceptible to stalling during flight. Upon receiving the complaint, in-house counsel meets with relevant business people and identifies a wide variety of categories of electronically stored information ("ESI") that may be relevant to the matter.

The Critical Early Steps With Regard To ESI

Upon notice of pending or reasonably anticipated litigation, an organization has an obligation to take reasonable and proportionate steps within a reasonable time frame to preserve relevant and discoverable materials, documents and ESI. Determining which steps are reasonable and proportionate in particular litigation is a fact specific inquiry that will vary from case to case, and generally evolves as the case progresses and more information about the issues and the relevant evidence becomes available. Common early steps include the following:

Implement a Legal Hold

Implementing a legal hold is a multi-step process. An initial determination must be made as to the scope of the hold, both in terms of which individuals are likely to have relevant evidence based on what is then known about the case and what materials, documents and ESI should be subject to the hold. Because timeliness is also important, it is advisable for organizations to proactively develop a process and pre-approved templates for these steps before specific disputes arise.

Identify Key Personnel to Receive the Legal Hold

Determining which individuals within the organization should receive the hold can be difficult and it is unrealistic to expect that the initial list will be exhaustive. Seeking perfection or near perfection comes at the cost of delay. It generally will be better to show that a legal hold was distributed within days, or weeks,

and covered a reasonable but imperfect list of individuals and types of evidence, and was expanded as investigation continued, than to assert that the initial list was perfect but was issued only after months of investigation. Organizations that experience a significant amount of litigation often invest in software that facilitates, manages and tracks the issuance of legal holds, including links into personnel databases. Departed employees and those who will leave the organization as the case progresses present special challenges. Reasonable steps should be put in place to safeguard their paper and electronic documents from being lost after their departure. An organization's legal hold program can minimize this risk by requiring responsible employees to determine if a departing employee is subject to a legal hold as part of the routine exit procedure.

Identify Key Document Types

The organization should also determine the types of potentially responsive information to be preserved. This may include, among other things, tangible things, hard copy documents, active electronic files, e-mails, backup systems or archives, and data on laptops, PDAs, or cell phones. This may also include sources of ESI that are *outside* the control of the directly involved individuals, such as corporate databases, shared files, online document depositories, offline data stored in network shares, portable storage media and corporate electronic archives. These sources of documents and ESI often will be identified only after some interviews and other investigation. It is often IT professionals whose active involvement will be needed to preserve such sources of ESI.

Suspend Routine Deletion of Documents if Necessary

Consider whether any routine electronic data operations need to be suspended or altered. The nature of electronic information systems is that data contained within them is routinely and automatically updated or overwritten or purged in the ordinary course of business. Some of this cannot reasonably be avoided, such as the routine updating of various metadata. However, some automatic functions, such as automated e-mail deletion processes or space limits imposed on e-mail users, might need to be lifted for individuals on legal hold.

Content of the Legal Hold Notice

The legal hold notice should spell out in reasonable detail, based on the information that is reasonably available to counsel at the time, what is expected of the recipients. This includes identifying relevant subject matters, suggesting types of ESI to be considered, providing any necessary instructions on how to comply, and providing contact information for a knowledgeable person on the litigation team who can answer questions about the legal hold.

It is a good practice to document the steps taken to implement a legal hold. It may be as important to be able to recall and explain the timely and reasonable steps that were taken to preserve evidence as it is to have taken those steps.

Important Follow-Up Steps

As important as the issuance of a timely and reasonable legal hold notice is the subsequent "affirmative steps" that are taken toward implementing an effective legal hold process. Such steps often will include:

- *Determine the existence and location of any non-standard ESI and archived material*. If the company has relevant and discoverable voicemail, text messages, or other non-standard ESI, consider whether it can and should be preserved. If so, work with the appropriate IT or administrative personnel to do so. Certain archived data, including any older tapes or other media containing system wide backup data, may fall into this category. This must be tempered by proportionality -- balancing the burdens with the ultimate benefits of preservation.

- *Determine if ESI relates to third party agents, including the need to preserve and collect data in the custody of such agents.* Under US federal law – and the laws of most US states – a party is required to preserve responsive information within its "control," which may include data in the physical possession of third parties. If the organization has the legal right to data in the possession of such a third party there may be an obligation to take steps to preserve, collect and produce it.

- *Determine if ESI relates to data maintained outside of the United States and consider local rules regarding the collection and review of such data*. Given the impact of globalization and cross-border ownership, it is not uncommon for information sought in discovery in US proceedings, including ESI, to be located outside the United States. Access to such information is complicated by the unique and differing perspectives of foreign jurisdictions toward the disclosure of such information. Consider the potential discoverability of such foreign data and that privacy laws may complicate or prevent compliance with discovery of foreign data in US litigation.

Effectively managing legal holds in large companies with substantial litigation dockets can be complex and involves significant risk. The process will go more smoothly and risk will be better managed where the company has proactively developed an effective program and adopted technology to help with the process. This can make the difference between defending a case on its merits or fighting primarily about alleged spoliation.

For inquiries related to this Tip of the Month, please contact Bob Entwisle at rentwisle@mayerbrown.com or Kim Leffert at kleffert@mayerbrown.com.

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

Please visit us at www.mayerbrown.com

MAYER·BROWN

Electronic Discovery & Records Management

Tip of the Month

How to Manage the Risks and Costs Associated with Searching ESI

Scenario

A large corporation is served with a complaint accusing it of participating in a price-fixing conspiracy. Multiple discovery requests follow seeking electronically stored information (ESI). In-house counsel speaks with the company's IT department to estimate the scale of the review and is disturbed by the sheer number of files to be reviewed. How can a meaningful review be accomplished in a reasonable time frame in a cost-effective way?

The Risks Associated with Using Search Terms

The use of search terms has become the new panacea of many electronic discovery vendors that trumpet the use of technology to reduce the costs of identifying relevant documents and the number of documents that need to be reviewed. But some critics contend that keyword searches may fail to identify potentially relevant information. As Magistrate Judge Paul Grimm observed in his 2008 *Victor Stanley* decision, "while it is universally acknowledged that keyword searches are useful tools for search and retrieval of ESI, … there is a growing body of literature that highlights the risks associated with conducting an unreliable or inadequate keyword search or relying exclusively on such searches."

While no computer-assisted information retrieval (IR) system yet developed can simply scan through a mountain of data and infallibly identify exactly those documents that an attorney would deem relevant, many IR options exist beyond traditional keyword searches that can reduce the risks associated with using search terms. For example, established search algorithms, commonly called "Boolean" or "set-theoretic" models, make binary decisions regarding the responsiveness of documents based on various simple tests, such as the presence of keywords within a certain distance of one another, linked by AND, OR, and NOT. A document is judged as either responsive or not, with no middle ground. Other search approaches, often broadly gathered under the rubric of "concept searches," move beyond this paradigm in a variety of ways.

Mitigating the Risks Associated with Using Search Terms

There are several ways to mitigate the risks of using traditional keyword searching. While not all of these options are appropriate in every case, consideration should be given to the following factors:

- Even within the Boolean paradigm, search tools can take advantage of "fuzzy" text comparisons and auxiliary structures such as thesauri to expand upon the queries generated by attorneys and thereby deal with the misspellings, optical character recognition (OCR) errors, synonymy (multiple words for a single concept) and polysemy (multiple meanings for a single word) that plague keyword searches. The keyword search also can be enhanced by interviewing key custodians about the language that they use in correspondence, and by consulting with electronic discovery experts who are trained in keyword search development.
- "Algebraic" IR methods generate a measure of how similar each document is to what a query ideally seeks, thereby enabling the tool to *rank* documents by relevance rather than simply assigning them to two undifferentiated camps: responsive and non-responsive.
- "Probabilistic" or "Bayesian" search algorithms make use of more user input than simply the initial query in order to estimate a particular document's relevance.
- Tools such as domain name restrictions, discussion threading, topic clustering, people analytics, and analytics to identify duplicate copies of files can facilitate effective review.

The advantages of choosing a search system that is suited to your particular problem can be significant. By ranking documents rather than simply tagging all responsive documents as equally good, algebraic and probabilistic algorithms facilitate faster identification of key documents. By taking into account reviewers' tagging decisions and not simply the initial query, these systems reduce the need for humans—who charge by the hour—to keep repeating their recommendations. (Systems can be calibrated to permit some redundancy, to ensure that tagging mistakes do not poison an entire search.) Seemingly abstruse discussions of IR algorithm improvements quickly resolve themselves into bottom-line impacts in terms of the cost and time required to respond to discovery requests.

The Risks Associated with Using Concept Searching

If the use of concept searching can reduce risks and costs associated with retrieving relevant documents, why are these tools not already more popular among lawyers? There are several remaining risks:

- There is not yet much case law certifying non-Boolean search methods as acceptable. While this is changing—for example, in a 2007 opinion, Judge Facciola of the District Court for the District of Columbia noted that "recent scholarship … argues that concept searching, as opposed to keyword searching, is more efficient and more likely to produce the most comprehensive results," —the use of concept searching remains untested in the law, and opposing lawyers may balk at its use. On the other hand, successfully challenging the thoughtful use of Bayesian concept clustering is much more difficult and complicated than simply pointing to omitted search terms in a Boolean search string.

- Boolean search tools are ubiquitous and fungible. By contrast, software packages supporting concept searching are less well known. Each package comes with its own idiosyncratic user interface (no universally agreed syntax here). And there are significant differences between mathematical concept searching and thesaurus based concept searching. Thus, choosing a quality vendor can be a bigger challenge.
- Boolean searches generate output that lawyers understand—or at least think they do. The output of a keyword search is a list of documents that match the search query and, more importantly, a list of documents that do not. When asked if all responsive documents have been produced, an attorney who trusts keyword searches implicitly will answer, without reservation, "yes." The *ranked* output from an algebraic or probabilistic search provides no bright lines and, thus, requires more nuanced communication with the court. This distinction just makes explicit the uncertainties that are already present in Boolean searches that the binary output obscures: user-defined queries are far from perfect, and the statement that no document responsive to the *search query* has been withheld is a far cry from certification that no document responsive to the *document request* has been withheld. Nontraditional search algorithms do not create this uncomfortable truth; they just bring it to the fore.

Regardless of the information retrieval methodology selected, documentation of which model was chosen and how it was implemented is an important tool to facilitate defense of the chosen process.

So, which search method is right for you? That can vary based on the types and volume of documents searched, the time frame and budget permitted, your aversion to risk, and your organization's comfort with technology, among other factors. But if the universe to be searched is large and costs are likely to be scrutinized, consideration should be given to making use of concept search technology, especially as prices for such technology have fallen dramatically.

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

Please visit us at www.mayerbrown.com

June 2010

MAYER·BROWN

Electronic Discovery & Records Management

Tip of the Month

Protecting Confidential Electronically Stored Information

Scenario

A sales person for a large, multi-national corporation keeps confidential customer and sales information on her laptop. During the course of a litigation against the corporation, some of the confidential information must be collected, reviewed and potentially produced. The sales person works at a small, remote office. The in-house lawyer is tasked with ensuring that the confidential information is collected properly, that only appropriate information is produced and that the risk of inadvertent disclosure is minimized.

Types of Confidential Information

Confidential information includes intellectual property, corporate secrets, customer health and financial information, social security numbers, driver's license numbers, customer addresses, credit and debit card information and even Internet browsing habits. Federal and state regulations, such as the Sarbanes-Oxley Act, the Health Information Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act, Right to Financial Privacy Act, the Bank Secrecy Act and the Fair and Accurate Credit Transactions Act, have created legal definitions of confidential information, and have established legal requirements for maintaining the privacy of that confidential information. States are also promulgating comprehensive privacy and data breach regulations and disposal requirements to address shortcomings in the existing patchwork federal regulation.

Establishing a Policy for Managing Confidential Information

Corporate policies and procedures should be established to create a uniform approach to the maintenance and potential disclosure of confidential electronically stored information (ESI) in order to properly address the issue of protecting confidential ESI and the obligations that arise as a result of the relevant rules and regulations as well as existing business relationships. These policies and procedures should outline the appropriate steps in the event that there is unauthorized access to ESI containing sensitive personal information. Currently, 47 US states plus the District of Columbia have data breach statutes that require timely notice to affected individuals in the event that their sensitive personal data is subject to unauthorized access. These statutes may also require notification of the state attorney general or other agency, law enforcement or the consumer reporting agencies. Without policies and procedures setting

forth the required steps, it may be difficult to discharge your legal obligations under these laws in a timely manner.

Although technology exists that can help maintain the privacy and security of confidential ESI, its effectiveness depends on the implementation of policies and procedures by organizations to protect the information. Moreover, an established protocol will facilitate the process of responding to a legal request in a timely and sufficient manner, while at the same time protecting privileged and confidential information and minimizing litigation costs.

Identifying Sources of Confidential Information

Companies should be aware of the wide variety of data sources that potentially house their confidential information, including networks, servers, laptops, portable media, shared drives, web sites and backup tapes. It is good practice to maintain an inventory of these sources and the confidential information that is maintained on each. Furthermore, companies should carefully catalog and monitor the confidential information provided to their vendors and take steps to ensure that the vendor maintains adequate policies and procedures to safeguard such information.

Organizations that utilize "cloud computing" need to take additional precautions in addressing confidentiality concerns. The use of integrated internet-based software, including the use of online programs for managing client relationships, maintaining data, and performing other IT-based services creates additional sources that may maintain confidential information, and should be incorporated into all relevant policies and procedures.

Assess Risks Associated with Each Source

After identifying the sources of confidential ESI, organizations should conduct an assessment of the risk associated with the disclosure of the information contained on each source. In conducting that assessment, the organization should consider the relevant regulatory obligations and the likelihood that the source will contain information that will be relevant to litigations. Confidential ESI can then be classified based on the results of the risk assessment, and policies and procedures can be developed for management, storage and backup of the various types of confidential ESI.

Establish Procedures for Maintaining Each Source of Confidential ESI

The policies and procedures for maintaining confidential ESI should establish rules for each data source, with designated custodians for each data type and application. Responsibilities for maintaining the security of these data sources should be allocated among data custodians and the IT department to prevent, identify and repair breaches in security.

It is also important to educate employees regarding the types and forms of confidential ESI that the company maintains, the relevant rules and regulations, the importance of protecting the privacy of that information and the security measures implemented to protect the information. For example, if employees are permitted to maintain confidential information on portable media devices, such as laptops

and flash drives, or if employees regularly transmit confidential information, they should obtain training with respect to the use of data encryption technology or other security devices. To the extent that that sensitive personal information is encrypted, the theft or loss of a portable media device or misdirection of email may not trigger the notice requirements under the state data breach laws.

A protocol should be incorporated for the regular updating of confidentiality policies and procedures. This may require the organization to periodically assess new sources of confidential information, new mechanisms to protect that information and new rules and regulations. In addition, organizations should consider periodically auditing the existing security measures.

Protecting Confidential ESI Requested During Discovery

A litigation or government investigation may require the production of confidential and private information. In civil litigation, it is common for the parties to enter into confidentiality agreements that dictate how confidential information will be treated. Pursuant to Rule 26(c) of the Federal Rules of Civil Procedure, a party may seek a protective order providing that confidential information may not be revealed or that it must be used in a limited manner. Protective orders and confidentiality agreement are sometimes reviewed and approved by the courts. Relevant factors to consider in drafting a protective order or a confidentiality agreement include:

- A tiered approached to confidentiality designations (for example, designations of confidential and highly confidential)
- Case-specific definitions of what would fall into each tier of confidentiality
- The manner in which confidential information can be used (for example, attorney's eyes only)
- Procedures for use of confidential information in court filings, at depositions, at trial and in expert discovery
- Use of confidential information outside of the litigation or investigation
- Production of confidential information in response to requests from third parties
- Return or destruction of confidential information after a litigation has concluded
- Procedures to correct an inadvertent failure to designate a document containing confidential information
- Procedures to challenge a confidentiality designation

Keeping confidential ESI protected should not be the concern of only the Risk Management and IT departments. Knowing where confidential ESI is kept, and having policies and procedures to maintain the confidentiality, will enhance protective measures needed due to inadvertent loss or required production.

For inquiries related to this Tip of the Month, please contact Jeffrey P. Taft at jtaft@mayerbrown.com, Kim Leffert at kleffert@mayerbrown.com or Rebecca Kahan at rkahan@mayerbrown.com.

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

Learn more about Mayer Brown's Privacy & Security practice or contact Rebecca S. Eisner at reisner@mayerbrown.com, John P. Mancini at jmancini@mayerbrown.com or Jeffrey P. Taft at jtaft@mayerbrown.com.

Please visit us at www.mayerbrown.com

July 2010

MAYER·BROWN

Electronic Discovery & Records Management

Tip of the Month

Managing the Risks and Costs of Preserving and Producing Structured Data from Databases

Scenario

A large pharmaceutical company maintains data related to its research and development in several proprietary, structured databases. The information contained in the database is regularly updated with results of new trials. The company receives a subpoena from a regulatory agency requesting documents related to clinical trials that were completed in advance of releasing a new product. To fully respond to the subpoena, information maintained in those databases must be collected, reviewed and potentially produced. The in-house lawyer responsible for the response to the subpoena is asked to identify all of the relevant sources of information, as well as any potential issues associated with the collection, review and production of information from those data sources.

Structured Data from Databases

An organization may have numerous data storage systems that are updated or changed over time, such as a database of customers, a document management system, or a database that holds information about clinical trials. The data in such databases are dynamic, and they create additional issues for an entity to consider when responding to a request for information, including: What is the best way to generate data from the database? When must an organization preserve the incremental changes for later production in litigations? What are the costs associated with collection, review and production of data?

Databases are typically large, and they do not lend themselves to traditional methods of document review. The raw data that are contained in the databases can be difficult to interpret in isolation, and it is often impractical to produce in litigation the myriad programs that utilize those raw data. Additionally, many databases create, update and discard certain information automatically. Terminating those functions is often impossible without disruption to the organization and, even in instances where it can be done, is typically costly and burdensome.

While it may not be practical or even necessary to save every incremental change to a database, there may be situations in which an entity should be prepared to preserve all electronically stored information (ESI) if

the ESI is relevant to pending or foreseeable litigation. Although Federal Rule of Civil Procedure 34(a) provides authority for compelling a recalcitrant party to either produce information or allow direct access to a database, the duty to preserve data does not require a party to undertake creating storage systems or installing software. In certain circumstances, it may be sufficient to produce summary reports out of databases.

To best address the issues associated with the collection, review and production of structured data from databases, an entity should be prepared to address the sources of potentially relevant data, the scope of review and the potential use of summary reports during the early stages of a litigation or investigation. Early discussions should focus on any unique preservations issues, such as the use of summary reports to capture the data contained in the database. If no agreement is reached and information in the underlying database changes in a significant manner by the time a report is eventually generated, a producing party risks spoliation sanctions or an order granting the opponent full access to the database.

Be Prepared for Discussions in Advance of Receiving a Subpoena

In order to be prepared for such discussions shortly after receiving a request for production, organizations should implement policies and procedures for identifying, and cataloging information regarding the databases that it maintains.

Develop Data Source Catalogs

An organization should consider developing a data source catalog as part of an effective information management program. This catalog would contain fact sheets on key data sources likely to be relevant across multiple litigations and investigations. A careful, updated catalog, prepared in cooperation with the IT department, can facilitate discussions about preservation and collection decisions for key data sources without the need to repeat the investigative process in each litigation or investigation.

A data source catalog could include the following categories, depending upon the nature and use of the application at issue:

- Data source
- Business area
- Key contacts
- Key functionality
- Brief description
- Inputs
- Outputs
- Date range and retention policy
- Backup schedule
- Retention period for backups
- Preservation considerations
- Production considerations, including whether system stores confidential or proprietary information
- Scheduled upgrades

- Legacy data sources
- Comments

Obtain Comprehensive Understanding of Relevant Systems

An organization should take steps to develop an understanding of all dynamic or transitory systems that are frequently sourced for litigations, investigations or third-party requests, and that understanding should be documented. In-house counsel should take steps to understand the burden of preserving and producing data from these systems, including any potential impediments to reviewing that data (such as the need for proprietary software) and costs associated with maintaining that data. Additionally, in-house counsel should be prepared to advise outside counsel of these issues.

Develop and Follow Guidelines for When to Preserve Data

Developing and following guidelines that incorporate an organization's understanding of any relevant dynamic or transitory systems is a way to ensure consistency of approach within the organization. These guidelines should provide guidance on when to agree to "snapshots" of such data, as well as the timing and frequency of such snapshots.

Develop Standard Disclosure Documents Regarding Data from Dynamic and Transitory Systems

To avoid possible misrepresentations or failures to disclose potentially relevant data, and to ensure consistency, an organization should consider developing and maintaining standard descriptions of its database applications that are often relevant to litigations, investigations and third-party requests. The process of developing those disclosures, along with the information about the appropriate internal burdens and costs, will be useful to outside counsel and will provide insights into the appropriate fact witnesses should it become necessary to object to preservation demands. To keep up with regular changes and updates to systems, the organization should consider a policy for regularly updating those disclosures.

For inquiries related to this Tip of the Month, please contact Rebecca Kahan at rkahan@mayerbrown.com.

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

Please visit us at www.mayerbrown.com

August 2010

MAYER·BROWN

Electronic Discovery & Records Management

Tip of the Month

Preserving Data on Custodians' Personal Email and Personal Phones, Devices and PDAs

Scenario

A large manufacturer is served with a class action complaint alleging that the company knowingly produced products that were unsafe in certain circumstances. In-house counsel meets to discuss and identify electronically stored information (ESI) that may be responsive to the complaint and learns that one potentially relevant source of information is employee text messages. While the company issues and supports BlackBerrys, many employees who may be custodians of data relevant to the litigation send work-related messages from their personal, unsupported cell phones, smartphones and PDAs.

Protecting Employee's Reasonable Expectation of Privacy while Meeting Discovery Obligations

If in-house counsel knows, or should know, that employees use personal devices or personal email for work-related communications, a duty to preserve—and potentially collect—that data may arise. Although the Federal Rules of Civil Procedure do not specifically address personal email, text messages or other information stored on personal devices, the 2006 Amendments adopted a broad definition of ESI that encompasses data "stored in any medium" from which it can be obtained and "translated, if necessary" into a "reasonably usable form." As a result, failure to preserve and, if necessary, collect information that is relevant to a lawsuit and that is stored on a personal device or sent through personal email accounts may expose an organization to claims of spoliation.

In fulfilling the obligations set forth in the Federal Rules, both in-house and outside counsel should be aware that the decision to preserve and/or collect data held on a personal device or sent through a personal email account can present issues with respect to employee privacy rights. Communications sent via personal devices or personal accounts, such as text messages, are often highly personal and sensitive in nature. If employees have a reasonable expectation of privacy in their communications sent via personal devices or personal email, either under state or federal statute or company policy, employers should be aware of their employees' rights when collecting such communications for discovery purposes.

Further, the law regarding employees' expectations of privacy in work-related electronic communications sent from personal devices or personal email is unsettled. For example, while some courts have held that

employees have a reasonable expectation of privacy in password-protected personal email accounts, even when accessed through a company-issued laptop, others have found an employer's search of its employee's text messages to be reasonable. The SEC has recently indicated that the recordkeeping requirements of the Securities Exchange Act encompass the personal email accounts of a broker-dealer's employees that were used for business-related activities. As a result, employers should proceed with caution and take steps to avoid any potential conflicts between privacy rights and discovery obligations.

Be Prepared to Respond to Requests for ESI

There are few clear-cut rules for how work-related data stored on a personal device, or work-related communications sent via personal email accounts, should be treated. Taking a proactive stance in considering and responding to the challenges such data presents can prevent conflicts down the road. Some issues that should be considered include:

- *Understand the company culture*. If employees are accustomed to sending and receiving work-related communications via personal devices or personal email, a policy that bans them outright is likely to fall victim to workarounds by resourceful employees. For example, disabling text messaging on company-issued phones or PDAs may simply lead to the less desirable outcome of work discussions occurring on personal phones.
- *Determine what devices to support*. The technology supporting cell phones, smartphones and PDAs is constantly changing, and each new device stores more information than the next. For example, permitting employees to receive company email messages on their iPhones may raise data collection issues, since those devices can store significant amounts of information. Similarly, allowing an employee to direct work related email messages and other such communications to personal hand held devices rather than company-issued devices can create additional challenges for employers in responding to discovery requests.
- *If not currently allowed, consider authorizing the use of work-related text messaging on employer-issued phones or PDAs*. There are numerous benefits for employers to issue and encourage employee use of such employer-issued devices. First, courts are less likely to find that an employee had a reasonable expectation of privacy in a company-issued device, thus minimizing potential privacy related conflicts. Second, messages can be set up to synchronize to the company server. In such instances, the messages stored on the devices themselves may be considered duplicative and unnecessary for production, thus minimizing the burden of collection from individual devices. Finally, uniformly supported devices minimize technological hurdles to collecting text messages, including translating data from multiple formats and maintaining the necessary tools and trained staff to collect from any number of unsupported phones or PDAs. In particularly sensitive matters, where information must be produced in its native format, this advantage becomes particularly salient.
- *Be prepared to explain the burdens and costs associated with preservation and collection*. Open and up-front conversations with opposing counsel about potential sources of relevant information and the burdens associated with collection and production can reduce the risk that an opponent will make a spoliation claim if certain data are not preserved. If both parties face the same challenges

with preserving and collecting work-related data stored on a personal device or work-related communications sent via personal email, the parties may agree to forgo or limit the preservation or collection of such data.

- *Have a written policy and follow it*. Organizations can consider adopting a clear policy about the use of personal devices and personal email accounts that is communicated to all employees. That policy may include the use of periodic audits for compliance. Courts may be more likely to find that a company's response to a discovery request was reasonable if they follow established policies.
- *Provide formal training to employees about the corporate policy*. It is important to educate employees about corporate policies and to make sure that they understand the risks associated with failure to comply. If employees are trained to only use work-issued devices and work email systems for work-related discussions, a court may be more sympathetic to the argument that collecting employees' personal phones is an undue burden.

In our mobile society, the line between personal and work-related communications is increasingly blurring. Organizations should be aware of the potential existence of, and risks associated with, work-related data stored on a personal device or work-related communications sent via personal email, and should take proactive steps to develop policies and strategies for managing those risks before litigation arises.

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 Michael Baltus at mbaltus@mayerbrown.com.

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

Please visit us at www.mayerbrown.com

MAYER·BROWN

Electronic Discovery & Records Management

Tip of the Month

Managing E-Discovery in State Courts

Scenario

A large pharmaceutical company recalls a product after serious safety-related concerns are raised. The company subsequently is faced with multiple lawsuits in state courts throughout the country. In-house counsel anticipates that plaintiffs' counsel will propound broad discovery requests seeking, among other things, electronically stored information ("ESI") from multiple custodians located in numerous e-mail accounts, databases and back-up tapes. In-house counsel is concerned with the prospect of complying with the e-discovery rules in each of these state courts.

E-Discovery Regimes in State Courts

In 2006, the Federal Rules of Civil Procedure were amended to provide a uniform set of rules across the federal courts to govern the preservation, collection and production of ESI. Most in-house and outside counsel who regularly litigate complex disputes are familiar with these federal e-discovery rules. At the state level, however, in-house and outside counsel must navigate a more byzantine legal landscape.

Some states – Alaska, Arizona, Arkansas, California, Indiana, Iowa, Kansas, Maine, Maryland, Michigan, Minnesota, Montana, New Jersey, New Mexico, North Dakota, Ohio, Utah, Vermont, Virginia, Washington, Wisconsin (effective 2011) and Wyoming – largely follow the 2006 amendments to the Federal Rules of Civil Procedure. Other states – Idaho, Mississippi and Texas – have enacted e-discovery rules that do not track the Federal Rules of Civil Procedure. A third group – Louisiana, Nebraska, New Hampshire and New York – have borrowed a more limited number of concepts from the Federal Rules of Civil Procedure and tweaked them to suit their needs. And Tennessee has enacted a unique set of rules that are an amalgam of a variety of sources. The remainder of the states have yet to address e-discovery through rule-making.

Diversity of State E-Discovery Rules

Counsel should also be aware that different states may take different approaches to the same e-discovery issue and that some states have developed unique rules and procedures. Initial disclosures are one example. Alaska, Arizona and Utah follow Federal Rule 26(a)(1)(A)(ii), and require that parties provide a

copy or description of ESI to all other parties in the litigation. Other states do not have similar provisions in their rules and procedures.

Meet-and-confer and preliminary conference requirements offer more examples. Some state courts, such as those in the Commercial Divisions of New York and Delaware, follow the framework of Federal Rules 16(b) and 26(f) and require that counsel discuss e-discovery issues at meet-and-confer sessions before attending mandatory preliminary conferences at which courts may "so-order" parties' discovery plans. Other states, such as Minnesota, grant parties the discretion to raise e-discovery issues at preliminary conferences with courts by motion.

State requirements may also differ on cost allocation. Delaware, for example, follows the federal presumption that costs associated with producing ESI will be borne by the producing party, while New York generally follows a requester-pays presumption under which the requesting party pays the cost of production, including costs associated with ESI. Other states have enacted cost-shifting statutes. Texas, for instance, has a mandatory cost-shifting statute where courts must order that the requesting party pay the reasonable expenses of any extraordinary steps undertaken by the producing party where the producing party shows that the data is not reasonably available. Idaho has enacted a similar statute that grants discretion to – rather than requires – a court to shift costs to the requesting party. Still other states have e-discovery requirements that address particular cost-allocation issues. In California, the Court of Appeal for the Sixth District held that the California Code of Civil Procedure mandated the requesting party to pay the costs of producing and translating ESI from back-up tapes into reasonably usable form even without a showing of undue burden or expense from the responding party. A nearly identical cost-shifting provision was included in California's Electronic Discovery Act of 2009 to apply in the context of producing ESI in response to a subpoena.

Absent guidance from state legislatures, state court administrators have also crafted e-discovery rules that are unique to their courts. For instance, New York, prompted by a recommendation in a comprehensive report regarding e-discovery in the state's courts, recently amended its administrative code to oblige counsel appearing at a preliminary conference to be "sufficiently versed in matters relating to their clients' technological systems to discuss competently all issues relating to electronic discovery[.]" Although counsel is allowed to bring a client representative or outside expert to the preliminary conference, it appears that counsel retains the primary obligation to be informed of these systems or face possible sanctions.

Navigating State Court E-Discovery

Organizations faced with litigation in state courts should consider developing e-discovery strategies that take into account the specific rules of each jurisdiction. To assist in that effort, some practical guidelines can be used to navigate state court litigation regardless of where a particular litigation arises:

- *Understand the nuances of the e-discovery rules in particular state courts*. There is no uniform body of rules governing e-discovery at the state level. Some states have failed to enact rules specifically addressing e-discovery and those states that have may or may not track the more familiar e-discovery rules set forth in the Federal Rules of Civil Procedure. Counsel should, therefore, become

familiar with the statutes, rules and case law that govern the preservation, collection, review and production of electronically stored information in the particular state court that will supervise discovery.

- *Facilitate discussions between outside counsel and the company's information technology personnel regarding the company's technological systems*. To ensure that outside counsel is prepared to propose reasonable e-discovery plans that are in harmony with an organization's actual systems and capabilities – as well as to defend that plan before the court – in-house counsel should take steps to ensure that outside counsel becomes familiar with the company's current and legacy electronic information systems, including any disaster recovery systems. In-house counsel may want to consider designating an employee who is thoroughly knowledgeable about these systems to educate outside counsel and also the court if necessary.
- *Develop an e-discovery plan in anticipation of a meet-and-confer with opposing counsel and a preliminary conference with the court*. Being prepared to address e-discovery issues early in the litigation can avoid later motion practice and complications. In-house counsel and outside counsel should work together to develop an e-discovery strategy as soon as the complaint is served – or even before if the organization reasonably anticipates litigation – and prior to contacting opposing counsel. Craft a list of questions regarding e-discovery to ask opposing counsel at the meet-and-confer session and prepare answers to these questions in the event the court asks similar questions at the preliminary conference.
- *Be aware of cost allocation rules*. Cost allocation rules will inform not only discovery strategy but also motion practice and ultimately settlement discussions. Where a state offers no clear rules on cost-shifting and instead applies a judicially created multi-factor test, counsel may want to seek a stipulation on cost allocation that the court can "so-order" at a preliminary conference to ensure clarity on this all important issue. If a cost allocation dispute cannot be resolved among the parties, counsel should seek court intervention *before* any ESI costs have been incurred.

For inquiries related to this Tip of the Month, please contact the authors, Anthony J. Diana at adiana@mayerbrown.com, Norman Cerullo at ncerullo@mayerbrown.com or James Ancone at jancone@mayerbrown.com.

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

Please visit us at www.mayerbrown.com

Electronic Discovery & Records Management

Tip of the Month

E-Discovery and Social Media

Scenario

The Equal Employment Opportunity Commission (EEOC) files a discrimination action against a multinational organization in federal court on behalf of employees who claim ongoing emotional distress caused by a hostile work environment. The organization receives a discovery request from the EEOC seeking the production of the personal Facebook and MySpace profiles of the employees accused of the discriminatory acts. The discovery request seeks the accused employees complete social media profiles, including their status updates, wall comments, photographs and activity streams.

The Proliferation of Social Media

The use of social media such as Facebook, MySpace, Twitter, YouTube and LinkedIn has exploded over the past few years. One study found that online social media use has risen more than 230 percent over the last three years. The ubiquity of social media has made it impossible for organizations to ignore. Seventy-nine percent of the Fortune 100 companies use at least one social media platform to communicate with their customers, and 20 percent of companies are using all four of the main social technologies (Twitter, YouTube, Facebook, and blogs). Social media can increase public awareness of an organization, offer branding and public relations opportunities, increase interaction between employees and consumers, and increase productivity by enabling time-sensitive access to information.

The Legal Treatment of Social Media

Although the content on social media sites is increasingly at issue in legal disputes, the legal system has been slow to articulate consistent guidelines for its treatment in litigation. By using email and other electronic communication formats as precedent, courts and regulators have looked to the Federal Rules of Civil Procedure and other laws—such as the Stored Communications Act of 1986—for guidance. But reference to decades-old electronic communication laws to analyze issues related to cutting-edge electronic communication through social media has translated into a perplexing mix of court decisions around the country. In particular, courts have grappled with an individual's privacy concerns when weighing whether content on social media sites is discoverable.

While individuals generally believe that information posted to a social media account with privacy settings is private and protected from disclosure, those privacy settings may not prevent disclosure when the content is relevant to a litigation. For example, one court ordered the production of content from the plaintiffs' Facebook and MySpace accounts where the plaintiffs' alleged damages included emotional distress. The court noted that the privacy settings on the social media sites did not provide a basis for protecting content from discovery.

In contrast, another court shielded from discovery the content from a plaintiff's Facebook and MySpace account to the extent that the content was not available to the general public. Still other courts have found that certain types of information on a Facebook account may be discoverable, while other types—such as pictures linked from another user's Facebook account—may not.

In addition to the legal standards promulgated by the courts, organizations should be aware that regulators have also recognized the relevance of communications via social media. For example, the Financial Industry Regulatory Authority (FINRA) recently issued guidance on the use of social media sites that requires member firms to retain records of communications with customers through social media sites related to the firms broker-dealer business, just as they would for other communications. And where an organization is required to retain certain types of communications, it can expect that those communications will be discoverable when relevant to a subsequent litigation.

Best Practices: Know the Risks & Develop a Plan

The legal uncertainty regarding social media in discovery—and the lack of standardized protocols for preservation, collection and production—makes managing the risks associated with social media use a challenge. Some organizations view the risks posed by social media as too great, banning the use of social media by employees as a matter of policy. However, as with most new technologies, a complete ban on the use of social media may be impractical for most companies.

- *Understand the risks associated with different types of social media use*. Use of social media can be organized into three categories, each of which presents different risks to an organization.
    - *Organization-sponsored, outwardly facing sites*. These sites are created by the organization to fit clear objectives. The content often creates a formal organizational presence on the social media site and is geared toward disseminating information to customers and others outside of the organization. In theory, this type of social media use is easier for the organization to control, but it presents many of the same risks associated with communications with customers through other means.
    - *Internal sites and blogs.* These types of social media facilitate communication within an organization. They focus on increasing productivity and employee interaction, and may create risks of discrimination or other employment-related claims.
    - *Employees' personal sites*. Use of this type of social media generally lacks organizational goals, but may nonetheless associate the user with the organization. Personal social media sites also give rise to the most confusion regarding privacy issues and whether the organization "controls" an employee's personal social media accounts for purposes of

discovery. The risks represented by these sites include misrepresentations about the organization by the employee, associating improper conduct by the employee with the organization or revealing confidential information to the public.

- *Understand how the organization uses social media*. Conduct an inventory of the social media being used by the organization and its employees, determine how they are being used and identify which are the most beneficial to achieving the organization's goals. Analyze the risks associated with social media in the context of the organization's business plan.
- *Develop policies and procedures*. Develop policies and procedures that ensure the organization and its personnel comply with the applicable requirements. Policies and procedures must consider social media in the context of the organization's business and its compliance and supervisory programs. A policy should clearly identify the individual employees, teams or groups authorized to access social media for the organization's benefit and to associate themselves with the organization in their personal social media accounts.
- *Ensure proper training*. Proper employee training and clear management communication are essential to the success of a social media policy. Employees must understand not only the risks presented by social media use to the organization and themselves, but also the benefits of appropriate use of this technology.
- *Enforce social media policies*. An organization must enforce its social media policies and procedures by incorporating them into current enforcement and compliance programs. Enforcement of a social media policy may require collaboration among an organizations' information technology, human resources and legal departments.
- *Anticipate discovery concerns*. Advanced planning can reduce the risks associated with preserving and producing information from social media sites. Develop a legal hold plan that incorporates social media and be prepared to discuss those issues with opposing counsel.

For inquiries related to this Tip of the Month, please contact Michael E. Lackey at mlackey@mayerbrown.com, John Nadolenco at jnadolenco@mayerbrown.com, or Justin Dillon at jdillon@mayerbrown.com.

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

Please visit us at www.mayerbrown.com

November 2010

MAYER·BROWN

Electronic Discovery & Records Management

Tip of the Month

Managing the Risks of Cloud Computing

Scenario

The IT department of a large international company is in the process of negotiating a contract with a cloud computing provider to maintain and hold all of the company's electronically stored information and data. The company's Chief Information Officer asks its General Counsel to review a nearly final draft of the contract with the cloud computing provider to make sure that any potential risks that might accompany the transition are addressed in the agreement.

What is Cloud Computing?

Cloud computing is Internet-based computing; it involves the use of remote computing resources that are usually shared and/or distributed rather than dedicated and centrally located. Cloud computing is generally a subscription-based service that satisfies both computing and storage needs with an infrastructure based in the Internet. Cloud computing, thus, is physically limitless, and can then be accessed by users "on demand" from virtually anywhere with an Internet connection with minimal administrative effort. This service is managed by a third-party provider rather than an internal IT department. For example, Gmail, Google's free email service, stores email "in the cloud" which means that any user's email "mailbox" may actually be stored in one of several different servers located all over the world and can easily be accessed from anywhere on the Internet.

Some of the benefits of cloud computing are that it potentially reduces costs and increases efficiency by freeing a company's IT department from the need to own and service its own hardware and software. Thus, many businesses are seeking to take advantage of the still-evolving technological development.

Potential Risks: Redefining "Possession, Custody and Control"

From a litigation and investigation perspective, storing a company's data in the cloud can lead to concerns about compliance with the company's obligations to preserve and produce electronically stored information ("ESI"). For example, although it may not technically be in the company's possession or custody, cloud-based ESI may still be considered to be in the company's "control," even though the company has little or no say over whether and when the ESI is destroyed, and even though the company may not have any assurance that the cloud provider will implement a legal hold correctly and quickly. The

company may also have limited access to its own data, and the access it does have may be insufficient or too slow to meet court requirements for production of ESI.

Another risk is that ESI may be co-mingled with the ESI of another company or of a separate but related corporate entity. This can lead to problems determining what entity actually has "possession, custody and control" of data and is under an obligation to preserve or produce it.

Finally, given that a cloud computing provider may store data in any one of its many servers anywhere in the world, storage in jurisdictions with strict data protection and transfer laws may complicate access and retrieval of this data.

Tips for Managing the Risks of Cloud Computing

- Ensure that the legal and compliance departments understand fully what data will be stored, or is being stored, by the company in the cloud, ideally before decisions are made to store the data.
- Develop procedures to ensure that data can be preserved and collected in a timely manner in response to a legal hold.
- Negotiate with the cloud computing provider to ensure that the service contract contains provisions that protect the company's interests and its need to comply with preservation and production obligations, including, if possible:
    - 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 needs the ability to reasonably direct acts of the provider to preserve and produce ESI for purposes of litigation.
    - Cooperation: The provider needs to be willing to comply with the company's directions regarding its ESI and ensure compliance with any and all legal holds.
    - Speed: The provider must agree to cease any data destruction (to comply with a legal hold) in a timely manner and produce data with sufficient speed to meet the company's obligations.
    - Metadata: The company should inquire in what form or format the data will be stored and returned for production during litigation, including whether metadata will be in tact.
    - Costs: Beyond the price of subscription 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: Ensure that the contract addresses confidentiality, data integrity and availability issues, including whether data will be commingled with data of other cloud customers.
    - Jurisdiction: Discuss with the provider where the data will be maintained. 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: Inquire about the security measures that the provider has in place to protect data privacy and attorney-client privilege. Determine if the company will be informed of a security breach.
- Policies: Determine whether the provider has policies and procedures that may impede the company's obligations to preserve, collect and produce ESI during litigation.
- Disaster Recovery: Have plans for what happens if a server crashes or data is otherwise lost or if the provider goes bankrupt or out of business. Stipulate that contractual provisions will continue to remain in force if the provider is acquired by another company.

The best way to manage the inherent risks associated with the use of cloud computing in relation to a company's obligations in litigation and regulatory investigations is to obtain a comprehensive understanding of how the company plans to use the cloud computing, and take pro-active steps to establish procedures and contract terms before the need arises to preserve and collect data from the cloud.

For inquiries related to this Tip of the Month, please contact Michael E. Lackey, Jr. at mlackey@mayerbrown.com, Kim Leffert at kleffert@mayerbrown.com, or Katie Fernandez at kfernandez@mayerbrown.com.

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

Please visit us at www.mayerbrown.com

December 2010

MAYER·BROWN

Electronic Discovery & Records Management

Tip of the Month

Preservation Obligations and Insurance Policy Notification Clauses

Scenario

An accounting firm becomes aware through news reports of the collapse of an alleged Ponzi scheme. Several of its audit clients are investment funds that are victims of the scheme. The accounting firm consults with counsel about whether the accounting firm has insurance coverage if sued by the investment funds for failure to discover the fraud and is advised that it should give its insurers notice that a circumstance has arisen that may give rise to a claim. The accounting firm is unsure whether notifying its insurers also triggers its obligation to preserve evidence relevant to potential future litigation.

Duty to Preserve

The duty to preserve evidence arises when an organization has notice, either actual or implied, that evidence in its custody or control is or may be relevant to current or potential litigation involving that party. Once an organization has such notice, it must suspend its normal document retention/destruction practices and put in place a legal hold to ensure that evidence is preserved. While notice is most commonly evidenced through the filing of a lawsuit or the receiving of discovery requests, other circumstances may also trigger an organization's duty to preserve.

It is commonly stated that an organization's duty to preserve is triggered when that organization "reasonably anticipates litigation." But where there is no complaint or discovery demand, there is no bright-line test for assessing whether a legal hold must be issued. Rather, a more fact-intensive inquiry is required to determine when an organization has sufficient notice to be subject to a duty to preserve evidence.

In determining whether an organization was subject to an obligation to preserve, courts commonly consider whether that organization exhibited a "fear" of litigation. For example, courts often consider the fact that an organization made comments discussing the likelihood of litigation or designated materials as attorney work product as evidence that the organization was anticipating litigation and, therefore, had sufficient notice of its obligation to preserve materials.

Insurance Notification Clauses

The notification provisions typically included in claims-made insurance policies often raise questions similar to those an organization must consider with respect to its preservation obligations. These

provisions typically state that if an insured provides notice to its insurer prior to expiration of the policy of a circumstance that may give rise to a claim, the policy will provide coverage for a later-made claim relating to that circumstance. However, if notice of the circumstance is not provided, a later-made claim will not be covered by the expired policy and also may not be covered by a new policy, which will generally exclude claims arising from matters for which the insured had notice prior to commencement of the new policy. A commonly stated test for when notice of a circumstance should be given to an insurer is whether the known facts are "sufficiently serious to lead a person of ordinary intelligence and prudence to believe that it might give rise to a claim for damages." As with the obligation to preserve evidence, whether a circumstance is significant enough to warrant reporting to an insurer is a fact-intensive inquiry for which there is no bright-line test. Thus, the question that arises is whether an organization must issue a legal hold every time it notifies its insurer of a circumstance that may give rise to a claim.

There is little guidance provided on this issue. However, at least one court has considered whether the act of providing notice to an insurance provider constituted a triggering event for a defendant's obligation to preserve documents. In *Phoenix Four, Inc. v. Strategic Resources Corporation*, an investment company sued its investment advisor for fraud and other claims. The complaint was filed in May 2005, but on at least two prior occasions, and as early as May 2003, the defendant notified its insurers that a dispute existed.

In March 2005, the defendant vacated its office space and left behind a number of computers containing relevant ESI and documents that the landlord subsequently discarded. During discovery, the plaintiff filed a motion for sanctions and sought an adverse inference instruction against the defendant for abandoning the materials. The plaintiff argued, citing defendants' notifications to the insurance company, that the defendant had an obligation to preserve the materials because it had notice that the evidence might be relevant to future litigation. The court found that the references to future litigation included in the notifications to the insurance company, while thin, were sufficient to support a finding that defendants knew or should have know that the prospect of litigation was real.

Best Practices

When notifying an insurer of a circumstance that may lead to a claim, an organization should also consider whether it is necessary to suspend normal document destruction programs and to implement a document hold.

- **Seek Advice of Counsel.** When reporting a circumstance to an insurance company in compliance with a notification provision, an organization should consider consulting with in-house or outside counsel regarding whether there is a duty to preserve ESI and other materials relevant to potential future litigation.
- **Establish Procedures and Lines of Communication.** Courts necessarily review, with the benefit of hindsight, whether a duty to preserve evidence existed at some earlier point in time. To counter such an analysis, it is very helpful to be able to prove that the preservation issue was analyzed contemporaneously, and to be able to show the considerations that drove that analysis. Establishing policies and procedures to ensure that a contemporaneous analysis of the preservation obligation is undertaken is the best way for an organization to protect its interests. Those policies and procedures should establish lines of communication between the employees or departments responsible for compliance with notice provisions in insurance policies and those employees or

departments responsible for implementing legal holds.

For inquiries related to this Tip of the Month, please contact Michael J. Gill at mgill@mayerbrown.com, Sarah E. Reynolds at sreynolds@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 or Michael E. Lackey at mlackey@mayerbrown.com.

Please visit us at www.mayerbrown.com