MAYER·BROWN

Electronic Discovery & Records Management

2009 TIPS OF THE MONTH



TABLE OF CONTENTS

Page

January - Managing Risks and Cutting Costs: Remediation of Legacy Data 1

February - Process of Instituting a Litigation Hold 4

March - Preservation of Dynamic or Transitory Systems 7

April - Best Practices in Preparing for a Meet and Confer 10

May - Managing International E-Discovery Conflicts: Liberal US Discovery Rules Meet Foreign Data Protection Laws 13

June - Discovery of Data from Backup Tapes: Managing Risks and Shifting Costs 16

July - The Next Generation of E-Discovery: Social Networking and Other Emerging Web 2.0 Technologies 19

August - Managing Discovery Risks Using Federal Rule of Evidence 502 22

September - Managing the Risks and Costs of Responding to Civil Third-Party Subpoenas ... 24

October - Prosecuting Spoliation Claims 27

November - Defending Spoliation Claims 30

December - Managing the Risks and Costs of Collecting ESI 33

Copyright 2010. Mayer Brown LLP, Mayer Brown International LLP, and/or JSM. All rights reserved

MAYER·BROWN

Electronic Discovery & Records Management

TIP OF THE MONTH



January 2009

Managing Risks and Cutting Costs: Remediation of Legacy Data

Scenario:

In 2005, a government investigation of a company was initiated and class action litigation quickly followed. In response to the investigation and litigation, the company pulled backup tapes, de-activated the auto-delete function for its email systems, and imaged dozens of employees' hard drives. Four years later, the investigation has been dormant for some time, and the class action litigation has now mostly settled or has otherwise been dismissed, but some opt-out litigation remains active. Now, due to cost-cutting initiatives at the company, Information Technology and Records Management are demanding that Legal provide authorization to return to normal retention practices.

The following addresses the costs and risks associated with "legacy data," and the steps to be taken to remediate legacy data.

Risks and Costs Associated with Legacy Data

Remediation of legacy data is becoming an increasingly important component of effective information management policies and procedures. Legacy data generally consists of data that was retained outside an organization's routine records retention schedule and beyond any useful business purpose it once may have had, and yet continues to be retained due to fear that some small part of it might be relevant to pending or threatened litigation.

The discovery rules now require transparency for sources of data that are not "reasonably accessible." As a result, unnecessary retention of legacy data exposes an organization to the risk of being forced into expensive fishing expeditions in litigation, particularly where knowledge about legacy data sources is limited. Moreover, the retention itself can result in substantial costs that often are hidden or not fully appreciated because they are dispersed across an organization in different departments or business units.

The continued retention of legacy data also undercuts the purposes of the records management policy and increases the risks and costs of data management itself. The cost to store and maintain large quantities of data can be significant, and the burden and costs for retrieving relevant data increases with the volume of legacy data. The risk of losing, or simply being unable to locate, the useful data also increases.

Additionally, unnecessary retention of legacy data complicates, and can add dramatic expense to, unforeseen litigation.

- In-house and outside counsel are required to analyze legacy data as part of their required "reasonable inquiry" into sources of potentially relevant information in order to make accurate representations and disclosures to adversaries and courts.
- To the extent that the legacy data appears likely to contain relevant evidence that is not available from more accessible sources, it will be necessary to disclose the existence of the legacy data to adversaries and the court. This transparency must be volunteered, even absent an inquiry from the adversary.
- Once the legacy data is disclosed, adversaries have a road map for where to exert pressure in discovery. This will often lead to expensive motion practice, which can lead to data sampling and even expansive data restoration and discovery.
- There is also the risk that the legacy data will be lost or destroyed through inadvertence. If a court finds that there was neglect, or worse, the organization may be subject to spoliation charges and related sanctions.

Steps Toward Remediation of Legacy Data

The goal of a remediation project is to identify and segregate that portion of the data that may be subject to active legal holds, and to discard the rest in order to bring the legacy data into compliance with record retention policies.

Create legal hold portfolio.

Every organization should have a written protocol or policy for managing legal holds, including issuing, enforcing and lifting legal holds. It is essential to know information about the legal holds that are currently in force, and what they cover, because the main impediment to discarding legacy data is the potential applicability of legal holds. Information collected about legal holds should include:

- the individuals subject to the legal hold;
- the databases and other systems subject to the legal hold;
- business units impacted by the legal hold;
- the kind of evidence that is relevant;
- the relevant date range; and,
- any other information that would be helpful in determining which legacy data is and is not on legal hold.

Software and database tools are available to help manage and track this information about legal holds.

Analyze legacy data.

The legacy data should be analyzed and, to the extent practicable, identified, organized and catalogued; there are many different forms of legacy data so many different approaches are available.

- The first priority will be to remediate legacy data that, based on a high level analysis, can be ruled out as subject to legal holds (e.g., outside relevant time period, custodians that are not relevant). It may be necessary to sample other data to make a determination whether it is, in whole or in part, subject to a legal hold.
- Sources of data that do appear to contain relevant information may be retained and disclosed in relevant cases. Alternatively, a search protocol may be developed to segregate the irrelevant data so that portion can be remediated.
- To further mitigate risk in either case, it can make sense to inform adversaries in material litigation, and the court if a dispute erupts, of the intent to dispose of legacy data.
- To the extent that some of the legacy data will be retained long term, it can reduce costs and facilitate future disposition to organize and catalog the data. It also can be useful to collect the legacy data in a central location, and to integrate the catalog with the litigation holds management system.

Following these steps can result in a successful legacy data remediation project that significantly reduces the costs of storage, the cost of accessing retained documents and the risks associated with disclosure and production in the event of government investigations or litigation.

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

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

Please visit us at www.mayerbrown.com.

MAYER·BROWN

Electronic Discovery & Records Management

TIP OF THE MONTH



February 2009

Process of Instituting a Litigation Hold

***Scenario**:*

A large company implements a set of policies that govern the retention and destruction of data and documents. On March 1, 2009, a lawsuit is filed alleging that the company engaged in a price-fixing conspiracy for the past several years. Under the company's retention policies, many of the documents relating to the pricing and sale of the product at issue would be eligible to be discarded or destroyed.

What to Do Before Litigation Occurs

Courts have held that when a party reasonably anticipates litigation, "it must suspend its routine document retention/destruction policy and put in place a litigation hold to ensure the preservation of regular documents."[1] Although the process of instituting a litigation hold is often viewed as the first step when responding to an anticipated litigation or investigation, there are a few other steps that organizations can take to help control the costs and minimize the risks associated with document preservation.

***Understand the ESI Landscape*.**
In order to implement an adequate and defensible litigation hold, an organization should understand the types of electronically stored information (ESI) that exist, where the ESI is located, and who has control over the ESI. To do so, it can be helpful to catalogue all of the organization's active and legacy ESI. The level of detail depends upon the business, but organization should consider developing a catalogue that will:

- Identify types of active and legacy ESI and places where ESI may reside
- Identify ESI custodians for shared ESI, such as company databases and web pages
- Identify applicable retention schedules and auto-delete functions

This catalogue can be updated regularly and whenever sources of ESI are added or deleted.

Designate a Litigation Response Team.
An organization may also, in advance of litigation, consider identifying a response team that represents the relevant constituencies within the organization, including legal personnel, IT personnel, records management, human resources, and administrators. A litigation response team will facilitate:

- Identification of relevant ESI
- Suspension of applicable auto-delete functions
- Identification of individuals who have or control ESI that should be subject to a litigation hold

Identify When the Preservation Duty Arises

Generally speaking, the preservation obligation is triggered by "reasonable anticipation" of litigation. There is not typically a bright line, and it can sometimes be difficult to determine (and prove in hindsight) the precise point in a developing dispute in which litigation becomes reasonably foreseeable. Consideration should be given to this question as disputes are evolving.

Determine the Scope of the Litigation Hold

Before a litigation hold can be issued, counsel must determine what ESI must be preserved and which custodians must be notified. A litigant is under no duty to keep or retain every document in its possession; rather, the litigant is under a duty to preserve what it knows, or it reasonably should know, is relevant in the action. Courts have accepted an approach to evidence preservation based on a focus on "key players" – those who are expected to have relevant evidence based on the allegations in the case and their roles in the company. No effort will ever be perfect. Reasonableness is the standard.

In order to establish reasonableness later, if a challenge arises, it is important to document the steps taken to identify the custodians and relevant repositories of ESI. The process is iterative and the scope of the hold should be expanded, or narrowed, as the case evolves and more information becomes available.

Since 2006, the Federal Rules of Civil Procedure have invited, and even required, cooperation and transparency in matters of discovery, and judges are calling for a new spirit of cooperation. Engaging opposing counsel in frank discussions regarding ESI, as uncomfortable as that can sometimes be, is not only expected by the courts but can be of strategic benefit. Counsel should be open about ESI issues and seek agreements setting reasonable limits on preservation and discovery obligations. Even if agreement is not possible, disputes can be heard and resolved by the court before spoliation becomes the issue. Diligently working to narrow the scope of the hold and the ESI collection and production is one of a party's best tools for reducing the burden and cost of litigation.

Issue Litigation Hold Notice

- The Federal Rules of Civil Procedure require prompt intervention in routine operations in order to establish the good faith that can protect against sanctions. As early as practicable, the organization should send a legal hold notice to affected employees and other agents. The legal hold can be expanded as more information becomes available. The first legal hold notice need only be reasonable given what is known at the very outset of the matter.
- Organizations should consider having a legal hold template at the ready. Such a template would include standard instructions about how to override any automatic deletion functions pending the legal department's consideration of implementing more robust precautions. The template could have a space to insert basic, readily available information about the nature of the case so the

recipients can know what information might be relevant. A more detailed legal hold notice may follow that identifies more precisely and completely the relevant topics and information sources.

Monitor and Audit Compliance

Some courts have held that it is not enough to issue a litigation hold. They expect the legal department, and outside counsel, to take other affirmative steps to ensure that relevant information is not being lost as a result of routine operations. To ensure compliance by individuals placed on legal hold, the party can issue periodic reminders or to take other measures to ensure that their information is retained. Counsel should establish a process to identify and address changing personnel so that information is not lost when an employee who is subject to a legal hold changes job functions or leaves the company. Custodians of centralized information, such as databases, web pages, and warehouses, should be identified and given clear instructions. Occasional "spot checks" are a useful tool in auditing compliance with the litigation hold.

Re-evaluate the Litigation Hold

The "final" step in the process is periodic re-evaluation of the litigation hold to determine whether it should be continued, expanded, contracted, or lifted. In most cases, a hold should only be lifted when it is determined that the matter has been ultimately concluded and counsel does not anticipate any further litigation involving the same ESI.

For inquiries related to this Client Alert, please contact the authors, Jason Fliegel at jfliegel@mayerbrown.com or Gabrielle Butcher at gbutcher@mayerbrown.com.

For information about Mayer Brown's Electronic Discovery & Records Management practice, please contact Anthony Diana at adiana@mayerbrown.com, Michael Lackey at mlackey@mayerbrown.com, Tom Lidbury at tlidbury@mayerbrown.com or Edmund Sautter at esautter@mayerbrown.com.

Learn more about our Electronic Discovery & Records Management practice.

Mayer Brown LLP's Electronic Discovery & Records Management (EDRM) practice's "Tip of the Month" series provides information about effective risk and cost management practices associated with EDRM.

Please visit us at www.mayerbrown.com.

[1] *Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422, 439 (S.D.N.Y. 2004) ("*Zubulake IV*").

MAYER·BROWN

Electronic Discovery & Records Management

TIP OF THE MONTH



March 2009

Preservation of Dynamic or Transitory Systems

Scenario:

A manufacturing company is sued by a class of consumers each of whom alleges to have suffered damage from a manufactured item. Information about the research and development, marketing and sales of this manufactured item is kept on a number of relational databases maintained by the company. The company wants to comply with its preservation obligations but is not sure how to preserve constantly changing databases without taking them out of service.

Issues Presented in the Preservation of Data on Dynamic or Transitory Systems

Organizations may have systems containing data that is updated or changed over time (e.g., customer or sales information, financial data, research and development information, memoranda that are revised over time). When litigation implicating this dynamic data arises, an organization faces some interesting challenges, including whether it is sufficient to preserve the data as it exists at the time that the preservation obligation commences, or whether the organization will be required to preserve incremental changes in the data over the course of the litigation.

If the organization routinely saves successive drafts of a document, or periodically records the data contained in a system (e.g., monthly or quarterly), then it may be relatively easy for the organization to comply with its obligations when litigation arises. However, if such information is *not* preserved as a matter of course, other considerations come into play. Given that no organization is required to maintain every scrap of paper generated, the burden and cost of preserving data on dynamic systems (which may be updated hundreds or thousands of times each day) will need to be weighed against the potential liability presented by the specific facts and claims underlying each dispute. Additionally, dynamic systems typically have not been developed with preservation in mind, and, as such, there may be unique challenges presented in seeking to preserve such data.

Steps Towards Identifying Dynamic or Transitory Systems

As with many issues concerning the preservation of electronically stored information, there is no substitute for pre-litigation preparation. Thus, as a best practice, organizations that maintain dynamic data should become familiar with their systems in advance of any litigation or other dispute. Steps to consider, as appropriate to the circumstances, include:

- Developing a comprehensive understanding of any dynamic or transitory systems, particularly those that are most often relevant to litigation, governmental investigations, and third-party requests. This might involve discussions with IT personnel and area managers as well as a review of the kind of data contained on these systems.
- Documenting the information about the dynamic or transitory systems in order to ensure consistency across various litigations or other requests and to create institutional memory should personnel change.
- Taking steps to be sure that in-house and outside counsel understand the burden both to the operation of the business and from a pure cost perspective of preserving (and producing) such dynamic data.
- Developing and following guidelines that specifically address the preservation of dynamic or transitory systems. This guidance may include a discussion of whether "snapshots" of the data can be created, and under what conditions the organization might agree to create such snapshots. Other preservation alternatives may include maintaining logs of all changes to the database and avoiding system or other changes that might result in the loss of data.
- Creating a plan that so that the appropriate personnel associated with the dynamic or transitory systems are copied on any litigation hold notice. This plan could include checks to verify that any periodic "snapshots" are being taken.

Discuss Dynamic or Transitory Data with Opposing Counsel.
One possible method to reduce the risks associated with the preservation of dynamic data (the most significant of which is the potential for allegations of spoliation) is to approach the opposing party at an early stage to seek agreement on the nature and extent of the data to be preserved. Where appropriate, such early engagement may provide an opportunity to discuss: (i) any unique preservation issues presented by dynamic data; (ii) any technical complexities of the databases themselves; (iii) the extent to which the information contained on these databases is equally available from other sources; (iv) possible, less burdensome alternatives; and (v) to get a feel for the type and volume of information sought by the requesting party.

Considering that, by nature, dynamic data is subject to frequent, if not constant, change, it is imperative that any objection to preservation be registered with an opposing party as soon as practicable and, in some cases, even before a request for production has been made. Again, this pro-active approach will help to support the argument that the organization was forthright and fully complied with its preservation obligations.

Develop Standard Disclosure Statements Regarding Dynamic or Transitory Data.
To further avoid any suggestion that potentially relevant information was not preserved, and to ensure consistency across litigations, an organization should consider developing standard descriptions of its

dynamic data. These descriptions will aid in responding to document or other requests. Further, although the data itself is subject to frequent change, an understanding of the processes associated with developing the data will be invaluable when talking to fact witnesses and, in some cases, in developing arguments and defenses to the claims asserted in the litigation.

Following these steps is part of a comprehensive approach to the preservation of data from dynamic or transitory systems that will help to reduce the risks and costs of litigation and place an organization in the best position to defend itself.

For inquiries related to this Tip of the Month, please contact the authors, Kim A. Leffert, at kleffert@mayerbrown.com and Andrew J. Calica, at acalica@mayerbrown.com.

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

Please visit us at www.mayerbrown.com.

MAYER·BROWN

Electronic Discovery & Records Management

TIP OF THE MONTH



April 2009

Best Practices in Preparing for a Meet and Confer

Scenario

A large company is involved in a commercial litigation dispute that requires the collection and production of electronically stored information (ESI) maintained by its offices in the United States, Europe and Asia. During the Rule 26(f) conference, the parties discuss a variety of topics but do not discuss the fact that the large company intends to use keywords to search its servers for responsive ESI. Upon learning that keywords were used to identify responsive ESI, opposing counsel seeks a court order allowing submission of additional keywords to be used to search the company's servers. Opposing counsel also seeks to re-depose several company officers, at the large company's expense, based on the supplemental production.

Using the Rule 26(f) Meet and Confer Process for Strategic Advantage

Unlike traditional hard copy documents, ESI often is not stored in a fashion that facilitates easy identification of responsive information, i.e., there is often no neatly labeled electronic "file cabinet." Rather, parties frequently must harvest large volumes of data in an effort to ensure that they fulfill their obligations to collect and produce responsive, accessible information. This process can be costly and fraught with risk. While this may seem daunting, with the proper preparation and timely disclosure of a comprehensive preservation, collection and production plan, a party may use the meet and confer to strategically control discovery, and the costs associated with it.

Indeed, early disclosure of a well-developed plan, at a time when the opposing party is unaware of how the producing party stores the information , limits the opposing party's ability to rationally object to the plan. When the opposing party does gain additional insight, it may be too late to challenge the plan, as no objection had been previously raised. This concept of early and comprehensive disclosure is counter-intuitive to many litigators, who often see providing any information to opposing counsel as contrary to the adversarial system. But the courts are mandating such disclosure, and ignoring this requirement often inflates the risks and costs associated with discovery.

For example, courts routinely focus on the defensibility of the process used to identify responsive information, with heavy emphasis on disclosure; courts also look to efforts made, where possible, to reach agreement with the opposing party on the search and review methods to be used. Courts recognize that

the use of appropriate search methodology, including keyword searches, can be invaluable in managing the costs and time involved in collecting, reviewing and producing the significant volumes of data that come into play with ESI.

But importantly, courts will not hesitate to second guess methods of search and retrieval where no disclosure of the search methods to be used, or agreement with the opposing party, has been reached. In *In re Seroquel Products Liability Litigation*, 2007 WL 2412946 at *16 (M.D. Fla. Aug. 21, 2007), the court raised the possibility of sanctions against the producing party for not having disclosed and discussed a planned method of searching for responsive documents with opposing counsel.

Thus, there is a strong argument in favor of disclosing planned search and collection methods, including the data sources to be searched (custodians, databases, legacy data sources, etc.), the key terms and concepts to be utilized to search or cull information, and any date limitations. Where possible, parties should attempt to agree on search protocols and procedures that allow for the possibility of refining or expanding those terms as discovery progresses and that are reasonably tailored to yield responsive information. However, even if there is no agreement, disclosure of the search and collection methods may protect the disclosing party from any sanctions.

Preparing for the meet and confer can facilitate the discussions; whenever practical, parties should come prepared with potential search terms, methods and protocols to assist the discussion. To be prepared for the meet and confer, and to craft a reasonable ESI search, the party and its counsel should:

- Discuss the subject matter of the litigation with the key players. It may be necessary to discuss whether certain topics are referred to in an abbreviated form or through acronyms;
- Discuss the date parameters for each search, including when certain individuals were involved with the matter being litigated;
- Run test searches using the identified keywords to see if they are over- or under-inclusive;
- Consider using advanced ESI search methods through the use of Bayesian search systems or other forms of concept clustering, which can, in some cases, reliably and efficiently assist in reducing the amount of ESI that must be reviewed.
- Create a comprehensive list of attorneys and their staff that may appear in the data to be searched, this will help identify potentially privileged documents at the outset;
- Consult with IT personnel regarding the operation and search capabilities of the systems where the data are stored;
- Learn about data sources or data types that are unique to the client, such as dynamic databases and proprietary software; and
- Retain an expert that can assist in crafting a defensible search methodology.

Disclosure of ESI search methodology allows litigants to identify expectations and resolve, or seek court intervention to resolve, disputes before embarking on an expensive and potentially wasteful ESI search and review.

For inquiries related to this Tip of the Month, please contact the authors, Anthony J. Diana at adiana@mayerbrown.com, Robert E. Entwisle at rentwisle@mayerbrown.com and Jason Fliegel at jfliegel@mayerbrown.com.

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

Please visit us at www.mayerbrown.com.

MAYER·BROWN

Electronic Discovery & Records Management

TIP OF THE MONTH



May 2009

Managing International E-Discovery Conflicts: Liberal US Discovery Rules Meet Foreign Data Protection Laws

Scenario:

A multinational corporation is a defendant in a products liability action in a US federal court. During discovery, the plaintiffs request production of relevant emails from employees of an overseas affiliate of the defendant who are stationed in the Netherlands, France and Germany.

Discovery Issues Associated with Foreign Data Protection Laws

Foreign data protection laws present unique and potentially serious issues for multinational companies involved in government investigations or civil discovery. Whereas the principal e-discovery challenges within the United States involve how a party can best meet its obligations to preserve, collect, review and produce relevant data, an increasing number of foreign jurisdictions prohibit or restrict these very activities. This presents significant practical hazards as e-discovery instincts that might seem standard within the United States — such as collecting and reviewing a broader collection of data than might be strictly required — could lead to violations of foreign law. US courts have, to date, been reluctant to relax parties' obligations to respond to discovery, even where compliance with US discovery obligations might result in a violation of foreign law.

Differing Conceptions of Discovery and Privacy

At the root of these conflicts between US and foreign law are differing fundamental approaches to two key questions.

Pretrial Discovery: Whereas US rules of civil procedure permit broad pretrial discovery with minimal participation by the court, most other countries have much more restrictive views of the proper scope (and cost) of civil discovery, and often require direct court involvement in discovery.

Employee Privacy: Whereas US employees are generally deemed not to have an "expectation of privacy" with respect to email and other data created and stored on an employer's computer system, this view is not widely shared overseas.

Foreign Statutes and Regulations

In recognition of these differences, and in some cases for the express purpose of protecting citizens from the burdens of litigation discovery, many foreign countries have enacted strict privacy regulations and discovery "blocking" statutes.

The most prominent such regulation is the European Union's data protection directive. Adopted in 1995, the directive, together with the implementing laws of the various EU member states, restricts the "processing" and overseas transfer of "personal data." The definitions of "processing" and "personal data" are broadly worded, and might be read to restrict even the preservation of data (as well as any subsequent filtering and review) and to apply to any document that contains so much as an individual's email address. While a number of exceptions may permit the processing and transfer of data under some circumstances (e.g., unambiguous consent of the individual in question, or where it is necessary for the purposes of "legitimate interests" of the employer), the scope of these exceptions is the subject of significant uncertainty.

It is important to note that the EU's data protection directive applies to all overseas transfers of personal data, including a multinational corporation's voluntary transfer of its *own* protected information to the United States for disclosure in discovery. Also, while US privacy concerns often can be assuaged by the entry of a stipulated protective order limiting the recipient's use of confidential employee information, this solution alone generally will not satisfy the requirements of foreign data privacy laws.

Foreign blocking statutes can be more straightforward — simply prohibiting any activities in furtherance of foreign discovery proceedings. For example, a French statute prohibits "requesting, seeking, or disclosing in writing, orally, or in any other form, documents or information of an economic, commercial, industrial, financial or technical nature for the purposes of constituting evidence in view of foreign judicial or administrative proceedings." In a rare reported case of enforcement of this statute, a French lawyer was recently fined €15,000 for seeking discovery in France in response to a US court order.

US Courts Enforcing Discovery Obligations

Despite the restrictions imposed by foreign law, US discovery obligations, which extend to all materials within the "possession, custody or control" of a party to a US litigation, may still require production of overseas data. US courts have been reluctant to recognize foreign data protection laws as insurmountable obstacles to the gathering of responsive information stored overseas. As one court recently observed regarding electronic discovery of data residing in the Netherlands:

It is well settled that foreign blocking statutes do not deprive an American court of the power to order a party subject to its jurisdiction to produce (let alone preserve) evidence even though the act of production may violate that statute.

US courts will apply a balancing test if called upon to determine whether to enforce discovery obligations in the face of a foreign blocking statute. Factors considered include: How important is the information? How narrow is the request? What is the impact of noncompliance with the foreign statute on the foreign state's interests? Further, although the authority exists to order production, US courts are unlikely to enforce

those orders through sanctions if the failure to comply is due to a legal proscription and there is no evidence of "willfulness, bad faith, or any fault of" the party subject to the discovery.

In general, the possibility of fines and other remedies under foreign blocking statutes has not led US courts to relieve parties of their obligation to produce evidence located in foreign countries.

Managing the Catch-22

Where does that leave the multinational corporate defendant when faced with the possibility of being caught between conflicting laws in the United States and abroad? Upon receipt of a discovery request relating to data that resides in a foreign country, the defendant might consider the following steps before acting to preserve or collect the foreign data:

- Confirm that the data are within the party's possession, custody or control, and determine the physical location of the data in question, as well as the jurisdiction of employment of the individual data custodians.
- Consult with counsel in the relevant jurisdictions regarding the scope of privacy and data protection laws, and regarding potential alternate means of obtaining discovery in those jurisdictions, such as Hague convention procedures or local government consent.
- If a conflict is identified, consider conducting an initial internal "balancing" of the risks and benefits of compliance with US discovery obligations versus compliance with foreign law. Is voluntary production appropriate notwithstanding foreign law? Would production be appropriate only if compelled by the US court? Is there a reasonable basis to resist production?
- If the decision is made to preserve, collect, review and produce the data in question, consider strategies to minimize the risk of being found in violation of foreign law. Depending on the circumstances, effective measures might include some combination of the following: (i) obtaining consent of affected individuals, (ii) minimizing the volume of affected data through early use of narrowly tailored search terms, (iii) redacting personal identifying information from the data, (iv) minimizing the quantity of data transferred by conducting the review in the host country, (v) using protective orders and certified vendors in the United States to ensure the continued security of the data following transfer and production.

While courts in and outside of the US may always have different rules and norms regarding discovery, being aware of and planning for the differences will make facing international e-discovery issues easier.

For inquiries related to this Tip of the Month, please contact the authors, Joseph Baker at jbaker@mayerbrown.com, Kim A. Leffert at kleffert@mayerbrown.com,or Edmund Sautter at esautter@mayerbrown.com.

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

Please visit us at www.mayerbrown.com

MAYER·BROWN

Electronic Discovery & Records Management

TIP OF THE MONTH



June 2009

Discovery of Data from Backup Tapes: Managing Risks and Shifting Costs

Scenario:

A company is sued by a class of investors. The investors issue a discovery request for a large number of data files that are only tangentially related to their claim. The company is sure the requested materials do not indicate liability, but it fears the substantial cost of digging through mountains of backup tapes and archived storage media to demonstrate this fact.

Allocation of Discovery Costs

The US Supreme Court has long held that in federal litigation, "the responding party must bear the expense of complying with discovery requests." Several provisions of the Federal Rules of Civil Procedure do limit the ability to abuse this rule by issuing broad discovery requests intended to increase an adversary's litigation costs.

One such restriction is Rule 26(b)(2)(B), which frees responding parties from producing electronically stored information (ESI) from sources they "identif[y] as not reasonably accessible because of undue burden or cost." This protection is not absolute, however, and a court may order discovery from sources not reasonably accessible "if the requesting party shows good cause." Still, such requests may not require expenditures disproportionate to the amount in controversy. *See* Fed. R. Civ. P. 26(g)(1)(B)(iii).

In close cases, courts sometimes take a "you get what you pay for" approach, compelling production only if the requesting party pays part of the responding party's costs. The Advisory Committee Note to the 2006 Amendment to Rule 26(b)(2) supports this approach in relation to ESI deemed not reasonably accessible. Such "cost-shifting" has proven especially important in relation to backup tapes, which are typically expensive to restore and search, and which commonly yield few—but perhaps not zero—relevant documents not available on other media.

Prior to the 2006 Amendments, there was no universally agreed upon framework for deciding when to shift the costs of producing inaccessible ESI. The leading tests came from *McPeek v. Ashcroft*, 202 F.R.D. 31 (D.D.C. 2001); *Rowe Entertainment, Inc. v. William Morris Agency, Inc.*, 205 F.R.D. 421 (S.D.N.Y 2002); and *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309 (S.D.N.Y. 2003). Each involved, at least in part, requests for ESI available only on backup tapes.

The earliest of these cases, *McPeek*, enunciated the principle that "[t]he more likely it is that the [ESI] contains information that is relevant to a claim or defense, the fairer it is that" the responding party pay production or search costs. Of course, the likelihood that inaccessible storage media contain relevant information may be hard to estimate, and the court lamented that it was "impossible to know in advance what is on these backup tapes." To inform the "marginal utility" calculation, therefore, the magistrate judge ordered that a small sample of the tapes be restored.

Rowe went a step further and addressed how to decide whether to shift costs when marginal utility estimates and other relevant parameters are known. Surveying earlier decisions, the court listed eight factors that guided this determination. *Zubulake*, in turn, refined and prioritized the *Rowe* factors, ultimately producing a list of seven factors to be considered. Of these, the most important are (i) the specificity of the requests; (ii) the availability of the requested information from other, more accessible sources; and (iii) the total cost of production as compared to the amount in controversy and the resources available to each party.

While the 2006 version of Rule 26(b)(2)(C)(i)-(iii) changed the focus of cost-shifting analysis, the extensive overlap between the *Zubulake* factors and the Rule 26 considerations means that courts continue to consider the same kinds of factors as before. In particular, several trends spanning the adoption of the 2006 Amendments are identifiable:

- Courts frequently require producing parties to bear the costs of discovery where those parties have, after litigation has commenced or become reasonably foreseeable, allowed data that was readily accessible to become available only in less accessible form.
- Consistent with Rule 26's concerns about duplicative discovery, cost-shifting may be more frequent when previously produced information is sought in a second format.
- As in *Zubulake* and *McPeek*, courts still sometimes issue orders for small samples of ESI to gauge relevance and importance when it is possible to take such a sample, as with data stored on multiple back-up tapes.
- Courts commonly shift the cost of paying for special masters or ESI experts.
- Cost-shifting is more frequent when ESI is requested from a third party.

Best Practices

With courts still coming to terms with the 2006 amendments, the outcome of a request for cost-shifting can be hard to predict. In the absence of definitive guidance, the trends described above suggest the following:

- When potentially responsive ESI resides on both active storage media and backup tapes, preserve the more accessible version. A requesting party that deletes accessible ESI will likely have to pay to restore the lost material from backup tapes.

- An index of backup tapes can aid with cost-shifting requests. With a fixed recycling schedule, a small number of tapes together with active storage are likely to contain most of the materials present on all the other tapes, and the index can improve the predictive power of a sample if partial restoration is ordered.
- It is often helpful to present the court with specific requests and objections. Cost-shifting inquiries are highly fact-sensitive and courts consequently possess a great deal of discretion in deciding them. Where economic and practical details, such as the cost of ESI discovery, the amount at stake, the resources of the parties or the recovery methods to be used go unspecified, the court may make a determination adverse to the party failing to provide the requisite information.
- When presenting to the court the anticipated cost of compliance, responding parties should include the costs of attorney review of ESI. Because the issue of whether these costs are subject to shifting is unsettled, some courts may allow them to be shifted.
- Parties should be attentive to the expense of ESI discovery and potential alternative methods and should confer about potential cost-shifting as part of their early ESI discussions.

For inquiries related to this Tip of the Month, please contact the authors, Jason Fliegel at jfliegel@mayerbrown.com, Michael E. Lackey at mlackey@mayerbrown.com or Zachary Ziliak at zziliak@mayerbrown.com.

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

Please visit us at www.mayerbrown.com

MAYER·BROWN

Electronic Discovery & Records Management

TIP OF THE MONTH



July 2009

The Next Generation of E-Discovery: Social Networking and Other Emerging Web 2.0 Technologies

Scenario:

A whistleblower alerts authorities that brokers in a large brokerage firm may have violated a number of regulations regarding communications. The US Securities and Exchange Commission (SEC) commences an investigation regarding whether one broker "tweeted" about a pending hostile takeover on his Twitter account and whether another broker received insider information about the takeover on his "wall" after a client "blogged" about it on Facebook. The firm receives a demand from the SEC to retain all electronically stored information relating to the investigation.

The Internet Has Changed How We Communicate

When the Federal Rules of Civil Procedure regarding electronic discovery were amended in 2006, the Judicial Conference and the Supreme Court recognized that they could not anticipate how communications would develop over time. As a result, they adopted broad language permitting discovery of information "stored in any medium." This has allowed the Federal Rules to remain flexible in the evolving world of electronic communications. It is the flexibility of the Internet, however, that continues to outpace organizations' electronically stored information (ESI) retention and discovery policies and to challenge an organization's ability to monitor and manage its communications.

The number of people—and organizations—using social networking sites and other Web 2.0 technologies to communicate is rapidly increasing. The purposes of such uses are limitless. Organizations use them to market their brands, share information, negotiate and develop contractual relationships, keep tabs on the competition and keep in touch with their customers. Individuals use them to quickly share both personal and professional information, to network and to keep up-to-date on the latest industry and social developments. Industries are increasingly adapting these technologies for their own data management and internal communications. Examples of popular social networking sites include:

- Facebook and MySpace are social networking web sites where individuals and organizations can connect with others to communicate privately, share photographs and make global announcements. Facebook and MySpace are web-based applications hosted on off-site servers; they are accessible directly from an Internet browser and boast users of more than 200 million and 185 million, respectively.

- LinkedIn is a web site that paved the way for professionals to network in cyberspace. It provides the technology to post a resume, send messages and connect with current and former colleagues; it has upwards of 40 million users.
- Twitter is a free social networking and micro-blogging service that enables its users to send and read each others' updates, known as "tweets." "Tweets" are limited to 140 characters, are displayed on the author's profile pages, and are delivered to other users who have subscribed to them.

Other types of Web 2.0 technologies include wikis, blogs, collaboration software like SharePoint and Google Docs and video-sharing sites such as YouTube.

The Developing Legal Landscape

We may not yet know exactly how the legal system will treat Web 2.0 technologies, but history provides us with a roadmap. Each time a new technology has developed, from facsimile to email to instant messaging, the legal community has eventually accepted these new communication formats, ratified their use and, where applicable, subjected them to regulation.

In fact, some federal courts have already moved in this direction, describing Facebook messages as a hybrid between emails and blog postings. Some US federal courts have permitted the discovery of communications shared on web sites such as Facebook and MySpace to the extent such communications relate to subjects at issue in a litigation. Similarly, in February 2009, a court in Ontario, Canada, specifically held that a party maintaining a Facebook profile is in control of that information and, therefore, must produce information relevant to the issues in the litigation contained on the site.

Further, the groundwork has already been laid for government regulation of the use of these technologies, particularly in light of the current economic crises and the call for greater government regulation of the financial industry, including sectors that have not previously been regulated, like hedge funds. In addition to existing government regulations such as the record-keeping requirements of the Securities Exchange Act of 1934 and the Sarbanes-Oxley Act, the potential use of social networking sites for soliciting business, communicating about business activities, and discussing and negotiating contracts will most certainly contribute to financial regulators' interest in the preservation of Web 2.0 records.

Best Practices: Develop A Policy, Communicate It, Enforce It

Organizations need to get on top of this trend *now*, rather than waiting for circumstances to force the issue. As with all new technologies, communications via Web 2.0 systems like social networking sites *will* be used by your organization, *will* be recognized by the courts, *will* be subject to regulation and *will* be sought in discovery. The best strategy for any organization is to proactively adapt to this evolution and invest in the proverbial "ounce of prevention."

- Understand how your organization is using social networking and other Web 2.0 technologies. Counsel, IT administrators, records management and business units should meet and discuss the use emerging technologies.

- Determine whether there is a legitimate business need for the use of social networking and other Web 2.0 technologies at your organization. Where there is not, consider taking steps to block employee access to those sites.
- Educate employees—including legal personnel—on the use of social networking and other Web 2.0 technologies. Company personnel should understand what these technologies are, how they are used and the risks of such use, including regulatory and litigation risks.
- Incorporate Web 2.0 technologies into your current business and document retention policies, as appropriate. Consider developing policies that are mindful of the business uses of these technologies and any legal or regulatory requirements, but also instruct employees on how to minimize the risks of such use. One option is to put in place procedures for monitoring your organization's use of social networking sites and other Web 2.0 technologies, and for ensuring that employees understand that their use of these social networking sites on behalf of the organization is being monitored.
- Think about developing procedures and methodologies for capturing the fluid data of Web 2.0 in its various incarnations. Software can be put in place to support the retention of those technologies where required, procedures can be established to notify third parties of the need to secure that data where applicable, and processes can be put in place to identify and collect such data when necessary. Keep in mind that, because each technology is different, a blanket procedure may not be sufficient.
- Finally, an organization should periodically audit its own policies to ensure it is complying with its own requirements, industry standards and adapting to new technologies.

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

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

Please visit us at www.mayerbrown.com

MAYER·BROWN

Electronic Discovery & Records Management

TIP OF THE MONTH



August 2009

Managing Discovery Risks Using Federal Rule of Evidence 502

Scenario:

A series of privileged communications between in-house counsel and the board of directors was unintentionally produced to the opposing side during the pre-deposition discovery period in a federal action. During the deposition of one of the board members, the opposing side submits the set of privileged documents as an exhibit. There is no agreement or court order on file in the case dealing with the inadvertent production of privileged documents.

Risks Associated with Inadvertent Privilege and Work Product Waiver

As many attorneys can attest, because of the volume of documents involved in many cases, even with the most diligent of privilege reviews, a party can inadvertently disclose privileged documents. Inadvertent disclosures can result in a waiver of privilege with the scope of the waiver depending on the jurisdiction of the court. Some courts have limited the scope of the waiver to, at most, the inadvertently produced documents themselves, while others have applied subject matter waiver.

Federal Rule of Evidence 502

The Federal Rules of Evidence include procedures to protect parties that inadvertently disclose privileged documents during litigation. This protection operates as long as the disclosure was unintentional, and the producing party behaved "reasonably" both before and after the disclosure. Federal Rule of Evidence 502 — which was signed into law on September 19, 2008 — protects against the inadvertent waiver of the attorney-client privilege; it is applicable in all proceedings pending on, or commenced after, its date of enactment.

FRE 502 states that there is no waiver of privilege in the event of an inadvertent disclosure of privileged or protected documents in federal proceedings if the holder took reasonable steps both to prevent the disclosure and to rectify the error when it did occur. In early August, in *Coburn Group, LLC v. Whitecap Advisors, LLC*, 2009 WL 2424079, the Northern District Court of Illinois cited FRE 502 when it ordered the return of an email that had been inadvertently produced to plaintiffs after a privilege review conducted by two experienced paralegals. Defendants learned of the inadvertent production when the email was used during the deposition of the email's author.

Crucially, unlike case management orders of the past, FRE 502(d) provides that non-waiver orders issued by a court in federal proceedings are binding on other federal and state courts. Non-waiver agreements between parties must be incorporated into an order to obtain the benefit of this protection.

Best Practices: React Quickly, Negotiate a Discovery Agreement and Obtain a Court Order

Generally, because of the reasonableness requirements found in FRE 502, organizations that wish to take advantage of the rule should adopt defensible privilege review policies and practices. Indeed, the best way to take advantage of the FRE 502 protections is to be diligent during the discovery process and react quickly to any instances of inadvertent disclosure of privileged documents. To best position themselves to gain the benefits of FRE 502, litigants should consider taking the following steps:

- Negotiate an agreement that sets forth what will be considered reasonable efforts to protect privilege and that provides for the return of privileged documents if inadvertently produced.
- Have the discovery agreement entered as an order of the court.
- Implement defensible privilege review practices. The traditional method is a page-by-page review of all documents for potential privilege, followed by a privilege-logging process where the final decisions are made. Given that most information is now electronic, and generally is electronically searchable, modern practice in cases with voluminous data usually also includes running searches for known lawyers and subjects likely to be privileged. The wisdom of this practice is reinforced by recent studies that call into question traditional assumptions about the superiority of human review relative to other methods. In fact, it may well be true that such electronic searches are equally or more efficacious than human review and should be considered an adequate substitute to linear document review.
- A litigant involved in simultaneous state and federal proceedings should seek protections through the federal system because, pursuant to FRE 502, a court order in a federal case granting protections against inadvertent waiver will automatically apply to subsequent state proceedings.
- Attorneys dealing with opposing counsel and attending depositions should be prepared to react quickly and reasonably if it becomes apparent that privileged information has been inadvertently produced.

For inquiries related to this Tip of the Month, please contact the authors, Jason Fliegel at jfliegel@mayerbrown.com or Vazantha Meyers at vmeyers@mayerbrown.com.

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

Please visit us at www.mayerbrown.com

MAYER·BROWN

Electronic Discovery & Records Management

TIP OF THE MONTH



September 2009

Managing the Risks and Costs of Responding to Civil Third-Party Subpoenas

Scenario:

A large, publicly traded manufacturing company is sued by a class of shareholders claiming various securities law violations as well as a failure to disclose the declining sales of one of the company's manufactured items. The plaintiff class issues a subpoena for documents to a key supplier of the manufactured item at issue. The subpoena specifically requests emails and other communications between the supplier and the defendant manufacturing company regarding manufacturing and supply problems during a specified period of time. To identify and collect all of the electronically stored information (ESI) that potentially would be responsive to this subpoena would take substantial time and effort on the part of the supplier's legal department, IT staff and business management. Further, the supplier suspects that some or all of the information can be more easily obtained from the defendant manufacturing firm.

Rule 45 Limits the Burdens on Third Parties

Under Federal Rule of Civil Procedure 45, a party seeking discovery from a third party has an affirmative duty to take reasonable steps to avoid imposing an undue burden or expense on the person or entity subpoenaed. Courts have consistently held that third-party status is a significant factor to be considered when determining whether a subpoena is unduly burdensome. Accordingly, a third party's obligation to preserve and produce relevant ESI is far more limited than that of the parties involved in litigation. Third parties, however, still should be mindful of their obligations to preserve ESI and documents where they reasonably anticipate being named *parties* to the litigation.

Best Practices for Third Parties Subject to a Subpoena

Rule 45 provides that if an objection is made to a subpoena, an order to compel production "must protect any person who is neither a party nor a party's officer from significant expense resulting from compliance." Rule 45(c)(3)(A) instructs that "[o]n timely motion, the issuing court must quash or modify a subpoena that … subjects a person to undue burden." Consistent with this approach to third parties, federal courts are not only empowered, but are directed, to quash the subpoena, to modify the subpoena, to shift some or all of the costs of production to the party issuing the subpoena or to impose another appropriate sanction on the

issuing party or its attorney (for example, attorneys' fees), where compliance by a third party would cause undue burden or expense.

Because many subpoenas use boilerplate language, they often contain ESI requests that are *not* narrowly tailored to avoid burden on third parties. Third-party recipients of these subpoenas need to quickly raise objections in order to avoid the burdens of preservation and production of ESI. These objections can and should include those relating to the form or forms in which ESI is requested to be produced, as well as objections limiting the production of ESI from inaccessible sources except for "good cause." Third parties may also refuse to preserve or produce particularly burdensome categories of ESI, such as metadata, dynamic or transitory data, voice mail and instant messages, and should so state in their objection to the subpoena.

Further, in objecting to a civil subpoena, third parties should clearly state what categories of ESI are being searched, what categories of ESI are not being searched and what steps (if any) are being taken to preserve relevant ESI. Once the third party makes clear that it not only objects, but also will not preserve certain data, the burden shifts to the requesting party to take steps to ensure that such data is preserved (that is, by filing a motion to compel or by notifying the third party that the data should be preserved) and to explain why the third party should incur such burdens.

This burden shifting is crucial to protect the interests of the third party. To ensure timely responses, an organization that regularly receives third party subpoenas can consider preparing standard objections relating to the preservation and production of ESI.

Note, however, that the limitations set forth in Rule 45 do not exempt a third party from promptly and properly complying with the terms of the subpoena to which it is not objecting. An organization served with a subpoena should employ reasonable measures to comply with the subpoena, such as distributing copies of the subpoena to those who are likely to have, or to know where to locate, the requested information, and consider issuing appropriate preservation notices.

Where ESI will be produced in response to the subpoena, counsel should ensure during the meet and confer process that the parameters of third party's obligations are clearly drawn. That is, outside counsel, with its client's help, should strive to identify the universe of custodians likely to possess the data sought and limit production to the smallest possible group of representative custodians. This will prevent the third party from incurring the processing and review costs of searching the data sources of every potential custodian.

In addition, the third party can consider in advance just how far it is willing to go in responding to the subpoena. Sometimes, after a representative group of custodians have been identified and their responsive data produced, the party seeking discovery will request that the data from additional custodians be searched. In some cases, accommodating such a request may be easier and more efficient than fighting a motion to compel. However, where it appears that the party seeking discovery is engaging in a fishing expedition, refusing to produce such data until so ordered by the court in response to a motion to compel may be the only reasonable alternative.

Finally, organizations should consider procedures to ensure that legal holds related to subpoenas are lifted within a reasonable time after compliance. One option is to notify requesting counsel, in writing that the third party intends to return to its normal retention policies after production of responsive ESI is complete and absent any objection from the requesting party.

For inquiries related to this Tip of the Month, please contact the authors, Kim A. Leffert at kleffert@mayerbrown.com, David K. Cole at dcoleIII@mayerbrown.com and Therese Craparo at tcraparo@mayerbrown.com.

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

Please visit us at www.mayerbrown.com

MAYER·BROWN

Electronic Discovery & Records Management

TIP OF THE MONTH



October 2009

Prosecuting Spoliation Claims

Scenario:

A large company is defending itself in a breach of contract lawsuit. In order to prepare its defense, the company requests documents from the plaintiff that include electronically stored information (ESI). The company believes that plaintiff possesses certain emails and drafts of the contract that may refute plaintiff's interpretation of the contract. However, plaintiff has not produced the requested documents. The defendant company suspects plaintiff has failed to preserve the ESI on backup tapes, perhaps even intentionally.

Prosecuting Spoliation

A party engages in spoliation when it destroys or significantly alters evidence that is relevant to pending, imminent, or reasonably foreseeable litigation, or if it fails to preserve property (such as a company laptop) for another's use in litigation. The specific elements of spoliation claims and their consequences vary widely among jurisdictions, and thus applicable law should be consulted. Most large organizations tend to think of spoliation as a defensive issue. However, an organization that takes appropriate steps to preserve relevant information may be in a strong position not only to defend itself from accusations of spoliation, but to affirmatively pursue spoliation claims against a litigation opponent that fails to meet its own preservation obligations.

If a party is found to have engaged in spoliation, it may face a number of consequences, including sanctions and the undermining of its credibility before the court. Accordingly, a litigant that has met its preservation obligations, and that determines that its opponent has not, can consider whether it is advantageous to pursue spoliation sanctions.

In determining whether to award sanctions, and which sanctions to apply, courts will typically consider the spoliator's degree of fault, the prejudice suffered by the opposing party, and the nature of the sanction being sought by the moving party. Potential sanctions for spoliation include:

- Monetary penalties;
- Stricken pleadings;
- Exclusion of evidence;
- Loss of attorney-client privilege or work-product protection;
- Adverse inference instructions; and

- Dismissal, default judgment and possible criminal penalties, in particularly egregious circumstances.

The most common spoliation sanction is a monetary penalty, which can take the form of a fine, an award of attorneys' fees or a shifting of legal costs. In one case, the District Court for the District of Columbia imposed a fine of several million dollars against a party in connection with its periodic system-wide destruction of email over a two-year period. The large sanction appears to have been issued, at least in part, as a result of the court's belief that the defendants continued to permit monthly destruction of email for several months after learning of the problem and waited more than four months to notify the court and opposing counsel.

A spoliator may also face more severe sanctions, such as an adverse inference instruction, which permits the jury to infer that the missing evidence would have harmed the spoliator's case, or a default judgment. In one 2005 case, a defendant financial institution was found to have engaged in a practice of overwriting email every 12 months, despite an SEC regulation that required the company to retain email for a two-year period. The trial court ordered the defendant to produce backup tapes, review emails, conduct searches, produce responsive emails and a privilege log, and certify compliance with the order. After the defendant certified compliance with this order, the trial court found that the defendant possessed more than 1,400 backup tapes that had not yet been processed or produced, and that the defendant continued to overwrite emails and fail to produce emails and attachments. The court ultimately granted plaintiff's motion for a default judgment in part and deemed certain facts admitted for purposes of trial. The court also revoked the *pro hac vice* admission of the defendant's counsel. At the conclusion of the trial, the jury awarded a judgment well in excess of one billion dollars against the defendant, more than half of which was punitive damages.

Best Practices

In order to lay the foundation to pursue a potential spoliation claim, a party to a lawsuit should consider whether taking the following affirmative steps is appropriate in their matter:

- Ensure that your organization has met its own preservation obligations.
- Send a preservation letter (also known as a "first-day letter") to the opposing party that identifies the types of ESI and hardware (e.g., personal laptops or computers) that would likely be subject to discovery. A first-day letter puts the opposing party on notice that you consider data from those sources of ESI to be relevant, and can then be used later as evidence if the ESI is subsequently destroyed.
- Seek a court order concerning the parties' obligations to preserve and produce relevant ESI. Like a preservation letter, such an order can help lay the groundwork for a subsequent spoliation motion.
- Use a Federal Rules of Civil Procedure 30(b)(6) deposition to obtain information regarding the steps that were taken to preserve and produce documents. You might also ask such questions during depositions of fact witnesses. Such questioning may expose holes in the opposing party's production.

- Seek out third parties who may possess relevant ESI. If that third party produces responsive ESI containing communications with the opposing party, but the opposing party never produces such ESI, this may point to possible spoliation.
- Employ a forensic computer expert to discover and prove a spoliation claim by having the expert examine the opposing party's computer systems to determine whether ESI was modified or destroyed.

For inquiries related to this Tip of the Month, please contact the authors, Jason Fliegel at jfliegel@mayerbrown.com, or Anne De Geest at adegeest@mayerbrown.com.

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

Please visit us at www.mayerbrown.com

MAYER·BROWN

Electronic Discovery & Records Management

TIP OF THE MONTH



November 2009

Defending Spoliation Claims

Scenario

A large company finds itself defending against a contentious employment discrimination lawsuit. During discovery, the company's document production includes electronically stored information (ESI). Plaintiff alleges a gap in the ESI produced by the company and asserts that it resulted from the company's failure to implement an adequate litigation hold. Accordingly, plaintiff makes a motion seeking spoliation sanctions.

Defending Against Spoliation

The duty to adopt appropriate measures to preserve relevant evidence arises when a party receives notice of or reasonably anticipates litigation. Significantly, the preservation obligation can occur well before a lawsuit is actually filed. Even after a "triggering event" has happened, a company still is not required to preserve "everything" — for example, every email sent or received, all of its hard copy or electronic documents, or every backup tape then in existence. Rather, the law attempts to strike an appropriate balance; one that allows companies the flexibility they need to continue day-to-day operations while also ensuring that the parties are able to conduct full and fair discovery.

Spoliation Factors

While there is no single test or set of factors to determine if spoliation sanctions are warranted, generally speaking, a party engages in spoliation when:

- It destroys or significantly alters evidence that is relevant to pending, imminent or reasonably foreseeable litigation, or
- It fails to preserve relevant property for another's use in litigation.

While a culpable state of mind is often considered a condition precedent to the imposition of sanctions, some courts have indicated that spoliation can result from mere negligence, particularly in cases where the relevance of the destroyed evidence is readily established or the degree of prejudice to the requesting party is significant. The specific elements of spoliation claims and the consequences of these vary widely among jurisdictions, so it is necessary to determine the applicable law in the relevant jurisdiction in order to properly defend against these claims.

Importance of the Litigation Hold

A comprehensive document retention policy that provides for the application of litigation holds can be critical in defending against spoliation claims. A litigation hold suspends routine destruction of discoverable ESI. While many courts treat the existence of a litigation hold as a necessary condition for avoiding spoliation penalties, implementation of the hold is equally important. Failure to timely implement a reasonable litigation hold can result in sanctions if that failure results in loss of relevant ESI.

Determining the proper scope of the litigation hold is also an important step to avoiding sanctions. As a general matter, the preservation duty attaches only to the ESI in a party's possession, custody or control that can be reasonably foreseen to be relevant and discoverable in the litigation. In assessing the proper scope of preservation, consideration should be given to, among other things, ESI in the control of a vendor or contractor providing outsourced services. A party also should consider whether non-traditional forms of ESI, such as audio recordings or voicemail records, fall within the scope of its preservation obligations.

The preservation and restoration of backup media is a frequently litigated issue. At least one court has found that inaccessible backup tapes are generally not subject to a litigation hold. Nonetheless, a litigant should consider whether it should preserve backup tapes that contain ESI for key custodians. A key factor to consider in making this determination is the extent to which the data on the backup media is duplicative of other, more accessible, sources of relevant data.

Potential Spoliation Sanctions

The severity of a spoliation sanction can vary substantially depending on whether the court determines that the loss happened intentionally, negligently or despite a party's reasonable preservation efforts. If a party is found to have engaged in spoliation, it may face a number of damaging consequences, including sanctions and the undermining of its credibility before the court. In determining whether to award sanctions, and which sanctions to apply, courts will typically consider:

- The spoliator's degree of fault,
- The prejudice suffered by the opposing party, and
- The nature of the sanction being sought by the moving party.

The most common spoliation sanction is a monetary penalty, which can take the form of a fine, an award of attorneys' fees or a shifting of costs. Other potential sanctions for spoliation can be more severe, including the striking of pleadings, the exclusion of evidence, the loss of attorney-client privilege or work-product protection, the issuance of an adverse inference instruction or even the dismissal of the suit or entry of a default judgment. Depending on the context, the loss of evidence can even lead to criminal penalties.

Best Practices

Having a comprehensive and defensible electronic discovery process is one of the best defenses to spoliation claims. Not only will such a program decrease the likelihood of losing relevant evidence, but it also can mitigate the severity of any adverse consequences should relevant evidence be lost. Thus, proper

documentation of preservation and discovery efforts is important because it can help demonstrate that a party has taken reasonable steps to comply with its discovery obligations. To successfully defend against spoliation claims, the following types of evidence can demonstrate good processes and show compliance with discovery obligations:

- The timing and scope of the litigation hold;
- The follow-up efforts to monitor compliance;
- The scope of successful evidence collection by source;
- The reasonable measures put in place to monitor compliance with the legal hold and to identify and collect relevant, discoverable evidence;
- The proportionality of preservation and collection measures to the case; and
- The search terms and/or other methodologies used to identify relevant ESI, why those terms or methods were selected, and how effective they were in identifying relevant ESI.

Parties are expected to meet a standard of reasonableness, not perfection, in their preservation efforts. A party's ability to show that it had a reasonable process, that it followed that process in a reasonable manner and that it acted in good faith should go a long way toward helping that party avoid a spoliation sanction where relevant evidence is lost despite those efforts.

For inquiries related to this Tip of the Month, please contact the authors Kim A. Leffert, kleffert@mayerbrown.com and Michael Daly, mdaly@mayerbrown.com.

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

Please visit us at www.mayerbrown.com

MAYER·BROWN

Electronic Discovery & Records Management

TIP OF THE MONTH



December 2009

Managing the Risks and Costs of Collecting ESI

Scenario

A large corporation was named as a defendant in a product liability lawsuit. The corporation has preserved a massive amount of electronically stored information (ESI) in response to the suit and is now considering how much of the ESI, and which portions, to collect in order to review and produce it.

Collecting ESI — Who, What, Where, When and How

While preservation may prevent spoliation of ESI, before such ESI can be reviewed and produced, it must actually be *collected*. The collection of ESI can be both a technically and legally complex endeavor. In order to manage the risks and costs of collecting ESI, a litigant is well advised to design and document an ESI collection plan which considers the following five questions: Who, What, Where, When and How.

WHO Should Collect the ESI?

One of the first decisions a collecting party faces is whether to handle the collection internally or to outsource the process to a specialized vendor. The appropriate choice will depend on the specific organization and the nature of the particular litigation and data at issue, as well as on such factors as the frequency with which the party finds itself in litigation, the capability and availability of internal IT resources to perform the collection, the financial stakes of the litigation, and the sensitivity of the data to be collected. Outsourcing the collection process is not an all-or-nothing decision, because parties may outsource some portions of the collection process while retaining direct control over others. Using a vendor to collect data can be more expensive than using internal staff. However, one must also consider whether internal staff persons have the appropriate time, sophistication and tools to collect the data properly and completely.

WHAT (and How Much) to Collect?

A producing party has no obligation to collect or produce "every shred of paper, every e-mail or electronic document, and every backup tape" it possesses. Collection need only be reasonable – not perfect – and proportionate to the needs of the case. The producing party should focus its effort on a reasonable and proportionate number of employees. The producing party also should adopt a collection protocol that minimizes over-collection. For example, the producing party might use inclusive or exclusive filters when collecting from desktop and laptop hard drives, or copies of those drives, to avoid paying to collect and process system files and executables, Internet "cookies" and temporary Internet files, "deleted" data that is only recoverable from fragmented or slack space using forensic tools and techniques, and other types of

data that generally are not important enough to warrant the expense associated with collection and processing. The producing party might rely on employees to identify their relevant email folders and/or run targeted searches for relevant email. What is reasonable and proportionate will vary depending on the nature of the case. The point is that there are many methods to keep the collection within a reasonable scope and producing parties should not simply assume they must perform a massive collection.

Where agreement on a collection protocol can be reached, that is desirable. Where agreement cannot be reached, producing parties can minimize their risks by being transparent about the limitations that they believe are reasonable and proportionate. This allows disagreements about those limitations to be aired and decided by the court at an early stage, before sanctions are likely to be an issue. It must be recalled that significant costs and risks also arise from over-collection.

WHERE (and from Whom) to Look?

The specifics of the lawsuit will determine where to look for ESI and who are the key players. In many cases, a significant portion of ESI that must be collected is retained or managed by the "key players" in that case. The collection team should interview these key players and their assistants, along with any IT professionals with knowledge of such persons' files to ascertain where relevant information is located. Examples of such systems and media include email and instant message (IM) servers; enterprise archival systems; hard drives in notebook and desktop computers; personal digital assistants (PDAs) such as BlackBerries; removable media; personal network storage locations; shared network storage locations; software applications with their associated databases; and telephone and voicemail systems. In some cases, collecting a 'mirror image' of a key player's hard drive is an important part of a forensically sound collection. However, it is often unnecessary, particularly when the circumstances of the case, the cost of collection and the cost of culling through irrelevant data do not justify taking mirror images. As with other aspects of collection described earlier, the identities of the individuals from whom data are collected can, in appropriate cases, be a topic of negotiation with the other parties to the litigation. Often agreement can be reached that there is no need to collect data from individuals at the relative periphery of the litigation.

In addition to looking for ESI possessed or managed by key players, a reasonable and good faith effort must be made to identify and collect the relevant and potentially discoverable ESI that may reside in a party's databases, website servers, and intranet servers, or with third parties in possession of data under the party's control. Note that collecting data from a complex, relational database is often not possible since the "file" is constantly changing; however, it may be sufficient to generate a report encapsulating all potentially relevant points and to collect that report instead.

WHEN Should Collection Occur?

It is no longer safe for producing parties to wait for discovery requests to begin looking for relevant evidence. The 2006 amendments to the Federal Rules of Civil Procedure require parties to take affirmative steps to reasonably ensure that relevant evidence is preserved. One approach to compliance is to "collect to preserve" at the outset of pending or threatened litigation. This comes at a cost, however, and other protocols may be put in place to comply with the duty to take affirmative steps to preserve relevant evidence.

HOW to Collect?

The actual collection methods can be as varied as the ESI to be collected. One option is to use specialized tools that collect ESI in a "forensically sound" manner. A forensically sound collection of ESI maintains the integrity of the collected files and their associated metadata and often assigns a hash code that can be used to detect subsequent iterations of the file. These tools range from systems that require the relevant custodians to identify relevant files themselves (which may be done under the supervision of a lawyer or paralegal) to systems that reach directly into ESI storage locations, (e.g., email servers, file servers, hard drives) and collect all files matching the established criteria. If the company lacks such tools then the company may hire a vendor that is capable of forensically sound collection of ESI.

Forensically sound collection may not always be necessary, reasonable or proportionate to the needs of the case. It is still common in many cases, particularly smaller cases, to collect and produce printed versions of ESI. There are also degrees of forensic soundness. For example, many collection methods exist that affect only limited metadata, such as the metadata which tracks the date a file was last opened. This type of metadata usually is not critical, or even useful. Adopting a collection method that affects such inconsequential metadata may be appropriate where there is no substantial reason to believe that it will turn out to be important to the case.

For inquiries related to this Tip of the Month, please contact the authors Tom Lidbury at tlidbury@mayerbrown.com, Kim A. Leffert at kleffert@mayerbrown.com and Christopher M. Barrett at cbarrett@mayerbrown.com.

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

Please visit us at www.mayerbrown.com